

COPYRIGHT NOTICE

**IT IS ILLEGAL TO REPRODUCE , SHARE, OR DISTRIBUTE THIS ELECTRONIC PUBLICATION.
IF YOU DESIRE TO PURCHASE ADDITIONAL COPIES,
PLEASE CALL 800/523-4778, Ext. 235
OR VISIT OUR WEBSITE WWW.PROBANK.COM.**

This electronic publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or accounting services. If legal advice is required, it is recommended that each financial institution consult its own counsel.

Professional Bank Services, Inc. grants permission for the individual purchaser to view, print or save this electronic publication limited to their own device for their own use. Purchaser agrees to be responsible for any electronic publication saved to their device and Professional Bank Services, Inc. assumes no liability for any reliance upon any stored publication on purchaser's device that may have become outdated.

©Copyrighted. Professional Bank Services, Inc. All rights reserved.

This publication or parts thereof may not be reproduced, shared or distributed in any form, stored in any retrieval system, or transmitted in any form by any means—electronic, mechanical, photocopy, recording, or otherwise—without prior written permission of the publisher. This electronic publication is intended for the individual purchaser's use only and should not be shared or distributed by any means.



ProBank Austin



2021 BANK SECRECY ACT TWO-DAY SCHOOL

A ProBank Austin Seminar

2021 Bank Secrecy Act Two-Day School



ProBank
Austin

**IT IS ILLEGAL TO REPRODUCE THESE MATERIALS. IF YOU DESIRE TO PURCHASE
ADDITIONAL COPIES, PLEASE CALL 800/523-4778, Ext. 235
OR VISIT OUR WEBSITE WWW.PROBANK.COM.**

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or accounting services. If legal advice is required, it is recommended that each financial institution consult its own counsel. **This material may not be reproduced without written permission of ProBank Austin.**

©ProfessionalBankServices, Inc.

April 5, 2021

Seminar Attendees Telephone Support



Call in questions

ProBank Austin is pleased to provide telephone support for seminar attendees to ask questions after the seminar for ninety (90) days after the program date—at no charge. Call us at 800.523.4778, Option 3.

Calling ProBank



- Please review the relevant portion of the manual prior to calling. Have it available for reference during the call.
- Your call will be routed to a voice mailbox, for distribution to one of our consultants. You will be asked to provide the following information—it is essential that you provide this information, otherwise we may not be able to assist you:
 - The name and date of the seminar you attended;
 - The instructor who taught the seminar;
 - Your name and telephone number (including the area code and any extension); and
 - A brief description of your question.
- Your call will be returned as soon as possible. However, please remember that all of our speakers and consultants are frequently traveling and/or on job sites. Since we return calls from all over the country, often we will attempt to reach you outside of normal office hours. If we cannot reach you personally, and you have left a clear, detailed question, we will leave you an answer on your messaging system.

Fees

We answer routine questions from seminar attendees for free, for ninety (90) days after the seminar.

We charge for calls

- If the caller did not attend the seminar;
- More than ninety (90) days after the caller attended the seminar; or
- Where it is necessary for us to review forms, policies, advertisements, documentation or conduct research. You will be given a quote of the applicable charge prior to any service being performed.

No Email

We are sorry, but we do not take nor answer questions via email, except from our current consulting clients.

Seminar information

Seminar Name: _____

Seminar Instructor: _____

Seminar Date & Location: _____

Privileges expire

Call in privileges good through _____ (ninety (90) days after seminar).



ProBank
Austin

950 Breckenridge Lane, Suite 280 • Louisville, Kentucky

AN OVERVIEW OF PROBANK AUSTIN'S COMPLIANCE CONSULTING SERVICES



ProBank Austin (ProBank) is a nationally recognized provider of consulting and training services for traditional financial institutions and online lenders. We specialize in issues relating to compliance with federal lending, deposit, and BSA/AML regulations. Founded in 1978, ProBank has presented seminars for more than 25 state banking associations and several state banking departments. Past clients include the Federal Deposit Insurance Corporation (FDIC) and various other governmental agencies.

INHOUSE TRAINING – ProBank has an impressive menu of educational programs designed to keep staff members up-to-date on the rules and regulations which govern their institution. Every program we offer in a traditional seminar environment can also be presented in-house to your staff. Whether the focus is to address deficiencies cited in regulatory or internal reviews or to clarify areas of compliance which consistently garner questions from your staff, we will deliver a program addressing concerns that are uniquely yours. Frequently we find such sessions are great team builders as well.

COMPLIANCE REVIEWS – These reviews are designed to evaluate an institution or line of business' overall compliance management system or program. Following an approach similar to regulatory agencies, our consultants conduct a risk assessment, then sample actual transactions. The broad scope review covers topics included in a regulatory compliance examination. If requested, reviews can be focused on specific topics. Our professionals conduct hundreds of these reviews coast-to-coast each year.

INDEPENDENT BSA/AML EVALUATIONS – This service is designed to satisfy regulatory expectations for financial institutions to conduct an annual, independent evaluation of its BSA/AML program. We review and assess the institution's written BSA policies and procedures, and monitor compliance with: recordkeeping requirements of 31 CFR 1000; exemption procedures; Customer Identification Programs; and Office of Foreign Assets Control (OFAC) requirements. Most importantly, this engagement evaluates the institution's ability to detect reportable currency transactions and suspicious activity. Further we have been approved by the FDIC as a qualified independent third party for mandated Look Back reviews.

VALIDATION AND OPTIMIZATION SERVICES FOR BSA TRANSACTION MONITORING SYSTEMS – Automated transaction monitoring is essential to manage money laundering and terrorist financing risks. Institutions using these systems must ensure they are reliable and appropriately controlled and monitored. As cited in the FFIEC BSA/AML Manual, independent validation of an automated monitoring system's programming methodology and effectiveness is a regulatory expectation. ProBank can evaluate the validity and reliability of your institution's monitoring system as well as the personnel tasked with such oversight. Our experience with rule-based and intelligent systems allows our reviews to adapt to your risk profile. Our professionals validate data mapping and extraction processes, as well as test the system's programming processes to ensure parameters and filtering criteria encompass key BSA/AML risks and that data output is reliable. Not only is this a regulatory expectation, it is the institutions primary defense against a Look Back situation occurring.

POLICIES AND PROCEDURES – Regulatory agencies expect institutions to develop comprehensive compliance programs which include written policies. We evaluate existing policies and, if needed, offer recommendations and assistance in preparing compliance policy manuals. Our process is specifically designed to assure your policy manuals are living documents, easily updated.

NON-DISCRIMINATION ANALYSIS – We conduct engagements designed to evaluate an institution's fair lending procedures. We review policies and interview personnel to identify potential discriminatory treatment or "Effects Tests" concerns. We then conduct "side-by-side" comparative file analysis, following interagency examination guidelines, focusing either on underwriting or terms and conditions. At the conclusion of these engagements, we offer recommendations and solutions designed to strengthen the institution's fair lending program. When asset size or risk factors dictate, we are able to add a data driven phase as well.

RESPONSES TO ENFORCEMENT ACTIONS – A financial institution's response must be immediate and appropriate when regulatory criticisms reach the level of a formal enforcement action. Our experience in working with clients in such circumstances assures effective allocation of time and resources to respond to regulatory agreements. Allow us to help alleviate the stress of such situations.

RESTITUTION – Truth-in-Lending disclosures, RESPA tolerance exceptions, or adjustable rate mortgage servicing errors can create reimbursable violations. Our professionals are experienced in overseeing reimbursement efforts with the joint purposes of complying with regulatory requirements while minimizing the cost to the institution.

PROBANK PERSONNEL – Our professionals possess a variety of banking, legal, regulatory, and training backgrounds. They have two common traits: excellent knowledge of regulatory requirements and a comprehensive understanding of the financial industry. This combination yields practical advice our clients can use to manage their compliance functions.

We can provide the compliance expertise you need. If you would like to discuss these or our many other services, please contact Martin (Marty) Mitchell at 800/523-4778, extension 258, complete the "contact us" form online at www.probank.com or complete the information card on the reverse side of this page and fax or mail it to ProBank Austin.

COMPLIANCE CONSULTING SERVICES



ProBank Austin

We appreciate your interest in our company and its services. If you would like additional information, please complete the following and fax, mail, or email it to us at the appropriate number or address listed below, or complete the "contact us" form online at www.probank.com.

ProBank Austin
ATTN: Martin (Marty) Mitchell, CRCM
950 Breckenridge Lane, Suite 280, Louisville, Kentucky 40207
800/523-4778, Ext. 258 (Phone) | 502/451-6755 (Fax)
www.probank.com | mmitchell@probank.com

I would like information on the following:

- | | |
|--|---|
| <input type="checkbox"/> Inhouse Training | <input type="checkbox"/> Policies and Procedures Development |
| <input type="checkbox"/> ProBank Advisor | <input type="checkbox"/> Fair Lending/Non-Discrimination Analysis |
| <input type="checkbox"/> BankED | <input type="checkbox"/> Community Reinvestment Act Evaluations |
| <input type="checkbox"/> Regulatory Compliance Reviews | <input type="checkbox"/> Enforcement Actions/Restitution |
| <input type="checkbox"/> Independent BSA/AML Evaluations | <input type="checkbox"/> Information Security Audits |
| <input type="checkbox"/> Validation Services BSA Transaction
Monitoring Systems | <input type="checkbox"/> ACH Self Audits |
| | <input type="checkbox"/> Other _____ |

Name

Title

Institution

Address

City

State

Zip

Phone Number

Fax Number

Email

The best time to contact



**ProBank
Austin**

**ProBank
Advisor** Trusted.
Compliance.
Advice.

Trusted guidance and smart advice. At your fingertips.

1.833.PROADVS | WWW.PROBANKADVISOR.COM

Powered by one of the financial industry's preeminent consulting, education, and investment banking firms, ProBank Advisor is an online advisory service helping financial industry professionals navigate U.S. federal regulatory compliance requirements.

Our Advisors are experts with decades of experience and real-world knowledge gained from answering countless compliance questions on Lending, Deposits, Bank Secrecy Act (BSA), Anti-Money Laundering (AML), Compliance Risk Management, and more.

Participate in the forum, check out the latest compliance topics and trends, or submit a policy for review. It's all possible through ProBank Advisor.



**ProBank
Austin**



Online Compliance Training. Anytime. Anywhere.

1.844.4BANKED | www.bankEDonline.com | info@probank.com

bankED is a comprehensive online video training platform, developed by industry experts, that provides the ideal way for financial industry professionals to keep informed of ever-evolving compliance rules and regulations. Affordable and easy-to-use, bankED provides financial industry professionals a user-friendly program to satisfy annual regulatory and policy-driven requirements at their own pace and in a way that you learn best. The best part is you learn it when it's convenient for you.

Whether a C-Suite Executive, Compliance Officer, Auditor, or Loan officer, all employees can benefit from bankED's full comprehensive course selection. bankED is also an excellent tool for acquainting new hires with initial training objectives. bankED is powered by the Education Division of ProBank Austin, the financial industry's preeminent consulting, education, and investment banking firm.



ProBank Austin

PUBLICATIONS

Newsletters & Manuals



Our Education Division offers a wide variety of publications ranging from a quarterly newsletter to a growing list of in-depth manuals on specific topics. Our newsletter, *InCompliance*, keeps you informed of the latest regulatory pronouncements and current issues, and provides helpful compliance and management tips.

We also publish manuals that are comprehensive, reliable reference guides on topics that are crucial for financial service institutions. Our manuals are written by ProBank Austin experts who use “plain English” to educate readers. Manuals are written to complement our educational seminars and are updated routinely to address all aspects of a particular topic including related laws and regulations.

Newsletter

[InCompliance – Quarterly Newsletter](#)

[InCompliance Special Edition: COVID-19: Regulatory Impacts & Compliance Requirements](#)

Quick Compliance Guides

[2020 Annual Threshold Quick Compliance Guide](#)

[Adverse Action Notices Quick Compliance Guides](#)

[Advertising Quick Compliance Guide](#)

[Human Smuggling and Human Trafficking Quick Compliance Guide](#)

[TRID Quick Compliance Guide](#)

Manuals

[ACH Processing and Compliance](#)

[Advanced TRID](#)

[Anti-Money Laundering & BSA Compliance School](#)

[Anti-Money Laundering and Bank Secrecy Act Compliance](#)

[Compliance for Commercial Loans](#)

Manuals, Continued

[Compliance Risk Management Program](#)

[Deposit Documentation](#)

[Fair Lending: Detect, Monitor & Exam](#)

[How To Ensure Compliance with Deposit Regulations](#)

[Introduction to Lending Compliance](#)

[IRA Administration](#)

[IRA Basics](#)

[Kentucky Account Administration Workshop](#)

[Lending Compliance 101](#)

[Mastering HMDA](#)

[Mortgage Lending – Start to Finish](#)

[Privacy, Security and Fraud: How to Protect Your Customer](#)

[Real Estate Lending Compliance](#)

[Social Media Boot Camp](#)

[TRID Fundamentals with Workshop](#)

[Truth-in-Lending/Regulation Z: In Depth](#)

[UDAP/UDAAP: What It Is and How to Spot It](#)

For more information and pricing on our publications:

- Visit us online at www.probank.com
- Contact us at 800-523-4778, Option 1
- Email us at registrar@probank.com

Faculty

Mark Dever, AAP, CAMS is a Vice President and Senior Consultant at ProBank Austin. Prior to joining the firm in 1996, Mr. Dever was Vice President and Manager of cash management operations for a multi-billion dollar regional bank holding company with several affiliates. He has extensive experience in many areas including the automated clearing house (ACH), domestic wire transfer, affiliate bank post-acquisition conversions and consolidations, bank operation centralizations, and payment system risk. He teaches a variety of ProBank Austin seminars including the ACH Processing and Compliance, and the Anti-Money Laundering and Bank Secrecy Act seminars. He has lectured at regional and national seminars, and at graduate schools of banking hosted by various bank associations and national industry groups. He has served on the faculty of both the OTS' Compliance I School, and the FDIC's Advanced Consumer Protection School. He has also taught undergraduate business and management classes in a community college setting. Mr. Dever is an Accredited Automated Clearing House Professional (AAP), and a Certified Anti-Money Laundering Specialist (CAMS).



[illegible]

[illegible]

[illegible]

**2021 BANK SECRECY ACT
TWO-DAY SCHOOL**

**2021 BANK SECRECY ACT
TWO-DAY SCHOOL**

Table of Contents, *Continued*

BACKGROUND AND OVERVIEW.....	1-1
I. Introduction	1-1
II. Background of BSA/AML.....	1-2
III. Definitions	1-7
IV. Coverage.....	1-8
V. Enforcement	1-8
VI. Compliance Resources	1-11
Exhibit 1-A - Federal and Other Guidance	1-15
Exhibit 1-B.....	1-17
Bank Secrecy Act/Anti-Money Laundering Questions	1-88
 CUSTOMER DUE DILIGENCE (CDD)/ENHANCED DUE DILIGENCE (EDD)	2-1
I. CDD Program	2-1
II. Identifying Suspicious Transactions.....	2-15
III. Money Services Businesses (MSB).....	2-16
Federally Defined Categories High-Risk Clients and Entities	2-25
High-Risk Categories/Factors	2-27
High-Risk Analysis Factors – Bank Secrecy Act Retail/Consumer Clients.....	2-28
High-Risk Analysis Factors – Bank Secrecy Act Business/Commercial Clients	2-29
Risk Assessment Format.....	2-30
FIN-2016-ROO3, September 7, 2018.....	2-32
Examination Procedures – Beneficial Ownership	2-45
Customer Due Diligence – Overview	2-49
Customer Due Diligence – Examination Procedures	2-56
FIN-2020-G002, August 3, 2020	2-58
Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons, August 21, 2020	2-61
Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations, November 19, 2020.....	2-65
Appendix F: Money Laundering and Terrorist Financing “Red Flags”	2-69
 SUSPICIOUS ACTIVITY REPORTING	3-1
I. Introduction	3-1
II. Reportable Transactions	3-2
III. The Suspicious Activity Report (SAR)	3-4
IV. Safe Harbor	3-11
The Suspicious Activity Report (SAR) – FinCEN 111	3-12
V. Limits on Disclosing SAR Information	3-19
VI. Other FinCEN SAR Guidance	3-21
VII. Internal Procedures	3-34
VIII. Exam Procedures	3-35
Appendix S: Key Suspicious Activity Monitoring Components.....	3-37
Exhibit 3A	3-49
 EXAMINATION PROCEDURES	4-1
I. Introduction	4-1
II. Risk Assessment.....	4-2
III. Compliance Program Structures	4-3
IV. Automated Clearinghouse.....	4-5
V. Initial Observations/Lessons Learned	4-7

**2021 BANK SECRECY ACT
TWO-DAY SCHOOL**

Table of Contents, *Continued*

RISK ASSESSMENT.....	5-1
I. Risk Assessment.....	5-1
Federally Defined Categories – High-Risk Products and Services	5-5
Federally Defined Categories – High-Risk Geographies	5-11
Quantity of Risk Matrix – BSA/AML DFI Identified (Appendix J -Modified)	5-15
Quantity of Risk Matrix – OFAC DFI Identified (Appendix M and Matrix B - Modified).....	5-20
Developing an Institutional Risk Assessment Program	5-27
 CURRENCY TRANSACTION REPORTING.....	 6-1
I. Reportable Transactions	6-1
II. Filing Requirements	6-3
Currency Transaction Report (CTR) -FinCEN 112.....	6-4
III. Exemptions	6-19
The New Designation of Exempt Person Form	6-28
Currency Transaction Reporting Questions.....	6-57
Exemption Questions.....	6-65
 OFFICE OF FOREIGN ASSETS CONTROL	 7-1
I. Introduction and Overview	7-1
II. A Framework for OFAC Compliance Commitments.....	7-5
OFAC Questions	7-35
 CUSTOMER IDENTIFICATION PROCEDURES.....	 8-1
I. General Requirements	8-1
II. Definitions	8-2
III. Program Requirements	8-3
FOREIGN CORRESPONDENT AND PRIVATE BANKING ACCOUNTS.....	8-11
I. Overview.....	8-11
II. Foreign Correspondent Accounts	8-11
III. Private Banking Accounts	8-12
IV. Beneficial Ownership	8-14
314(a) INFORMATION REQUESTS.....	8-15
I. Overview.....	8-15
II. Requirements	8-15
III. Sharing Information with Other Financial Institutions	8-18
ANTI-MONEY LAUNDERING PROGRAM FOR INSURANCE COMPANIES REQUIREMENTS AND THAT INSURANCE COMPANIES REPORT SUSPICIOUS TRANSACTIONS	8-20
I. General Requirements	8-20
II. Definitions	8-20
III. Impacts on Banks, Savings and Loans, and Credit Unions	8-21
IV. Final Rules	8-21
V. "Red Flags"	8-21
VI. Examination Procedures	8-22
USA PATRIOT ACT/Title III Questions.....	8-34
 RECORDKEEPING REQUIREMENTS	 9-1
I. Introduction	9-1
II. Records Required to be Maintained.....	9-1
III. Recordkeeping for Funds Transfers and Transmittals of Funds by Banks.....	9-5

BACKGROUND AND OVERVIEW OF BANK SECRECY ACT AND ANTI-MONEY LAUNDERING

I. INTRODUCTION

- A. Purpose** - Financial institutions collect significant amounts of information in connection with the transactions conducted on behalf of their customers. While the vast majority of these transactions are legal, financial institutions are sometimes unwittingly used in connection with illegal activity. In those instances, information collected by those institutions can be of significant value to law enforcement.

The Bank Secrecy Act (“BSA”) and related laws and regulations require financial institutions take reasonable steps to verify the identity of their customers, monitor and report certain currency, suspicious and foreign transactions, and maintain specific records. These steps:

1. require financial institutions to keep records that will provide a “paper trail” that law enforcement can utilize; and
2. provide penalties for individuals and entities attempting to avoid those requirements.

- B. Records** - Records originated in the ordinary course of business are required to be kept as either originals or copies (copies would include photocopies, microfilm or microfiche, computer stored images, etc.). However, records must be able to be retrieved and reproduced within a reasonable period of time. Provisions of the USA PATRIOT Act require institutions to present records:

- Within 120 hours if the request is from the financial institution’s principal federal regulator and involves anti-money laundering or terrorist activities; and
- Within seven days if law enforcement issues a written request for information on foreign correspondent bank accounts.

All records required to be maintained under the BSA must be retained for a period of five years.

- C. Report Submission – BSA E-Filing** – Reports required to be submitted under the BSA must be filed electronically (77FR12367-12370, 02/29/12) using the highly secure network known as the *BSA E-Filing System*, which allows financial institutions to quickly and securely file BSA reports over the Internet. FinCEN Guidance 2013-G002 (06/24/13) indicated that FinCEN recognizes that financial institutions may, on limited occasions, have administrative difficulties in submitting BSA reports electronically within the required timeframes. This could be due to circumstances such as natural disasters, emergency situations, or other systemic issues. Financial institutions affected by such should contact FinCEN’s Regulatory Help Line, (800) 949-2732 to make FinCEN aware of the compliance concerns and to determine possible alternatives for timely BSA reporting.

The *BSA E-Filing System* supports:

1. Discrete, or single-report Filing – a solution for smaller institutions or those that only file small numbers of BSA reports;
2. Batch Report Filing – a solution for medium-size or larger institutions or those that consistently file larger numbers of reports; or
3. System-to-System Filing (Secure Data Transfer Mode) – a batch filing solution for the largest filers.

The *BSA E-Filing System* “help desk” can be reached at (866) 346-9478 or by completing the “BSA E-Filing Technical Support Request Form” available at the BSA E-Filing System home page.

II. BACKGROUND OF BSA/AML - Over the past forty plus years, Congress has passed several laws which have impacted a financial institution's responsibilities related to BSA. With each new law, the institution became more accountable to identify and understand the nature of its customers, and to scrutinize activity which might be illegal, or at a minimum, would appear abnormal or suspicious. In today's regulatory environment, increased emphasis is placed on efforts to prevent money laundering; therefore, references to BSA/AML (Anti-Money Laundering) should be considered one topic for this manual.

A. 1970 - Financial Recordkeeping and Currency and Foreign Transaction Reporting Act - CTRs - The first Act requiring institutions to maintain records and to file reports when transactions involving currency in excess of \$10,000 occurred.

B. 1986 - Money Laundering Control Act (BSA) - This Act made money laundering a crime and required institutions to formalize their efforts by establishing minimum components of a BSA program which include:

1. A system of internal controls to assure ongoing compliance - The interagency BSA/AML Examination Manual indicates an expanded focus on internal controls. Items that should be considered and tailored to the specific financial institution's risk profile include:
 - a. Identify operations (products, services, clients, entities, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the institution's risk profile; and provide for a BSA/AML program tailored to manage risks;
 - b. Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective actions taken, and notify directors and senior management of SARs filed;
 - c. Identify a person or persons responsible for BSA/AML compliance;
 - d. Provide for program continuity despite changes in management or employee composition of structure;

- e. Meet all regulatory recordkeeping and reporting requirements. Meet recommendations for BSA/AML compliance, and provide timely updates in response to changes in regulations;
- f. Implement risk-based client due diligence (CDD) policies, procedures, and processes;
- g. Identify reportable transactions and accurately file all required reports including SARs, CTRs, and CTR Exemptions. (Financial institutions should consider centralizing the review and report filing functions within the banking organization);
- h. Provide sufficient controls and systems for filing CTRs and CTR exemptions.
- i. Provide for dual control and segregation of duties to the extent possible. For example, employees that complete reporting forms (such as SARs and CTRs) should not also be responsible for the decision to file the report or grant the exemptions.
- j. Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity; and
- k. Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations; and
- l. Incorporate BSA compliance into the job descriptions and performance evaluations of appropriate personnel.
- m. Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines.

The “Overview” section of the BSA/AML Examination Manual provides additional guidance and recommendations as to an “appropriate” system of internal controls.

- 2. Independent Testing – conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. Depending upon the federal examination agency, a sound practice is for the institution to conduct independent testing generally every 12 months. The persons conducting the testing should report directly to the board or a designated board committee comprised primarily or completely of outside directors. The audit should be risk based and evaluate the quality of risk management for all of the institution’s operations, departments, and subsidiaries. The “Overview” section of the BSA/AML Examination Manual provides additional information and the minimum inclusions expected by the federal examiners.
- 3. Designation of qualified individual or individuals responsible for compliance – an officer responsible for the day-to-day BSA/AML compliance of the institution, and who is charged with managing all aspects of the BSA/AML program. While the title of the individual responsible for overall BSA/AML compliance is not important, his or her

level of authority and responsibility within the institution is critical. The BSA compliance officer may delegate BSA/AML duties to others, but that officer is responsible for overall BSA compliance. The individual(s) selected should be fully knowledgeable of the BSA and all related regulations, and should fully understand the institution's products, services, clients, entities, and geographies, and the potential money laundering and terrorist financing risks associated with such activities. The appointment of a BSA officer who does not have the expertise, authority, or the time to satisfactorily complete the job will not meet the regulatory requirements of the BSA. The "Overview" section of the BSA/AML Examination Manual provides additional information on a "qualified" BSA officer.

4. Training – all appropriate personnel are trained in all aspects of the BSA. The training should include regulatory requirements, and the institution's internal BSA/AML policies, procedures, and processes. The training should be tailored to the person's specific responsibilities. Through their training, the board of directors should understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the institution. The board should also be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. The "Overview" section of the BSA/AML Examination Manual provides additional guidance as to "appropriate" training.
 5. Appropriate risk-based procedures to conduct ongoing Customer Due Diligence, to include, but not be limited to:
 - a. Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
 - b. Conducting ongoing monitoring to identify and report suspicious transactions, and on a risk basis, to maintain and update customer information including information regarding beneficial owners of legal entity customers.
- C. 1988 - Anti-Drug Abuse Act - Civil Asset Forfeiture** -This law effectively gave the federal government the right to seize assets of those convicted of certain illegal activities. As a result of this Act, financial institutions are placed in a position of having a "vested" interest in how the customer uses the bank's collateral.
- D. 1990 - Financial Crimes Enforcement Network (FinCEN) Created**
- E. 1992 - Annunzio-Wylie Act** - This law specified recordkeeping requirements for certain types of funds transfers and provided financial institutions a "safe harbor" protection when filing Suspicious Activity Reports.
- F. 1994 - Money Laundering Suppression Act** - This law introduced the concept of "Know Your Customer," established what were then new guidelines for granting exemptions from filing currency transaction reports, and increased awareness of the Office of Foreign Assets Control.
- G. 1998 - Money Laundering and Financial Crimes Strategy Act** - This Act tasked the Department of Treasury to develop a national strategy to combat money laundering and related financial crimes, which includes detection and prosecution

initiatives including seizure and forfeiture of proceeds derived from such crimes. The strategy impacts the industry as indicated:

1. Department of Treasury and Department of Justice provide the industry with “guidance” on enhancing bank scrutiny of certain transactions or patterns of transactions in high-risk accounts.
2. Regulatory agencies continue to identify and implement enhancements to examination procedures where necessary to address the ever-changing nature of money laundering. The regulators will also continue to place greater focus on BSA compliance and respond more frequently with enforcement and other regulatory actions. Lessons learned from the recent enforcement actions include:
 - a. Develop a process to assess, identify, and assign risk to clients, entities, products, services, and geographies that identifies and addresses gaps in the management of BSA risks;
 - b. Conduct an annual “risk-assessment” of the client base to identify categories of high-risk clients;
 - c. Identify high-risk clients at account opening, and apply appropriate on-going monitoring to the new “high-risk” clients;
 - d. Identify and “risk manage” clients involved in funds transfer activity, especially funds transfers to or from “jurisdictions of primary concern” identified by the State Department or FATF;
 - e. Identify and “risk-manage” all politically exposed persons (PEPs);
 - f. Identify and “risk-manage” all money services businesses (MSBs) by applying the FinCEN guidance from 04/26/05;
 - g. Provide adequate Board and management oversight. Board members may be held personally liable;
 - h. Provide an adequate and requisite level of staffing in the BSA compliance area(s);
 - i. Provide “above adequate” testing by having audit render an opinion on the overall adequacy of the AML program. Audit should also comment on the institution’s ability to detect, monitor, and report suspicious activity;
 - j. Heed the advice of your “independent” auditor when such advice is provided;
 - k. Provide institution wide “above adequate” training, tailored to the specific LOBs and containing the appropriate materials;
 - l. Do not forget the basics of BSA, as basic CTR reporting and overall recordkeeping and reporting remain critical pieces in the total success of a BSA compliance program;

- m. Provide adequate monitoring systems and resist the temptation to “cap” number of “suspicious alerts” to accommodate the number of available compliance personnel;
- n. There is no “too small to err” scenario in BSA examinations;
- o. Correct previously identified errors, omissions, and deficiencies;
- p. Do not introduce or continue to offer higher risk products and services without the proper due diligence, risk assessment analysis, nor proper controls to minimize and mitigate the risks;
- q. Refrain from conspiring to violate BSA by ignoring the law or related regulations;
- r. Consider enforcement action results in acquisition discussions;
- s. Consider rejecting inbound international wire transfers that do not contain the required “Travel Rule” information and report such using SAR (not a mandate);
- t. Search for all types of crimes and inconsistencies not just money laundering and terrorist financing, and do not knowingly facilitate a ponzi scheme;
- u. Consider adding BSA and OFAC compliance into the performance evaluations for senior and line of business management; and
- v. Review deposited items from check-cashing MSBs to identify and report suspicious transactions (e.g., tax-refund fraud, healthcare fraud, etal).

NOTE: See FinCEN Advisory 2014-A007 on promoting a culture of compliance.

H. 2001 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) -

Among other things, this law increases the fight against terrorism and illegal activities by expanding the types of business entities classified as a financial institution, requires financial institutions to adopt specific procedures to identify customers, and expedites the flow of information between law enforcement and the financial industry.

I. 2020 -- National Defense Authorization Act (NDAA) – This act, which includes **the Anti-Money Laundering Act of 2020 (AMLA 2020) and the Corporate Transparency Act of 2020**, among other things, establishes uniform beneficial ownership requirements, modernizes anti-money laundering (AML) and countering the financing of terrorism (CFT) laws to adapt the government and private sector response to new and emerging threats, reinforces that AML policies, procedures, and processes shall be risk-based, encourages technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and the financing of terrorism, and improves coordination and information sharing among the parties tasked with administering and complying with the various AML and CFT requirements.

III. DEFINITIONS

A. Definitions

1. Bank – For BSA purposes, a “bank” includes:
 - a. An insured bank (as defined in the Federal Deposit Insurance Act);
 - b. A commercial bank and trust company;
 - c. A private bank;
 - d. A thrift institution;
 - e. Any credit union; and
 - f. An agency or branch of a foreign bank.
2. Currency Transaction Report (CTR) – The FinCEN form to be completed when certain currency transactions exceeding \$10,000 occur on any given business day.
3. Financial Crimes Enforcement Network (FinCEN) – A bureau within the U.S. Treasury Department that manages the network that works with financial institutions, law enforcement agencies and financial regulators to help fight a wide variety of domestic and international financial crimes, including money laundering.
4. Money Laundering - Criminal finance. It can include disguising the source or ownership of illegally gained funds to make them appear legitimate; hiding lawfully acquired money to evade taxation; or using legally gained money in the pursuit of illegal activities (e.g., terrorism)- “Reverse Money Laundering.”

A person who conducts a financial transaction “with knowledge” that the funds or property involved are the proceeds of crime, and who intends to further that crime, or to conceal or disguise those proceeds, is laundering money. Laundering typically involves three independent stages that may occur separately or simultaneously:

- a. **Placement** - Physically placing bulk cash into the banking system or legitimate commerce;

Example: Cash in amounts of less than \$10,000 is deposited into a deposit account with check writing or wire transfer capability.

Example: Cash in amounts of less than \$3,000 is used to purchase money orders, cashiers checks, or traveler’s checks.

Example: Cash is shipped in large quantities outside the U.S. and the funds are wired back to a U.S. bank account.

- b. **Layering** - Separating the source of cash from its criminal origins by passing it through several financial transactions;

Example: Cash is deposited into an account. Funds from the account are used to purchase a certificate of deposit. The certificate is then used as collateral for loan.

- c. **Integration** - Aggregating the funds or cash with legitimately obtained funds and providing a legitimate explanation for its ownership.

Example: Cash is deposited into an account for a legitimate business and commingled with the cash receipts of the business. The business enterprise requires significant volume to justify the amount of cash going into the account.

- 5. Mutual Funds – Effective May 14, 2010, Mutual Funds are considered “financial institutions” for BSA purposes, and must begin filing FinCEN Form 104 (CTR) to report transactions in currency greater than \$10,000. With this change, effective January 10, 2011, Mutual Funds have to comply with the funds transfer recordkeeping requirements found within the BSA. (75FR19241-19245, 4/14/2010).
- 6. Non-Bank Residential Mortgage Lenders and Originators – Effective April 16, 2012, non-bank residential mortgage lenders and originators (RMLO) are defined as loan or finance companies for purposes of the Bank Secrecy Act (BSA). As such, they are required to establish anti-money laundering programs, and report both suspicious activities and large currency transactions, as well as participate in the recordkeeping and information sharing requirements applied to loan or finance companies under the BSA. (The compliance date for 31 CFR 1029.210 is 08/13/2012 – (77 FR 8148 – 8160, 02/14/12)).

IV. COVERAGE – Although many of the provisions of the Bank Secrecy Act and related statutes and regulations apply to a variety of financial institutions, this manual primarily focuses on the duties of “banks” as previously defined.

V. ENFORCEMENT - The Department of the Treasury issues the regulations interpreting the substantive provisions of the Bank Secrecy Act. The financial regulatory agencies are required to develop their own regulations regarding BSA compliance programs for the institutions they supervise. An institution's failure to comply with these regulations, knowing or inadvertent involvement in money laundering, and/or the absence of an effective BSA compliance program reflects poorly on the bank's management and can result in the bank receiving one of the following enforcement actions:

- A. Civil Money Penalties (CMP)** - Treasury has traditionally had the power to assess civil money penalties for violations of Treasury regulations, but Congress has conferred the same power to the financial regulatory agencies. The penalty structure is intended to be prohibitive, not just punitive:

TABLE 1 OF § 1010.821—PENALTY ADJUSTMENT TABLE			
U.S. Code citation	Civil monetary penalty description	Penalties as last amended by statute	Maximum penalty amounts or range of minimum and maximum penalty amounts for penalties assessed on or after [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]
12 U.S.C. 1829b(j)	Relating to Recordkeeping Violations For Funds Transfers	\$10,000	\$21,663
12 U.S.C. 1955	Willful or Grossly Negligent Recordkeeping Violations	10,000	21,663
31 U.S.C. 5318(k)(3)(C)	Failure to Terminate Correspondent Relationship with Foreign Bank.	10,000	14,653
31 U.S.C. 5321(a)(1)	General Civil Penalty Provision for Willful Violations of Bank Secrecy Act Requirements.	25,000–100,000	59,017–236,071
31 U.S.C. 5321(a)(5)(B)(i)	Foreign Financial Agency Transaction—Non-Willful Violation of Transaction.	10,000	13,640
31 U.S.C. 5321(a)(5)(C)(i)(I)	Foreign Financial Agency Transaction—Willful Violation of Transaction.	100,000	136,399
31 U.S.C. 5321(a)(6)(A)	Negligent Violation by Financial Institution or Non-Financial Trade or Business.	500	1,180
31 U.S.C. 5321(a)(6)(B)	Pattern of Negligent Activity by Financial Institution or Non-Financial Trade or Business.	50,000	91,816
31 U.S.C. 5321(a)(7)	Violation of Certain Due Diligence Requirements, Prohibition on Correspondent Accounts for Shell Banks, and Special Measures.	1,000,000	1,465,309
31 U.S.C. 5330(e)	Civil Penalty for Failure to Register as Money Transmitting Business.	5,000	8,708

* **Effective 01/28/21**

B. Enforcement Actions - The financial regulatory agencies also have the power to begin a variety of enforcement actions (both informal and formal) under the Federal Deposit Insurance Act (FDI Act) and the Federal Credit Union Act (FCUA), some of which would be appropriate for serious BSA violations:

1. Power to issue a Cease and Desist action;
2. Power to issue a temporary Cease and Desist action;
3. Power to suspend or remove a bank officer or director;
4. Power to prohibit participation in bank affairs; and
5. Civil money penalties.

On August 18, 2020, FinCEN issued a “*Statement on Enforcement of the Bank Secrecy Act*” describing FinCEN’s approach to enforcing the Bank Secrecy Act (BSA) and the factors it will use to determine the appropriate enforcement response when it identifies actual or possible violations of the BSA. When FinCEN takes an enforcement action, it will seek to establish a violation of law based on the applicable statutes and regulations. FinCEN will not treat noncompliance with a standard of conduct announced solely in a guidance document as itself a violation of law. FinCEN has the authority to take the following enforcement actions when it identifies an actual or possible violation of the BSA or any BSA regulation or order: No Action; Warning Letter; Equitable Remedies (injunctions or equitable relief); Settlements; Civil Money Penalties; and/or Criminal Referral. In all matters, FinCEN will consider the need to impose compliance commitments deemed necessary and appropriate to ensure that financial institutions are fully complying with their BSA obligations. FinCEN considers a range of factors when evaluating an appropriate disposition upon identifying actual or possible violations of the BSA. FinCEN considers both compliance with specific BSA

requirements as well as the adequacy of an anti-money laundering (AML) program. The statement is available at: <https://www.fincen.gov/news/news-releases/fincen-statement-enforcement-bank-secrecy-act>.

- C. Compliance Program Violations** - The financial regulatory agencies can also use their powers under the FDI Act (discussed above) to compel compliance with other agency regulations.
- D. BSA Criminal Penalties** - The Department of Justice is responsible for criminal prosecutions. Willful violations of BSA are also punishable as crimes. Conviction for a willful BSA violation can generate:
 - 1. Fines of up to \$250,000; and/or
 - 2. Prison sentences up to 5 years.
- E. Money Laundering Criminal Penalties** - The Department of Justice prosecutes violations of anti-money laundering statutes. Conviction for violation of anti-money laundering statutes can generate:
 - 1. fines of up to \$500,000;
 - 2. prison sentences up to 20 years;
 - 3. appointment of a conservator to oversee operations;
 - 4. revocation of its banking license; and
 - 5. termination of FDIC insurance pursuant to Sec. 8(w) of the FDI Act.
- F. USA PATRIOT Act Penalties** - The USA PATRIOT Act amended BSA to authorize Treasury to impose penalties that range from \$1 million up to \$1.423 million for violations of the restrictions on accounts with Shell Banks and/or for violations of the due diligence requirements for private banking and correspondent banking accounts maintained for “Non U.S. persons.”
- G. Anti-Money Laundering Act (AMLA) Penalties** – The Anti-Money Laundering Act of 2020 amended the BSA by authorizing additional fines and penalties including:
 - 1. Repeat Violations - Additional damages for repeat violations up to three times the profit gained, or loss avoided, or if not calculable, two times the maximum penalty with respect to the violation (Sec. 6309);
 - 2. Egregious Violations - Persons found to have committed an egregious violation of the BSA shall be barred from serving on the board of directors of a United States financial institution during the 10-year period that begins on the date on which the conviction or judgement with respect to the egregious violation is entered (Sec. 6310) (An egregious violation is defined as either a criminal violation for which the individual is convicted and for which the term of imprisonment is more than one year, or a civil violation in which the individual willfully committed the violation and the violation facilitated money laundering or the financing of terrorism (Sec. 6309));

3. Return of Profits or Bonuses – Persons convicted of violating a provision of the BSA shall be fined in an amount equal to the profit gained by such person by reason of the violation, and if the person is a partner, director, or officer of a financial institution at the time the violation occurred, repay to the financial institution any bonus paid to the individual during the calendar year in which the violation occurred or the calendar year after which the violation occurred (Sec. 6312); and
4. Whistleblower Incentives/rewards and protections – AMLA modified the BSA to indicate that the Secretary (of Treasury) shall pay an award to those persons (with certain exclusions for regulatory and law enforcement persons) to those who provide original information leading to the successful enforcement of various money laundering laws, equal to 30% of the government's collection if the monetary sanctions imposed exceeded \$ 1 Million. AMLA also strengthened the whistleblower protection provisions prohibiting employers from engaging in retaliatory acts, such as discharging, demoting, threatening, or harassing employees who provide information relating to money laundering and BSA violations to the Attorney General, Secretary of Treasury, regulators, and others (Sec. 6314).

VI. COMPLIANCE RESOURCES - A large amount of information is available on BSA requirements. Much of it is included in the manuals and materials supplied to regulatory agency personnel and can be purchased at little or no cost. The following are also useful sources of information:

NOTE: The authors strongly encourage the institution to have, at a minimum, copies or immediate access to the publications of its primary regulatory agency.

A. Legal Authority

1. Statute, 31 USC 5311 et seq.
2. Treasury Regulations, 31 CFR 1000 et seq.

NOTE: On March 01, 2011, FinCEN's simplified Rules and Regulations took effect, and are found at 31 CFR 1000 et seq. Information on the new regulatory "structure" can be found at www.fincen.gov/statutes_regs/ChapterX/. (DFIs should ensure all policies, procedures, and other BSA documents are updated).

3. Treasury Administrative Rulings
4. Treasury Official Commentary (pending)
5. Financial Regulatory Agency Program Regulations
 - a. FDIC regulations, 12 CFR 326.8
 - b. Federal Reserve regulations, 12 CFR 208.63
 - c. NCUA regulations, 12 CFR 748.2
 - d. OCC regulations, 12 CFR 21.21

- e. OTS regulations, 12 CFR 563.177
- 6. FDI Act Section 8(s) and 12 USC 1818(s)

B. Regulatory Agency/Federal Government Communications/Other Sites

- 1. Federal Deposit Insurance Corporation (FDIC)
 - a. www.fdic.gov
 - b. Financial Institution Letters (FIL)
- 2. Federal Reserve Bank (FRB)
 - a. www.federalreserve.gov
 - b. www.frb.services.org
 - c. Supervision and Regulation Letters (SR)
 - d. Press Releases/Enforcement Actions
- 3. Comptroller of the Currency (OCC)
 - a. www.occ.treas.gov
 - b. Advisory Letters (AL)
 - c. Bulletins
 - d. Alerts
- 4. National Credit Union Administration (NCUA)
 - a. www.ncua.gov
 - b. Letters to Credit Unions
- 5. National Information Center
 - a. www.ffiec.gov/nicpubweb/content/help/HelpBranchLocatorSearch.htm
 - b. Location of Branch RSSD Numbers
- 6. Financial Crimes Enforcement Network (FinCEN)
 - a. www.fincen.gov
 - b. FinCEN Regulatory Help Line – 800-949-2732
 - c. SAR Hotline Relating to Terrorist Activity – 866-556-3974
 - d. BSA E-Filing Help Desk – 866-346-9478

- e. Forms and Publications
 - f. *SAR Activity Review and SAR STATS*
 - g. HIFCA Designations and Explanations
 - h. MSB Compliance Information (04/20/09)
7. Office of Foreign Asset Control
- a. <http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>
 - b. Specially Designated Nationals (SDNs)
 - c. SDN Information - 800-540-6322
 - d. “In-Process” Wire Hotline
www.treasury.gov/about/organizational-structure/offices/Terrorism-Fin-Intel/Pages/OfficeOfForeignAssetsControlHotline.aspx
8. Federal Trade Commission (FTC)
- a. www.ftc.gov
 - b. www.consumer.gov/idtheft
 - c. Consumer Privacy Protection
 - d. Identity Theft Information
9. Office of the Federal Register
- a. www.federalregister.gov
 - b. Link to the Federal Register
10. Federal Financial Institution Examination Council (FFIEC)
- a. <https://bsaaml.ffiec.gov/manual>
 - b. BSA/AML InfoBase - Exam Materials
11. Financial Action Task Force (FATF)
- a. www.fatf-gafi.org
 - b. Money Laundering Typologies Reports
 - c. Guidance on Detecting Terrorist Financing
 - d. “HRNCJ” designations

12. Wolfsberg AML Principles
 - a. www.wolfsberg-principles.com/wolfsberg_principles.html
 - b. Updated Anti-Money Laundering Principles for Private Banking.
 - c. AML Principles for Correspondent Banking
 - d. The Suppression of the Financing of Terrorism.
13. Office of National Drug Control Policy (ONDCP)
 - a. www.whitehouse.gov/ondcp
 - b. HIDTA Designations and Explanations
 - c. National Drug Control Program
14. U.S. Treasury Office of Terrorism and Financial Intelligence. (TFI)
 - a. www.treasury.gov/about/organizational-structure/offices/pages/office-of-terrorism-and-financial-intelligence.aspx
 - b. Central focal point coordinating CTF Resources.
15. Drug Enforcement Agency
 - a. www.usdoj.gov/dea/statistics.html
 - b. National Drug Threat Assessment
 - c. National Drug Intelligence Center
16. Federal Reserve Financial Services
 - a. www.frbservices.org
 - b. Information on FRB Financial Services and Products
17. Federal Reserve Payments Improvement
 - a. <https://fedpaymentsimprovement.org>
 - b. Real-Time Gross Settlement Service (RTGS) and 24 x 7 x 365 Payment Processing
 - c. FedNowSM

EXHIBIT 9-A

FEDERAL AND OTHER GUIDANCE

As part of the National Money Laundering Strategy, the regulatory agencies continue to keep the industry updated on ways to enhance financial institution scrutiny of certain transactions or patterns of transactions in potentially high-risk accounts. Below are listed some of the recent guidance documents:

- FATF (Financial Action Task Force) // Updated COVID-19 Related Money Laundering and Terrorist Financing // December 2020 // www.fatf-gafi.org
- FATF (Financial Action Task Force) // Trade-Based Money Laundering Trends and Developments // December 2020 // www.fatf-gafi.org
- U.S. Treasury // National Strategy for Combating Terrorist and Other Illicit Financing // February 2020 // <https://home.treasury.gov/news/press-releases/sm902>
- FinCEN // Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision // July 22, 2019 // <https://www.fincen.gov/news/news-releases/joint-statement-risk-focused-bank-secrecy-actanti-money-laundering-supervision>
- FATF (Financial Action Task Force) // *Terrorist Financial Risk Assessment Guidance* // July 2019 // www.fatf-gafi.org
- FinCEN // Interagency Statement Encouraging Innovative Industry Approaches to AML Compliance // December 3, 2018 // www.fincen.gov
- FinCEN // Interagency Statement on Sharing Bank Secrecy Act Resources // October 3, 2018 // www.fincen.gov
- FATF (Financial Action Task Force) // Financing of Recruitment for Terrorist Purposes // January 2018 // www.fatf-gafi.org
- FATF (Financial Action Task Force) // *Consolidated FATF Strategy on Combatting Terrorist Financing* // February 2016 // www.fatf-gafi.org
- FATF (Financial Action Task Force) // *Money Laundering Through the Physical Transportation of Cash* // October 2015 // www.fatf-gafi.org
- FATF (Financial Action Task Force) // *Combating the Abuse of Non-Profit Organizations* // June 2015 // www.fatf-gafi.org
- FATF (Financial Action Task Force) // *Guidance for a Risk-Based Approach to Virtual Currencies* // June 2015 // www.fatf-gafi.org
- FinCEN // Electronic Filing Requirements For FinCEN's Currency Transaction Report (CTR) // April 2020 // <https://sdtmut.fincen.treas.gov/main.html>
- FinCEN // Electronic Filing Requirements For FinCEN's Suspicious Activity Report (SAR) // July 2020 // <https://sdtmut.fincen.treas.gov/main.html>
- FinCEN // Electronic Filing Requirements for FinCEN's Designation of Exempt Person (DOEP) // October 2019 // <https://sdtmut.fincen.treas.gov/main.html>

EXHIBIT 1-A

The National Defense Authorization Act



On January 1, 2021, Congress enacted the FY2021 National Defense Authorization Act (NDAA), which included significant reforms to the U.S. anti-money laundering (AML) regime. The NDAA includes the Anti-Money Laundering Act of 2020 (AML Act) and, within the AML Act, the Corporate Transparency Act (CTA).

The AML Act seeks to strengthen, modernize, and streamline the existing AML regime by promoting innovation, regulatory reform, and industry engagement through forums, such as the Bank Secrecy Act Advisory Group (BSAAG) and FinCEN Exchange. The Act also calls for FinCEN to work closely with our regulatory, national security, and law enforcement partners to identify risks and priorities and provide valuable feedback to our industry partners.

The CTA establishes uniform beneficial ownership reporting requirements for corporations, limited liability companies, and other similar entities formed or registered to do business in the United States. The CTA authorizes FinCEN to collect that information and share it with authorized government authorities and financial institutions, subject to effective safeguards and controls.

Many provisions of the AML Act and the CTA require rulemaking or periodic reporting to Congress on implementation efforts, assessments, and findings. Some key requirements include:

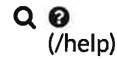
1. Establishing standards for the reporting of information on beneficial ownership, building an IT system to collect and secure the data, and creating access protocols;
2. Establishing national anti-money laundering and countering the financing of terrorism priorities;
3. Enhancing the whistleblower provisions to provide for a robust whistleblower program and new anti-retaliation protections;
4. Reviewing, and revising as appropriate, Currency Transaction Report (CTR) and Suspicious Activity Report (SAR) reporting requirements, and other existing Bank Secrecy Act (BSA) regulations and guidance;
5. Expanding BSA requirements and obligations to persons engaged in the trade of antiquities, and mandating a study on the potential expansion of BSA requirements to persons engaged in the art trade;
6. Codifying the FinCEN Exchange program;
7. Hosting a Financial Crimes Tech Symposium, and establishing new BSAAG subcommittees and a supervisory committee to address public-private partnerships;
8. Establishing a BSA Analytical Hub;
9. Law enforcement reporting to FinCEN on the use of BSA data, procedures for additional feedback between FinCEN and financial institutions on the usefulness of SARs, and semi-annual publication of review of SAR activity and other BSA reports, including threat patterns, trends, and typologies; and
10. Codifying a pilot program to allow financial institutions to share SARs with their foreign branches, subsidiaries, and affiliates.

Timely and effective NDAA implementation will be challenging and is FinCEN's top priority, and we are working diligently with our domestic and international industry partners and law enforcement and regulatory stakeholders to further the national security of the United States and protect the American people.

EXHIBIT 1-B

FFIEC BSA/AML Glossary

<https://bsaaml.ffiec.gov/references/glossary>



BSA/AML GLOSSARY

A B C D E F G H I L N O P R S T U V

#

311

The USA PATRIOT Act added 31 USC 5318A to the BSA, which authorizes the Secretary of the Treasury to require domestic financial institutions and domestic financial agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern.

314(a)

§1020.520 A federal, state, local, or foreign law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution or a group of financial institutions. Banks must conduct a one-time search of their records to identify accounts or transactions of a named suspect.

314(b)

§1020.540 A voluntary program encouraging financial institutions and associations of financial institutions located in the United States to share information in order to identify and report activities that may involve terrorist activity or money laundering.

A

ACH Operator

An ACH Operator processes all ACH transactions that flow between different depository financial institutions. There are

EXHIBIT 1-B

currently two ACH Operators: FedACH and Electronic Payments Network (EPN).

Affiliate

Any company under common control with, or controlled by, the same depository institution.

Aggregation

§1020.313 - Multiple currency transactions totaling more than \$10,000 during any one business day are treated as a single transaction if the bank has knowledge that they are by or on behalf of the same person. Transactions throughout the bank should be aggregated when determining multiple transactions.

Anti-money laundering program

§1020.210 Banks must have a written BSA/AML compliance program, approved by the board of directors, and noted in the board minutes. At a minimum, the program must include: a system of internal controls to ensure ongoing compliance, independent testing of BSA/AML compliance, a designated individual or individuals responsible for managing BSA compliance (BSA compliance officer), and training for appropriate personnel.

Automated Clearing House (ACH)

A batch-processed, value-dated, electronic funds transfer between an originating and a receiving bank with payment instructions to either credit or debit a deposit account.

B

Bankers Bank

A bank organized and chartered to do business with other banks.

Bearer Shares

An equity security wholly owned by whoever holds the physical stock certificate. The issuing firm neither registers the owner of the stock nor tracks transfers of ownership; the company disperses dividends when a physical coupon is presented to the firm.

EXHIBIT 1-B

Beneficial Owner

An individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however, without any corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner.

Blocked Transactions

U.S. law requires that assets and accounts of an OFAC-specified country, entity, or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities.

Board of Governors of the Federal Reserve System (Federal Reserve, FRB)

A federal banking agency responsible for the oversight of state member banks (SMBs); Edge and Agreement Corporations; uninsured branches, agencies, or representative offices of foreign financial institutions operating in the United States; and bank holding companies and their nonbank subsidiaries.

BSA compliance officer

A qualified individual designated by the bank's board of directors that is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the bank's adherence to the BSA and its implementing regulations.

BSA E-Filing

The system that supports electronic filing of BSA forms (CTR, SAR, DOEP, etc.), either individually or in batches, through a FinCEN secure network. BSA E-Filing provides a faster, more convenient, more secure, and more cost-effective method for submitting BSA forms.

BSA Identifier (BSA ID)

EXHIBIT 1-B

A unique, 14-character number that is assigned by BSA E-Filing to each individual report filed by a bank. The BSA ID can be used by banks to correct or amend filings and by regulators and law enforcement to search FinCEN Query.

Bulk Shipments of Currency

Sometimes referred to as wholesale cash, it entails the transportation of large volumes of U.S. or foreign bank notes. Bulk shipments of currency can be sent from sources either inside or outside the United States to a bank in the United States. Shipments are also made from a bank in the United States to a recipient in a foreign jurisdiction.

C

Cash-Intensive Businesses

Businesses that tend to deal heavily in receipts of cash, such as convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages.

Clearing House Interbank Payments System (CHIPS)

A privately operated, real-time, multilateral payments system typically used for large-dollar payments. CHIPS is owned by banks, and any banking organization with a regulated U.S. presence may become a participant in the system.

Close Associate

A person who is widely and publicly known to maintain an unusually close relationship with a senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure.

Common Control

Another company directly or indirectly or acting through one or more other persons owns, controls, or has the power to vote 25 percent or more of any class of the voting securities of the company and the depository institution; or controls in any manner the election of a majority of the directors or trustees of the company and the depository institution.

EXHIBIT 1-B

Concentration Accounts

Internal accounts at a bank established to facilitate the processing and settlement of multiple or individual customer transactions within the bank, usually on the same day. These accounts may also be known as special-use, omnibus, suspense, settlement, intraday, sweep, or collection accounts and are frequently used to facilitate transactions for private banking, trust and custody accounts, funds transfers, and international affiliates.

Conference of State Bank Supervisors (CSBS)

CSBS supports state regulators in advancing the system of state financial supervision by ensuring safety, soundness and consumer protection; promoting economic growth; and fostering innovative, responsive supervision. CSBS represents the State Liaison Committee on the FFIEC Bank Secrecy Act Working Group.

Continuing Activity

Suspicious activity that continues over a period of time and should be made known to law enforcement and the federal banking agencies.

Continuous Linked Settlement Bank (CLS)

A private-sector, special-purpose bank that settles simultaneously both payment obligations that arise from a single foreign exchange transaction.

Controlled By

The depository institution directly or indirectly has the power to vote 25 percent or more of any class of the voting securities of the company; or controls in any manner the election of a majority of the directors or trustees of the company. See 12 USC 1841(a)(2).

Controlling Company

A bank holding company (BHC), as defined in section 2 of the BHC Act, a savings and loan holding company, as defined in section 10(a) of the Home Owners' Loan Act, a company having the power, directly or indirectly, to direct the management policies of an industrial loan company or a parent company or to vote 25 percent or more of any class of voting shares of an

EXHIBIT 1-B

industrial loan company or parent company.

Covered Financial Institution

Refers to Depository institutions, including insured banks, commercial banks, savings associations, federally-insured credit unions, federally-regulated trust companies, U.S. agencies and branches of a foreign bank, and Edge Act corporations; securities broker-dealers; mutual funds; and futures commission merchants and introducing brokers in commodities.

Cover Payments

A cover payment occurs when the originator's bank and the beneficiary's bank do not have a relationship that allows them to settle the payment directly. In that case, the originator's bank instructs the beneficiary's bank to effect the payment and advises that transmission of funds to "cover" the obligation created by the payment order has been arranged through correspondent accounts at one or more intermediary banks.

CSV File (CSV)

A Microsoft Excel-compatible comma separated value file no larger than one (1) megabyte may be included as an attachment as part of a SAR report

Currency Transaction Report (CTR)

§1020.310 - A bank must electronically file a Currency Transaction Report (CTR) for each transaction in currency (deposit, withdrawal, exchange, or other payment or transfer) of more than \$10,000 by, through, or to the bank.

Currency Transaction Report Backfiling

If a bank has failed to file CTRs on reportable transactions, the bank should begin filing CTRs from that point forward and should contact FinCEN's Regulatory Helpline to request a determination on whether the backfiling of unreported transactions is necessary.

Currency Transaction Report Exemption

§1020.315 - Recognition that the routine reporting of some types of large currency transactions does not necessarily aid law enforcement authorities and may place unreasonable

EXHIBIT 1-B

burdens on banks. Consequently, a bank may exempt certain types of customers from currency transaction reporting.

Currency Transaction Report Timing and Retention

§1010.306(a)(1) and (2) A completed CTR must be electronically filed with FinCEN within 15 calendar days after the date of the transaction. The bank must retain copies of CTRs for five years from the date of the report. The bank can retain hard copies or copies in electronic format.

Customer Due Diligence (CDD)

Information collected on a customer that enables the bank to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes also assist the bank in determining when transactions are potentially suspicious.

Customer Identification Program

§1020.220 Refers to the minimum information that a financial institution is required to obtain from an individual to form a reasonable belief that it knows the true identity of each customer.

D

Domestic

Refers to entities formed or organized in the United States.

Domestic Correspondent Account

Accounts maintained by one domestic bank at another domestic bank to provide certain services that can be performed more economically or efficiently because of the other bank's size, expertise in a specific line of business, or geographic location.

E

Enhanced Due Diligence (EDD)

§1020.610(b) Risk-based enhanced policies, procedures, and controls when establishing, maintaining, administering, or managing a correspondent account in the United States for

EXHIBIT 1-B

certain foreign banks.

F

Federal Deposit Insurance Corporation (FDIC)

A federal banking agency responsible for the oversight of state non-member banks.

Federal Financial Institutions Examination Council (FFIEC)

The FFIEC was established in March 1979 to prescribe uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions. The Council has six voting members: the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and the State Liaison Committee. The Council's activities are supported by interagency task forces and by an advisory State Liaison Committee, composed of five representatives of state agencies that supervise financial institutions.

Fedwire

A payment system operated by the Federal Reserve Banks that allows certain financial institution participants to transfer funds from its master account at the Federal Reserve Banks to the master account of any other bank.

Financial Action Task Force (FATF)

An inter-governmental body that sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

Financial Institution Letters (FIL)

Letters to FDIC-supervised banks that may announce new regulations and policies, new FDIC publications, and a variety of other matters of principal interest to those responsible for

EXHIBIT 1-B

operating a bank or savings association.

Financial Crimes Enforcement Network (*FinCEN*)

A bureau of the U.S. Treasury Department and administrator of the BSA.

FinCEN Query

A web application that allows authorized users to access 11 years of FinCEN data. It has been designed and built using modern web search technology that allows users to easily access, query, and analyze FinCEN data across forms and years; apply filters and narrow search results; take advantage of enhanced data and address standardization; import lists of data; build and save complex queries for later use; apply advanced search logic; and manipulate search results via sorting and filtering.

Foreign Correspondent Account

§1020.630 and §1020.670 An account established by a bank for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of the foreign bank, or to handle other financial transactions related to the foreign bank.

Funds Transfers Recordkeeping

§1020.410 Requires each bank involved in funds transfers to collect and retain certain information in connection with funds transfers of \$3,000 or more.

G

Gateway Operator (*GO*)

A financial institution, ACH Operator, or ODFI that acts as an entry or exit point to or from the United States.

H

High Intensity Drug Trafficking Areas (*HIDTA*)

Created by Congress with the Anti-Drug Abuse Act of 1988, provides assistance to Federal, state, local, and tribal law enforcement agencies operating in areas determined to be critical drug-trafficking regions of the United States. There are

EXHIBIT 1-B

currently 28 HIDTAs, which include approximately 18 percent of all counties in the United States and 66 percent of the U.S. population. HIDTA-designated counties are located in 49 states, as well as in Puerto Rico, the U.S. Virgin Islands, and the District of Columbia.

High Intensity Financial Crime Areas (HIFCA)

A program that concentrates law enforcement efforts at the federal, state, and local level to combat money laundering in designated high-intensity money laundering zones. In order to implement this goal, a money-laundering action team was created or identified within each HIFCA to spearhead a coordinated federal, state, and local anti-money laundering effort. Each action team is composed of all relevant federal, state, and local enforcement authorities, prosecutors, and financial regulators.

I

Identifying information

Name, date of birth for individuals, address, identification number

Independent Sales Organization (ISO)

An agent for merchants, including ATM owners, to process electronic transactions.

Independent testing

Should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, a sound practice is for the bank to conduct independent testing generally every 12 to 18 months, commensurate with the BSA/AML risk profile of the bank.

Ineligible Businesses

A business engaged primarily in: serving as a financial institution or as agents for a financial institution of any type; purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment, or mobile homes; practicing law, accounting, or medicine; auctioning of goods; chartering or operation of ships, buses, or aircraft; operating a pawn

EXHIBIT 1-B

brokerage; engaging in gaming of any kind (other than licensed pari-mutuel betting at race tracks); engaging in investment advisory services or investment banking services; operating a real estate brokerage; operating in title insurance activities and real estate closings; engaging in trade union activities; engaging in any other activity that may, from time to time, be specified by FinCEN, such as marijuana-related businesses.

Informal Value Transfer System (IVTS)

A term used to describe a currency or value transfer system that operates informally to transfer money as a business, such as hawalas. In countries lacking a stable financial sector or with large areas not served by formal banks, IVTS may be the only method for conducting financial transactions.

Internal controls

The bank's policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the bank.

Integration

The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets.

International ACH Transaction (IAT)

An IAT is an ACH entry that is part of a payment transaction involving a financial agency's office that is not located in the territorial jurisdiction of the United States.

International Business Corporation (IBC)

Entities formed outside of a person's country of residence that can be used to maintain confidentiality or hide assets. Ownership can, based on jurisdiction, be conveyed through

EXHIBIT 1-B

registered or bearer shares.

L

Layering

The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or wiring or transferring funds to and through numerous accounts in one or more financial institutions.

Letter of Credit

A letter issued by a bank to another bank (typically in a different country) to serve as a guarantee for payments made to a specified person under specified conditions.

Letters to Credit Unions (LCU)

LCUs are used by the NCUA to share information, announce new policies, and provide guidance for credit unions and credit union examination staff.

N

National Credit Union Administration (NCUA)

A federal banking agency responsible for the oversight of federally insured credit unions.

National Security Letters (NSL)

Written investigative demands that may be issued by the local FBI and other federal government authorities in counterintelligence and counterterrorism investigations.

Nationwide Multistate Licensing System & Registry (NMLS)

The system of record for non-depository, financial services licensing or registration in participating state agencies, including the District of Columbia and U.S. Territories of Puerto Rico, the U.S. Virgin Islands, and Guam.

Nested Accounts

EXHIBIT 1-B

When a foreign financial institution gains access to the U.S. financial system by operating through a U.S. correspondent account belonging to another foreign financial institution.

Nominee Incorporation Services (NIS)

Intermediaries that establish U.S. shell companies and bank accounts on behalf of foreign clients.

Nondeposit Investment Products (NDIP)

A wide array of investment products (e.g., securities, bonds, and fixed or variable annuities) or sales programs that include cash management sweep accounts to retail and commercial clients offered by the bank directly.

Non-listed Business

A commercial enterprise to the extent of its domestic operations.

Nonresident Alien

A non-U.S. citizen who: (i) is not a lawful permanent resident of the United States during the calendar year and who does not meet the substantial presence test, or (ii) has not been issued an alien registration receipt card, also known as a green card.

O

OCC Advisory Letters

Issuances published for OCC-supervised banks that contain information of continuing importance to bankers and examiners.

OCC Alerts

Issuances published for OCC-supervised banks with special urgency to notify bankers and examiners of matters of pressing concern, often suspicious or illegal banking practices.

OCC Bulletins

Issuances published for OCC-supervised banks that contain information of continuing importance to bankers and examiners.

Office of Foreign Assets Control (OFAC)

EXHIBIT 1-B

An office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime.

Office of the Comptroller of the Currency (OCC)

A federal banking agency responsible for the oversight of national banks, federal branches and agencies of foreign banks licensed or chartered by the OCC, and savings associations.

Offshore Financial Centers (OFC)

A jurisdiction specializing in providing corporate and commercial services (such as establishing IBCs) that provide ownership privacy and impose few or no tax obligations. Many OFCs have limited organizational disclosure and recordkeeping requirements for establishing foreign business entities.

Open Loop Prepaid Cards

Cards that can be used for purchases at any merchant that accepts cards issued for use on the payment network associated with the card and to access cash at any automated teller machine (ATM) that connects to the affiliated ATM network.

Originating Depository Financial Institution (ODFI)

The Originator's depository financial institution that forwards the ACH transaction into the national ACH network through an ACH Operator.

P

Parallel Banking

When at least one U.S. bank and one foreign financial institution are controlled either directly or indirectly by the same person or group of persons who are closely associated in their business dealings or otherwise acting together, but are not subject to consolidated supervision by a single home country supervisor.

EXHIBIT 1-B

Payable Through Accounts (PTA)

A way for a foreign financial institution to provide their customers with access to the U.S. banking system through the foreign financial institution's account at a U.S. bank. The foreign financial institution provides its customers, commonly referred to as "subacccountholders," with checks that allow them to draw funds from the foreign financial institution's account at the U.S. bank. Also known as "pass-through" or "pass-by" accounts.

Payable Upon Proper Identification (PUPID)

Funds transfers for which there is no specific account to deposit the funds into and the beneficiary of the funds is not a bank customer. The beneficiary bank may place the incoming funds into a suspense account and ultimately release the funds when the individual provides proof of identity.

Payroll Customer

A customer who withdrawals for payroll purposes from existing exemptible accounts.

Placement

The first and most vulnerable stage of laundering money. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. An example may include: dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a canceled vacation package or insurance policy, or purchasing a series of monetary instruments (e.g., cashier's checks or money orders) that are then collected and deposited into accounts at another location or financial institution.

Politically exposed persons (PEPs)

See 1010.605(p)(1) and senior foreign political figure.

Pouch Activity

Use of a carrier, courier (either independent or common), or a referral agent employed by the courier, to transport currency, monetary instruments, and other documents from outside the

EXHIBIT 1-B

United States to a bank in the United States.

Private Investment Company (PIC)

Essential a subset of an international business corporation.

They are typically used to hold individual funds and investments, and ownership can be vested through bearer shares or registered shares.

Professional Service Provider

Lawyers, accountants, investment brokers, and other third parties that act as financial liaisons (or intermediaries) for their clients. These providers may conduct financial dealings for their clients.

Prohibited Transactions

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected, (i.e., not processed).

Prohibition of SAR Disclosure

No bank, and no director, officer, employee, or agent of a bank that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities.

R

Receiver

An organization or person that authorizes the Originator to initiate an ACH transaction, either as a debit or credit to an account.

Receiving Depository Financial Institution (RDFI)

The Receiver's depository institution that receives the ACH transaction from the ACH Operators and credits or debits funds from their receivers' accounts.

Regulatory Alerts (RA)

EXHIBIT 1-B

RAs are used by the NCUA to share information, announce new policies, and provide guidance for credit unions and credit union examination staff.

Remote Deposit Capture (RDC)

A deposit transaction delivery system that allows a bank's customers to scan a check or monetary instrument, and then transmit the scanned or digitized image to the institution.

S

SAR Filing on Continuing Activity

Continuing suspicious activity should be reported by filing a SAR after a 90 day review with the filing deadline being 120 calendar days after the date of the previously related SAR filing.

SAR Timing

SAR rules require that a SAR be electronically filed through the BSA E-Filing System no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days.

Section 311

The USA PATRIOT Act added 31 USC 5318A to the BSA, which authorizes the Secretary of the Treasury to require domestic financial institutions and domestic financial agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern.

Secure Information Sharing System (S/ISS)

A web-based system used by FinCEN to post, and banks to retrieve, 314(a) subject lists every two weeks or more frequently if an emergency request is transmitted.

Shell Company

An entity without a physical presence in any country.

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

EXHIBIT 1-B

A messaging infrastructure, not a payments system, which provides users with a private international communications link among themselves.

Specially Designated Nationals

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them.

Standby Letter of Credit

A guarantee of payment issued by a bank on behalf of a client that is used as "payment of last resort" should the client fail to fulfill a contractual commitment with a third party.

Supervision and Regulation Letters (SR Letters)

Issued by the Board of Governors' Division of Supervision and Regulation, SR Letters are an important means of disseminating information to banking supervision staff at the Board of Governors and the Reserve Banks and, in some instances, to supervised banking organizations. They often address significant policy and procedural matters related to the Federal Reserve System's supervisory responsibilities.

T

Technical Violations

Isolated or limited instances of noncompliance with the BSA that occur within an otherwise adequate system of policies, procedures, and processes.

Terrorist Financing (TF)

The process by which terrorists fund their operations in order to perform terrorist acts. The motivation behind terrorist financing is ideological as opposed to profit-seeking.

Third-Party Payment Processors (TPPP)

EXHIBIT 1-B

Bank customers that provide payment-processing services to merchants and other business entities.

Trade Finance

Short-term financing to facilitate the import and export of goods.

Training

Appropriate personnel must be trained in applicable aspects of the BSA. Training should include regulatory requirements and the bank's internal BSA/AML policies, procedures, and processes. At a minimum, the bank's training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person's specific responsibilities.

Transactions of Exempt Persons

§1020.315 - Recognition that the routine reporting of some types of large currency transactions does not necessarily aid law enforcement authorities and may place unreasonable burdens on banks. Consequently, a bank may exempt certain types of customers from currency transaction reporting.

Travel Rule

§1020.410(f) For fund transmittals of \$3,000 or more, the transmitter's financial institution must include certain information in the transmittal order at the time that a transmittal order is sent to a receiving financial institution.

Trust Accounts

A legal arrangement in which one party (the trustor or grantor) transfers ownership of assets to a person or bank (the trustee) to be held or used for the benefit of others. These arrangements include the broad categories of court-supervised accounts (e.g., executorships and guardianships), personal trusts (e.g., living trusts, trusts established under a will, and charitable trusts), and corporate trusts (e.g., bond trusteeships, ERISA trusts).

U

USA PATRIOT Act

EXHIBIT 1-B

FFIEC BSA/AML Glossary

<https://bsaaml.ffiec.gov/references/glossary>

Uniting and Strengthening America by Providing Appropriate
Tool Required to Intercept and Obstruct Terrorism Act of 2001.

V

Virtual Currency

A medium of exchange that operates like a currency in some environments, but does not have legal tender status in any jurisdiction. Virtual currency must be converted into U.S. dollars through the services of an administrator or exchanger prior to deposit into the banking system.

FFIEC Bank Secrecy Act/Anti-Money Laundering InfoBase
Privacy Policy (<https://www.ffiec.gov/privacy.htm>) /
FOIA (<https://www.ffiec.gov/foia.htm>) /
Accessibility (<https://www.ffiec.gov/pdfhelp.htm>) /
FFIEC Disclaimer (<https://www.ffiec.gov/disclaimer.htm>) /
USA.gov (<https://www.usa.gov>) /
Contact (<mailto:ffiecinfobase@frb.gov>)

2021.0225.147

ASSESSING THE BSA/AML COMPLIANCE PROGRAM

ASSESSING THE BSA/AML COMPLIANCE PROGRAM

Objective: *Assess whether the bank has designed, implemented, and maintains an adequate BSA/AML compliance program that complies with BSA regulatory requirements.*

Banks must establish and maintain procedures reasonably designed to assure and monitor compliance with BSA regulatory requirements (BSA/AML compliance program).⁹ The BSA/AML compliance program¹⁰ must be written, approved by the board of directors,¹¹ and noted in the board minutes. To achieve the purposes of the BSA, the BSA/AML compliance program should be commensurate with the bank's ML/TF and other illicit financial activity risk profile. Refer to the [BSA/AML Risk Assessment](#) section and [Appendix I - Risk Assessment Link to the BSA/AML Compliance Program](#) for more information.

Written policies, procedures, and processes alone are not sufficient to have an adequate BSA/AML compliance program; practices that correspond with the bank's written policies, procedures, and processes are needed for implementation. Importantly, policies, procedures, processes, and practices should align with the bank's unique ML/TF and other illicit financial activity risk profile. The BSA/AML compliance program must provide for the following requirements:¹²

- A system of internal controls to assure ongoing compliance.
- Independent testing for compliance to be conducted by bank personnel or by an outside party.
- Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance (BSA compliance officer).
- Training for appropriate personnel.

In addition, the BSA/AML compliance program must include a customer identification program (CIP) with risk-based procedures that enable the bank to form a reasonable belief that it knows

⁹ 12 USC 1818(s) and 12 USC 1786(q).

¹⁰ The Federal Reserve requires Edge and agreement corporations and U.S. branches, agencies, and other offices of foreign banks supervised by the Federal Reserve to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations (refer to Regulation K, 12 CFR 211.5(m)(1) and 12 CFR 211.24(j)(1)). Because the BSA does not apply extraterritorially, foreign offices of domestic banks are expected to have policies, procedures, and processes in place to protect against risks of money laundering and terrorist financing (12 CFR 208.63, 12 CFR 326.8, and 12 CFR 21.21).

¹¹ The Federal Reserve, the FDIC, and the OCC, each require the U.S. branches, agencies, and representative offices of the foreign banks they supervise operating in the United States to develop written BSA compliance programs that are approved by their respective bank's board of directors and noted in the minutes, or that are approved by delegates acting under the express authority of their respective bank's board of directors to approve the BSA compliance programs. "Express authority" means the head office must be aware of its U.S. AML program requirements and there must be some indication of purposeful delegation.

¹² 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (Federal Reserve); 12 CFR 326.8 (FDIC); 12 CFR 748.2 (NCUA); 12 CFR 21.21 (OCC).

EXHIBIT 1-B

the true identity of its customers. The BSA/AML compliance program must also include appropriate risk-based procedures for conducting ongoing customer due diligence (CDD) and complying with beneficial ownership requirements for legal entity customers as set forth in regulations issued by Financial Crimes Enforcement Network (FinCEN). Refer to the [Customer Identification Program](#), [Customer Due Diligence](#), and [Beneficial Ownership Requirements for Legal Entity Customers](#) sections for more information.

The assessment of the adequacy of the bank's BSA/AML compliance program is bank-specific, and examiners should consider all pertinent information. A review of the bank's written policies, procedures, and processes is a first step in determining the overall adequacy of the BSA/AML compliance program. The completion of examination and testing procedures is necessary to support overall conclusions regarding the BSA/AML compliance program. BSA/AML examination findings should be discussed with relevant bank management, and findings must be included in the report of examination (ROE) or supervisory correspondence.

Preliminary Evaluation

Once examiners complete the review of the bank's BSA/AML compliance program, they should develop and document a preliminary assessment of the bank's program. At this point, examiners should revisit the initial BSA/AML examination plan to determine whether additional areas of review are necessary to assess the adequacy of the bank's BSA/AML compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements. These adjustments to the initial examination plan could be based on information identified during the review, such as a new product or business line at the bank or independent testing report findings. Examiners should document and support any changes to the examination plan, if necessary, then proceed to the applicable examination and testing procedures in *Assessing Compliance with BSA Regulatory Requirements, Risks Associated with Money Laundering and Terrorist Financing*, and [Office of Foreign Assets Control](#). Once all relevant examination and testing procedures are completed as documented in the examination plan, examiners should proceed to [Developing Conclusions and Finalizing the Examination](#).

[Return to Contents](#)

BSA/AML INTERNAL CONTROLS

Objective: *Assess the bank's system of internal controls to assure ongoing compliance with BSA regulatory requirements.*

The board of directors, acting through senior management, is ultimately responsible for ensuring that the bank maintains a system of internal controls to assure ongoing compliance with BSA regulatory requirements.¹³ Internal controls are the bank's policies, procedures, and processes designed to mitigate and manage ML/TF and other illicit financial activity risks and to achieve compliance with BSA regulatory requirements. The board of directors plays an important role in establishing and maintaining an appropriate culture that places a priority on compliance, and a structure that provides oversight and holds senior management accountable for implementing the bank's BSA/AML internal controls. The system of internal controls, including the level and type, should be commensurate with the bank's size or complexity, and organizational structure. Large or more complex banks may implement specific departmental internal controls for BSA/AML compliance. Departmental internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive, bank-wide BSA/AML compliance program.

Examiners should determine whether the bank's internal controls are designed to assure ongoing compliance with BSA regulatory requirements and:

- Incorporate the bank's BSA/AML risk assessment and the identification of ML/TF and other illicit financial activity risks, along with any changes in those risks.
- Provide for program continuity despite changes in operations, management, or employee composition or structure.
- Facilitate oversight of information technology sources, systems, and processes that support BSA/AML compliance.
- Provide for timely updates in response to changes in regulations.
- Incorporate dual controls and the segregation of duties to the extent possible. For example, employees who complete the reporting forms (such as suspicious activity reports (SARs), currency transaction reports (CTRs), and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.
- Include mechanisms to identify and inform the board of directors, or a committee thereof, and senior management of BSA compliance initiatives, identified compliance deficiencies and corrective action taken, and notify the board of directors of SARs filed.
- Identify and establish specific BSA compliance responsibilities for bank personnel and provide oversight for execution of those responsibilities, as appropriate.

¹³ 12 CFR 208.63(c)(1), (Federal Reserve); 12 CFR 326.8(c)(1) (FDIC); 12 CFR 748.2(c)(1) (NCUA); 12 CFR 21.21(d)(1) (OCC).

EXHIBIT 1-B

This list is not all-inclusive and should be tailored to reflect the bank's ML/TF and other illicit financial activity risk profile. More information concerning individual regulatory requirements and specific risk areas is in the *Assessing Compliance with BSA Regulatory Requirements* and *Risks Associated with Money Laundering and Terrorist Financing* sections.

Examiners should determine whether the bank's system of internal controls is designed to mitigate and manage the ML/TF and other illicit financial activity risks, and comply with BSA regulatory requirements. Examiners should assess the adequacy of internal controls based on the factors listed above.

[Return to Contents](#)

BSA/AML INDEPENDENT TESTING

Objective: *Assess the adequacy of the bank's independent testing program.*

The purpose of independent testing (audit) is to assess the bank's compliance with BSA regulatory requirements, relative to its risk profile, and assess the overall adequacy of the BSA/AML compliance program. Independent testing should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties.¹⁴

Banks that do not employ outside auditors or consultants or do not have internal audit departments may comply with this requirement by using qualified bank staff who are not involved in the function being tested. Banks engaging outside auditors or consultants should ensure that the persons conducting the BSA/AML independent testing are not involved in other BSA-related functions at the bank that may present a conflict of interest or lack of independence, such as training or developing policies and procedures. Regardless of who performs the independent testing, the party conducting the BSA/AML independent testing should report directly to the board of directors or to a designated board committee comprised primarily, or completely, of outside directors. Banks with a community focus, less complex operations, and lower-risk profiles for ML/TF and other illicit financial activities may consider utilizing a shared resource as part of a collaborative arrangement to conduct independent testing.¹⁵

There is no regulatory requirement establishing BSA/AML independent testing frequency. Independent testing, including the frequency, should be commensurate with the ML/TF and other illicit financial activity risk profile of the bank and the bank's overall risk management strategy. The bank may conduct independent testing over periodic intervals (for example, every 12-18 months) and/or when there are significant changes in the bank's risk profile, systems, compliance staff, or processes. More frequent independent testing may be appropriate when errors or deficiencies in some aspect of the BSA/AML compliance program have been identified or to verify or validate mitigating or remedial actions.

Independent testing of specific BSA requirements should be risk-based and evaluate the quality of risk management related to ML/TF and other illicit financial activity risks for significant banking operations across the organization. Risk-based independent testing focuses on the bank's risk assessment to tailor independent testing to the areas identified as being of greatest risk and concern. Risk-based independent testing programs vary depending on the bank's size or complexity, organizational structure, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. Risk-based independent testing should include evaluating pertinent internal controls and information technology sources, systems, and processes used to support the BSA/AML compliance program. Consideration should also be given to the expansion into new product lines, services, customer types, and geographic locations through organic growth or merger activity.

¹⁴ 12 CFR 208.63(c)(2) (Federal Reserve); 12 CFR 326.8(c)(2) (FDIC); 12 CFR 748.2(c)(2) (NCUA); 12 CFR 21.21(d)(2) (OCC)

¹⁵ For detailed information on collaborative arrangements see "Interagency Statement on Sharing Bank Secrecy Act Resources," issued by Federal Reserve, FDIC, FinCEN, NCUA, and OCC, October 3, 2018.

EXHIBIT 1-B

The independent testing should evaluate the overall adequacy of the bank's BSA/AML compliance program and the bank's compliance with BSA regulatory requirements. This evaluation helps inform the board of directors and senior management of weakness, or areas in need of enhancements or stronger controls. Typically, this evaluation includes an explicit statement in the report(s) about the bank's overall compliance with BSA regulatory requirements. At a minimum, the independent testing should contain sufficient information for the reviewer (e.g., board of directors, senior management, BSA compliance officer, review auditor, or an examiner) to reach a conclusion about the overall adequacy of the BSA/AML compliance program.

To contain sufficient information to reach this conclusion, independent testing of the BSA/AML compliance program and BSA regulatory requirements may include a risk-based review of whether:

- The bank's BSA/AML risk assessment aligns with the bank's risk profile (products, services, customers, and geographic locations).
- The bank's policies, procedures, and processes for BSA compliance align with the bank's risk profile.
- The bank adheres to its policies, procedures, and processes for BSA compliance.
- The bank complies with BSA recordkeeping and reporting requirements (e.g., customer information program (CIP), customer due diligence (CDD), beneficial ownership, suspicious activity reports (SARs), currency transaction reports (CTRs) and CTR exemptions, and information sharing requests).
- The bank's overall process for identifying and reporting suspicious activity is adequate. This review may include evaluating filed or prepared SARs to determine their accuracy, timeliness, completeness, and conformance to the bank's policies, procedures, and processes.
- The bank's information technology sources, systems, and processes used to support the BSA/AML compliance program are complete and accurate. These may include reports or automated programs used to: identify large currency transactions, aggregate daily currency transactions, record monetary instrument sales and funds transfer transactions, and provide analytical and trend reports.
- Training is provided for appropriate personnel, tailored to specific functions and positions, and includes supporting documentation.
- Management took appropriate and timely action to address any violations and other deficiencies noted in previous independent testing and regulatory examinations, including progress in addressing outstanding supervisory enforcement actions, if applicable.

Auditors should document the independent testing scope, procedures performed, transaction testing completed, and any findings. All independent testing documentation and supporting workpapers should be available for examiner review. Violations; exceptions to bank policies, procedures, or processes; or other deficiencies noted during the independent testing should be documented and reported to the board of directors or a designated board committee in a timely

EXHIBIT 1-B

manner. The board of directors, or a designated board committee, and appropriate staff should track deficiencies and document progress implementing corrective actions.

Examiners should review relevant documents such as the auditor's report(s), scope, and supporting workpapers, as needed. Examiners should determine whether there is an explicit statement in the report(s) about the bank's overall compliance with BSA regulatory requirements or, at a minimum, sufficient information to reach a conclusion about the overall adequacy of the BSA/AML compliance program. Examiners should determine whether the testing was conducted in an independent manner. Examiners may also evaluate, as applicable,¹⁶ the subject matter expertise, qualifications, and independence of the person or persons performing the independent testing. Examiners should determine whether the independent testing sufficiently covers ML/TF and other illicit financial activity risks within the bank's operations and whether the frequency is commensurate with the bank's risk profile. Examiners should also review whether violations; exceptions to policies, procedures, or processes; or other deficiencies are reported to the board of directors or a designated board committee in a timely manner, whether they are tracked, and whether corrective actions are documented.

[Return to Contents](#)

¹⁶ For more information, *see e.g.*, OCC Safety and Soundness Standards, 12 C.F.R. Part 30 App. D, II.L.

BSA COMPLIANCE OFFICER

Objective: *Confirm that the bank's board of directors has designated a qualified individual or individuals (BSA compliance officer) responsible for coordinating and monitoring day-to-day compliance with BSA regulatory requirements. Assess whether the BSA compliance officer has the appropriate authority, independence, access to resources, and competence to effectively execute all duties.*

The bank's board of directors must designate a qualified individual or individuals to serve as the BSA compliance officer.¹⁸ The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program, including managing the bank's compliance with BSA regulatory requirements. The board of directors is ultimately responsible for the bank's BSA/AML compliance and should provide oversight for senior management and the BSA compliance officer in the implementation of the bank's board-approved BSA/AML compliance program.¹⁹

The act by the bank's board of directors of appointing a BSA compliance officer is not, by itself, sufficient to meet the regulatory requirement to establish and maintain a BSA/AML compliance program reasonably designed to assure and monitor compliance with the BSA. The board of directors is responsible for ensuring that the BSA compliance officer has appropriate authority, independence, and access to resources to administer an adequate BSA/AML compliance program based on the bank's ML/TF and other illicit financial activity risk profile. The BSA compliance officer should regularly report the status of ongoing compliance with the BSA to the board of directors and senior management so that they can make informed decisions about existing risk exposure and the overall BSA/AML compliance program. Reporting to the board of directors or a designated board committee about the status of ongoing compliance should include pertinent BSA-related information, including the required notification of suspicious activity report (SAR) filings.

The BSA compliance officer is responsible for carrying out the board's direction, including the implementation of the bank's BSA/AML policies, procedures, and processes. The BSA compliance officer may delegate BSA/AML duties to staff, but the officer is responsible for overseeing the day-to-day BSA/AML compliance program.

The BSA compliance officer should be competent, as demonstrated by knowledge of the BSA and related regulations, implementation of the bank's BSA/AML compliance program, and understanding of the bank's ML/TF and other illicit financial activity risk profile associated with its banking activities. The actual title of the individual responsible for overall BSA compliance is not important; however, the individual's authority, independence, and access to resources within the bank is critical.

¹⁸ 12 CFR 208.63(c)(3), (Federal Reserve); 12 CFR 326.8(c)(3) (FDIC); 12 CFR 748.2(c)(3) (NCUA); 12 CFR 21.21(d)(3) (OCC).

¹⁹ FinCEN (2014), "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance," FIN-2014-A007.

EXHIBIT 1-B

Indicators of appropriate authority of the BSA compliance officer may include senior management seeking the BSA compliance officer's input regarding: the ML/TF and other illicit financial activity risks related to expansion into new products, services, customer types and geographic locations; or operational changes, such as the implementation of, or adjustments to, systems that impact the BSA compliance function. Indicators of appropriate independence of the BSA compliance officer may include, but are not limited to: clear lines of reporting and communication ultimately up to the board of directors or a designated board committee that do not compromise the BSA compliance officer's independence, the ability to undertake the BSA compliance officer's role without undue influence from the bank's business lines, and identification and reporting of issues to senior management and the board of directors.

The BSA compliance officer should have access to suitable resources. This may include, but is not limited to: adequate staffing with the skills and expertise necessary for the bank's overall risk level (based on products, services, customers, and geographic locations), size or complexity, and organizational structure; and systems to support the timely identification, measurement, monitoring, reporting, and management of the bank's ML/TF and other illicit financial activity risks.

Examiners should confirm that the bank's board of directors has designated an individual or individuals responsible for the overall BSA/AML compliance program who are appropriately qualified. Examiners should review reports to the board of directors and senior management regarding the status of ongoing compliance and pertinent BSA-related information, including the required notification of SAR filings. Examiners should confirm that the BSA compliance officer has the appropriate authority, independence, and access to resources.

[Return to Contents](#)

BSA/AML TRAINING

Objective: *Confirm that the bank has developed a BSA/AML training program and delivered training to appropriate personnel.*

Banks must provide training for appropriate personnel.²⁰ Training should cover the aspects of the BSA that are relevant to the bank and its risk profile, and appropriate personnel includes those whose duties require knowledge or involve some aspect of BSA/AML compliance. Training should cover BSA regulatory requirements, supervisory guidance, and the bank's internal BSA/AML policies, procedures, and processes. Training should be tailored to each individual's specific responsibilities, as appropriate. In addition, targeted training may be necessary for specific ML/TF and other illicit financial activity risks and requirements applicable to certain business lines or operational units, such as lending, trust services, foreign correspondent banking, and private banking. An overview of the purposes of the BSA and its regulatory requirements are typically provided to new staff during employee orientation or reasonably thereafter. The BSA compliance officer and BSA compliance staff should receive periodic training that is relevant and appropriate to remain informed of changes to regulatory requirements and changes to the bank's risk profile.

The board of directors and senior management should receive foundational training and be informed of changes and new developments in the BSA, including its implementing regulations, the federal banking agencies' regulations, and supervisory guidance. While the board of directors may not require the same degree of training as banking operations personnel, the training should provide board members with sufficient understanding of the bank's risk profile and BSA regulatory requirements. Without a general understanding of the BSA, it is more difficult for the board of directors to provide adequate oversight of the BSA/AML compliance program, including approving the written BSA/AML compliance program, establishing appropriate independence for the BSA/AML compliance function, and providing sufficient BSA/AML resources.

Periodic training for appropriate personnel should incorporate current developments and changes to BSA regulatory requirements; supervisory guidance; internal policies, procedures, and processes; and the bank's products, services, customers, and geographic locations. Changes to information technology sources, systems, and processes used in BSA compliance may be covered during training for appropriate personnel. The training program may be used to reinforce the importance that the board of directors and senior management place on the bank's compliance with the BSA and that all employees understand their role in maintaining an adequate BSA/AML compliance program.

Training programs should include examples of money laundering and suspicious activity monitoring and reporting that are tailored, as appropriate, to each operational area. For example, training for tellers should focus on examples involving large currency transactions

²⁰ 12 CFR 208.63(c)(4) (Federal Reserve); 12 CFR 326.8(c)(4) (FDIC); 12 CFR 748.2(c)(4) (NCUA); 12 CFR 21.21(d)(4) (OCC).

EXHIBIT 1-B

or suspicious activities, and training for the loan department should provide examples involving money laundering through lending arrangements. The bank should provide training for any agents who are responsible for conducting BSA-related functions on behalf of the bank. If the bank relies on another financial institution or other party to perform training, appropriate documentation should be maintained.²¹

Banks should document their training programs. Training and testing materials (if training-related testing is used by the bank), and the dates of training sessions should be maintained by the bank. Additionally, training materials and records should be available for auditor or examiner review. The bank should maintain documentation of attendance records and any failures of personnel to take the required training in a timely manner, as well as any corrective actions taken to address such failures.

Examiners should determine whether all personnel whose duties require knowledge of the BSA are included in the training program and whether materials include training on BSA regulatory requirements, supervisory guidance, and the bank's internal BSA/AML policies, procedures, and processes.

[Return to Contents](#)

²¹ For more information on collaborative arrangements, see "Interagency Statement on Sharing Bank Secrecy Act Resources," issued by Federal Reserve, FDIC, FinCEN, NCUA, and OCC, October 3, 2018.

EXHIBIT 1-B

responsibility should be clear with respect to the content and comprehensiveness of MIS reports, the depth and frequency of monitoring efforts, and the role of different parties within the banking organization (e.g., risk, business lines, operations) in BSA/AML compliance decision-making processes. Clearly communicating which functions have been delegated and which remain centralized helps to ensure consistent implementation of the BSA/AML compliance program among lines of business, affiliates, and jurisdictions. In addition, a clear line of responsibility may help to avoid conflicts of interest and ensure that objectivity is maintained.

Regardless of the management structure or size of the institution, BSA/AML compliance staff located within lines of business is not precluded from close interaction with the management and staff of the various business lines. BSA/AML compliance functions are often most effective when strong working relationships exist between compliance and business line staff.

In some compliance structures, the compliance staff reports to the management of the business line. This can occur in smaller institutions when the BSA/AML compliance staff reports to a senior bank officer; in larger institutions when the compliance staff reports to a line of business manager; or in a foreign banking organization's U.S. operations when the staff reports to a single office or executive. These situations can present risks of potential conflicts of interest that could hinder effective BSA/AML compliance. To ensure the strength of compliance controls, an appropriate level of BSA/AML compliance independence should be maintained, for example, by:

- Providing BSA/AML compliance staff a reporting line to the corporate compliance or other independent function;
- Ensuring that BSA/AML compliance staff is actively involved in all matters affecting AML risk (e.g., new products, review or termination of customer relationships, filing determinations);
- Establishing a process for escalating and objectively resolving disputes between BSA/AML compliance staff and business line management; and
- Establishing internal controls to ensure that compliance objectivity is maintained when BSA/AML compliance staff is assigned additional bank responsibilities.

Management and Oversight of the BSA/AML Compliance Program

The board of directors and senior management of a bank have different responsibilities and roles in overseeing, and managing BSA/AML compliance risk. The board of directors has primary responsibility for ensuring that the bank has a comprehensive and effective BSA/AML compliance program and oversight framework that is reasonably designed to ensure compliance with BSA/AML regulation. Senior management is responsible for implementing the board-approved BSA/AML compliance program.

Boards of directors.¹⁶⁹ The board of directors is responsible for approving the BSA/AML compliance program and for overseeing the structure and management of the bank's BSA/AML compliance function. The board is responsible for setting an appropriate culture of BSA/AML compliance, establishing clear policies regarding the management of key BSA/AML risks, and ensuring that these policies are adhered to in practice.

The board should ensure that senior management is fully capable, qualified, and properly motivated to manage the BSA/AML compliance risks arising from the organization's business activities in a manner that is consistent with the board's expectations. The board should ensure that the BSA/AML compliance function has an appropriately prominent status within the organization. Senior management within the BSA/AML compliance function and senior compliance personnel within the individual business lines should have the appropriate authority, independence, and access to personnel and information within the organization, and appropriate resources to conduct their activities effectively. The board should ensure that its views about the importance of BSA/AML compliance are understood and communicated across all levels of the banking organization. The board also should ensure that senior management has established appropriate incentives to integrate BSA/AML compliance objectives into management goals and compensation structure across the organization, and that corrective actions, including disciplinary measures, if appropriate, are taken when serious BSA/AML compliance failures are identified.

Senior management. Senior management is responsible for communicating and reinforcing the BSA/AML compliance culture established by the board, and implementing and enforcing the board-approved BSA/AML compliance program. If the banking organization has a separate BSA/AML compliance function, senior management of the function should establish, support, and oversee the organization's BSA/AML compliance program. BSA/AML compliance staff should report to the board, or a committee thereof, on the effectiveness of the BSA/AML compliance program and significant BSA/AML compliance matters.

Senior management of a foreign banking organization's U.S. operations should provide sufficient information relating to the U.S. operations' BSA/AML compliance to the governance or control functions in its home country, and should ensure that responsible senior management in the home country has an appropriate understanding of the BSA/AML risk and control environment governing U.S. operations. U.S. management should assess the effectiveness of established BSA/AML control mechanisms for U.S. operations on an ongoing basis and report and escalate areas of concern as needed. As appropriate, corrective action then should be developed, implemented and validated.

Consolidated BSA/AML Compliance Programs

Banking organizations that centrally manage the operations and functions of their subsidiary banks, other subsidiaries, and business lines should ensure that comprehensive risk management policies, procedures, and processes are in place across the organization to

¹⁶⁹ Foreign banking organizations should ensure that, with respect to their U.S. operations, the responsibilities of the board described in this section are fulfilled in an appropriate manner through their oversight structure and BSA/AML risk management framework.

EXHIBIT 1-B

(Blank Page)

Appendix D: Statutory Definition of Financial Institution

As defined in the BSA 31 USC 5312(a)(2), the term “financial institution” includes the following:

- An insured bank (as defined in section 3(h) of the FDI Act (12 USC 1813(h))).
- A commercial bank or trust company.
- A private banker.
- An agency or branch of a foreign bank in the United States.
- Any credit union.
- A thrift institution.
- A broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 USC 78a *et seq.*).
- A broker or dealer in securities or commodities.
- An investment banker or investment company.
- A currency exchange.
- An issuer, redeemer, or cashier of traveler’s checks, checks, money orders, or similar instruments.
- An operator of a credit card system.
- An insurance company.
- A dealer in precious metals, stones, or jewels.
- A pawnbroker.
- A loan or finance company.
- A travel agency.
- A licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.
- A telegraph company.
- A business engaged in vehicle sales, including automobile, airplane, and boat sales.
- Persons involved in real estate closings and settlements.
- The U.S. Postal Service.

EXHIBIT 1-B

Appendix D: Statutory Definition of Financial Institution

- An agency of the United States government or of a state or local government carrying out a duty or power of a business described in this paragraph.
- A casino, gambling casino, or gaming establishment with an annual gaming revenue of more than \$1 million that —
 - Is licensed as a casino, gambling casino, or gaming establishment under the laws of any state or any political subdivision of any state; or
 - Is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation that is limited to class I gaming (as defined in section 4(6) of such act).
- Any business or agency that engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity that is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage.
- Any other business designated by the Secretary whose currency transactions have a high degree of usefulness in criminal, tax, or regulatory matters.
- Any futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act (7 USC 1, *et seq.*).

Appendix G: Structuring

Structuring transactions to evade BSA reporting and certain recordkeeping requirements can result in civil and criminal penalties under the BSA. Under the BSA (31 USC 5324), no person shall, for the purpose of evading the CTR or a geographic targeting order reporting requirement, or certain BSA recordkeeping requirements:

- Cause or attempt to cause a bank to fail to file a CTR or a report required under a geographic targeting order or to maintain a record required under BSA regulations.
- Cause or attempt to cause a bank to file a CTR or report required under a geographic targeting order, or to maintain a BSA record that contain a material omission or misstatement of fact.
- Structure, as defined above, or attempt to structure or assist in structuring, any transaction with one or more banks.

The definition of structuring, as set forth in 31 CFR 1010.100 (xx) (which was implemented before a USA PATRIOT Act provision extended the prohibition on structuring to geographic targeting orders and BSA recordkeeping requirements), states, “a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the [CTR filing requirements].” “In any manner” includes, but is not limited to, breaking down a single currency sum exceeding \$10,000 into smaller amounts that may be conducted as a series of transactions at or less than \$10,000. The transactions need not exceed the \$10,000 CTR filing threshold at any one bank on any single day in order to constitute structuring.

Money launderers and criminals have developed many ways to structure large amounts of currency to evade the CTR filing requirements. Unless currency is smuggled out of the United States or commingled with the deposits of an otherwise legitimate business, any money laundering scheme that begins with a need to convert the currency proceeds of criminal activity into more legitimate-looking forms of financial instruments, accounts, or investments, is likely to involve some form of structuring. Structuring remains one of the most commonly reported suspected crimes on SARs.

Bank employees should be aware of and alert to structuring schemes. For example, a customer may structure currency deposit or withdrawal transactions, so that each is less than the \$10,000 CTR filing threshold; use currency to purchase official bank checks, money orders, or traveler’s checks with currency in amounts less than \$10,000 (and possibly in amounts less than the \$3,000 recordkeeping threshold for the currency purchase of monetary instruments to avoid having to produce identification in the process); or exchange small bank notes for large ones in amounts less than \$10,000.

However, two transactions slightly under the \$10,000 threshold conducted days or weeks apart may not necessarily be structuring. For example, if a customer deposits \$9,900 in currency on Monday and deposits \$9,900 in currency on Wednesday, it should not be assumed that structuring has occurred. Instead, further review and research may be

EXHIBIT 1-B

Appendix G: Structuring

necessary to determine the nature of the transactions, prior account history, and other relevant customer information to assess whether the activity is suspicious. Even if structuring has not occurred, the bank should review the transactions for suspicious activity.

In addition, structuring may occur before a customer brings the funds to a bank. In these instances, a bank may be able to identify the aftermath of structuring. Deposits of monetary instruments that may have been purchased elsewhere might be structured to evade the CTR filing requirements or the recordkeeping requirements for the currency purchase of monetary instruments. These instruments are often numbered sequentially in groups totaling less than \$10,000 or \$3,000; bear the same handwriting (for the most part) and often the same small mark, stamp, or initials; or appear to have been purchased at numerous places on the same or different days.

EXHIBIT 1-B

2014 NAICS

SEPTEMBER, 2014

The following North American Industry Classification System (NAICS) codes are taken from the U.S. Census Bureau 2012 NAICS and have been authorized by Financial Crimes Enforcement Network (FinCEN) for use with the BSA E-Filing System. The use of any additional NAICS code with the BSA E-Filing System is prohibited.

Accommodation and Food Services		Hospitals	622
Accommodation	721	Medical and Diagnostic Laboratories	6215
Food Services and Drinking Places	722	Nursing and Residential Care Facilities	623
Administrative and Support and Waste Management and Remediation		Nursing Care Facilities	6231
Administrative and Support Services	561	Offices of Dentists	6212
Waste Management and Remediation Services	562	Offices of Other Health Practitioners	6213
Agriculture, Forestry, Fishing and Hunting		Offices of Physicians	6211
Animal Production	112	Other Ambulatory Health Care Services	6219
Crop Production	111	Other Residential Care Facilities	6239
Fishing, Hunting and Trapping	114	Outpatient Care Centers	6214
Forestry and Logging	113	Psychiatric and Substance Abuse Hospitals	6222
Support Activities for Agriculture and Forestry	115	Residential Mental Retardation, Mental Health and Substance Abuse Facilities	6232
Arts, Entertainment, and Recreation		Social Assistance	624
Amusement Parks and Arcades	7131	Specialty (except Psychiatric and Substance Abuse) Hospitals	6223
Amusement, Gambling, and Recreation Industries	713	Information	
Gambling Industries	7132	Broadcasting (except Internet)	515
Museums, Historical Sites, and Similar Institutions	712	Data Processing, Hosting and Related Services	518
Other Amusement and Recreation Industries	7139	Motion Picture and Sound Recording Industries	512
Performing Arts, Spectator Sports, and Related Industries	711	Other Information Services	519
Construction		Other Telecommunications	5179
Construction of Buildings	236	Publishing Industries (except Internet)	511
Heavy and Civil Engineering Construction	237	Satellite Telecommunications	5174
Specialty Trade Contractors	238	Telecommunications	517
Educational Services		Wired Telecommunications Carriers	5171
Educational Services	611	Wireless Telecommunications Carriers (except Satellite)	5172
Finance and Insurance		Management of Companies and Enterprises	
Activities Related to Credit Intermediation	5223	Management of Companies and Enterprises	551
Agencies, Brokerages, and Other Insurance Related Activities	5242	Manufacturing	
Credit Intermediation and Related Activities	522	Apparel Manufacturing	315
Depository Credit Intermediation	5221	Beverage and Tobacco Product Manufacturing	312
Funds, Trusts, and Other Financial Vehicles	525	Chemical Manufacturing	325
Insurance and Employee Benefit Funds	5251	Computer and Electronic Product Manufacturing	334
Insurance Carriers	5241	Electrical Equipment, Appliance, and Component Manufacturing	335
Insurance Carriers and Related Activities	524	Fabricated Metal Product Manufacturing	332
Monetary Authorities-Central Bank	521	Food Manufacturing	311
Mortgage and nonmortgage loan brokers'	52231	Furniture and Related Product Manufacturing	337
Other Financial Investment Activities	5239	Leather and Allied Product Manufacturing	316
Other Investment Pools and Funds	5259	Machinery Manufacturing	333
Securities and Commodity Contracts Intermediation and Brokerage	5231	Miscellaneous Manufacturing	339
Securities and Commodity Exchanges	5232	Nonmetallic Mineral Product Manufacturing	327
Securities, Commodity Contracts, and Other Financial Investments and Related Activities	523	Paper Manufacturing	322
Health Care and Social Assistance		Petroleum and Coal Products Manufacturing	324
Ambulatory Health Care Services	621	Plastics and Rubber Products Manufacturing	326
Community Care Facilities for the Elderly	6233	Primary Metal Manufacturing	331
General Medical and Surgical Hospitals	6221	Printing and Related Support Activities	323
Home Health Care Services	6216	Textile Mills	313
		Textile Product Mills	314
		Transportation Equipment Manufacturing	336
		Wood Product Manufacturing	321
		Mining, Quarrying, and Oil and Gas Extraction	
		Mining (except Oil and Gas)	212
		Oil and Gas Extraction	211
		Support Activities for Mining	213

EXHIBIT 1-B

2014 NAICS

SEPTEMBER, 2014

Professional, Scientific, and Technical Services			
Accounting, Tax Preparation, Bookkeeping, and Payroll Services	5412	Couriers and Messengers	492
Advertising, Public Relations, and Related Services	5418	Local Messengers and Local Delivery	4922
Architectural, Engineering, and Related Services	5413	Other Pipeline Transportation	4869
Computer Systems Design and Related Services	5415	Pipeline Transportation	486
Legal Services	5411	Pipeline Transportation of Crude Oil	4861
Management, Scientific, and Technical Consulting Services	5416	Pipeline Transportation of Natural Gas	4862
Other Professional, Scientific, and Technical Services	5419	Postal Service	491
Professional, Scientific, and Technical Services	541	Rail Transportation	482
Scientific Research and Development Services	5417	Scenic and Sightseeing Transportation	487
Specialized Design Services	5414	Support Activities for Transportation	488
		Transit and Ground Passenger Transportation	485
		Truck Transportation	484
		Warehousing and Storage	493
		Water Transportation	483
Public Administration		Utilities	
Administration of Economic Programs	926	Utilities	221
Administration of Environmental Quality Programs	924		
Administration of Housing Programs, Urban Planning, and Community Development	925		
Administration of Human Resource Programs	923	Wholesale Trade	
Executive, Legislative, and Other General Government Support	921	Apparel, Piece Goods, and Notions Merchant Wholesalers	4243
Justice, Public Order, and Safety Activities	922	Beer, Wine, and Distilled Alcoholic Beverage Merchant Wholesalers	4248
National Security and International Affairs	928	Chemical and Allied Products Merchant Wholesalers	4246
Space Research and Technology	927	Drugs and Druggists' Sundries Merchant Wholesalers	4242
		Electrical and Electronic Goods Merchant Wholesalers	4236
		Farm Product Raw Material Merchant Wholesalers	4245
		Furniture and Home Furnishing Merchant Wholesalers	4232
		Grocery and Related Product Merchant Wholesalers	4244
		Hardware, and Plumbing and Heating Equipment and Supplies Merchant Wholesalers	4237
		Lumber and Other Construction Materials Merchant Wholesalers	4233
		Machinery, Equipment, and Supplies Merchant Wholesalers	4238
		Merchant Wholesalers, Durable Goods	423
		Merchant Wholesalers, Nondurable Goods	424
		Metal and Mineral (except Petroleum) Merchant Wholesalers	4235
		Miscellaneous Durable Goods Merchant Wholesalers	4239
		Miscellaneous Nondurable Goods Merchant Wholesalers	4249
		Motor Vehicle and Motor Vehicle Parts and Supplies Merchant Wholesalers	4231
		Paper and Paper Product Merchant Wholesalers	4241
		Petroleum and Petroleum Products Merchant Wholesalers	4247
		Professional and Commercial Equipment and Supplies Merchant Wholesalers	4234
		Wholesale Electronic Markets and Agents and Brokers	425
Real Estate and Rental and Leasing		Other Services (except Public Administration)	
Activities Related to Real Estate	5313	Business, Professional, Labor, Political, and Similar Organizations	8139
Automotive Equipment Rental and Leasing	5321	Civic and Social Organizations	8134
Commercial and Industrial Machinery and Equipment Rental and Leasing	5324	Grantmaking and Giving Services	8132
Consumer Goods Rental	5322	Personal and Laundry Services	812
General Rental Centers	5323	Private Households	814
Lessors of Nonfinancial Intangible Assets (except Copyrighted Works)	533	Religious Organizations	8131
Lessors of Real Estate	5311	Religious, Grantmaking, Civic, Professional, and Similar Organizations	813
Offices of Real Estate Agents and Brokers	5312	Repair and Maintenance	811
Real Estate	531	Social Advocacy Organizations	8133
Rental and Leasing Services	532		
Retail Trade			
Automobile Dealers	4411		
Automotive Parts, Accessories, and Tire Stores	4413		
Building Material and Garden Equipment and Supplies Dealers	444		
Clothing and Clothing Accessories Stores	448		
Clothing Stores	4481		
Direct Selling Establishments	4543		
Electronic Shopping and Mail-Order Houses	4541		
Electronics and Appliance Stores	443		
Food and Beverage Stores	445		
Furniture and Home Furnishings Stores	442		
Gasoline Stations	447		
General Merchandise Stores	452		
Health and Personal Care Stores	446		
Jewelry, Luggage, and Leather Goods Stores	4483		
Miscellaneous Store Retailers	453		
Motor Vehicle and Parts Dealers	441		
Nonstore Retailers	454		
Other Motor Vehicle Dealers	4412		
Shoe Stores	4482		
Sporting Goods, Hobby, Book, and Music Stores	451		
Vending Machine Operators	4542		
Transportation and Warehousing			
Air Transportation	481		
Couriers and Express Delivery Services	4921		

* NAICS code 52231 added in September 2014.



FIN-2014-A007

August 11, 2014

Advisory

Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance

BSA/AML shortcomings have triggered recent civil and criminal enforcement actions — FinCEN seeks to highlight the importance of a strong culture of BSA/AML compliance for senior management, leadership and owners of all financial institutions subject to FinCEN's regulations regardless of size or industry sector.

Shortcomings identified in recent Anti-Money Laundering (AML) enforcement actions confirm that the culture of an organization is critical to its compliance. Although enforcement actions are specific to the subject financial institution and the characteristics of the situation, certain general lessons could be gleaned from these actions that could be instructive to the leadership of all financial institutions required to comply with the Bank Secrecy Act (BSA). Accordingly, the Financial Crimes Enforcement Network (FinCEN) issues this Advisory to highlight general principles illustrating how financial institutions and their leadership may improve and strengthen organizational compliance with BSA obligations.¹

Regardless of its size and business model, a financial institution with a poor culture of compliance is likely to have shortcomings in its BSA/AML program. A financial institution can strengthen its BSA/AML compliance culture by ensuring that (1) its leadership actively supports and understands compliance efforts; (2) efforts to manage and mitigate BSA/AML deficiencies and risks are not compromised by revenue interests; (3) relevant information from the various departments within the organization is shared with compliance staff to further BSA/AML efforts; (4) the institution devotes adequate resources to its compliance function; (5) the compliance program is effective by, among other things,

1. This advisory does not change any existing expectations or obligations under BSA/AML requirements. Similarly, this advisory is not intended to change or otherwise interpret regulatory expectations or obligations that financial institutions may have outside of the BSA. Financial institutions should also be familiar with and follow the guidance and requirements of their federal functional regulator and Self-Regulatory Organization (SRO) regarding any other applicable compliance obligations, such as those relating to safety and soundness, governance programs and enterprise-wide compliance. This advisory should not be interpreted in a manner inconsistent with previous guidance issued by FinCEN or any federal functional regulator or SRO. Financial institutions may refer to detailed guidance on FinCEN's website organized by industry as well as to guidance provided by their appropriate federal functional regulator or SRO.

EXHIBIT 1-B

FINCEN ADVISORY

ensuring that it is tested by an independent and competent party; and (6) its leadership and staff understand the purpose of its BSA/AML efforts and how its reporting is used. This advisory describes each of these areas in more detail

below. Financial institutions should consider how to incorporate the guidance outlined in this advisory in a manner that is commensurate with their risk profile and business model.

FinCEN Guidance to Financial Institutions

Leadership Should Be Engaged

A financial institution's leadership is responsible for performance in all areas of the institution including compliance with the BSA. As applicable, an institution's leadership may include its board of directors, senior and executive management, owners and operators. These leaders are responsible for understanding an institution's responsibilities regarding compliance with the BSA and creating a culture of compliance at that institution. The commitment of an organization's leaders should be visible within the organization, as such commitment influences the attitudes of others within the organization.

For a BSA/AML compliance program to be effective, it should have the demonstrable support of the leadership (as appropriate based on the financial institution's size and structure). The institution's leaders should also receive periodic BSA/AML training that is tailored to their roles. In addition to supporting a culture of compliance, an appropriate understanding of BSA/AML obligations and compliance will help an organization's leadership make informed decisions with regard to the allocation of resources to the BSA/AML function. The leaders of the organization should also remain informed of the state of BSA/AML compliance within the institution.

Compliance Should Not Be Compromised By Revenue Interests

Compliance staff should be empowered with sufficient authority and autonomy to implement an institution's AML program. An institution's interest in revenue should not compromise efforts to effectively manage and mitigate BSA/AML deficiencies and risks, including submission of appropriate and accurate reports to FinCEN. An effective governance structure should allow for the BSA/AML compliance function to work independently and to take any appropriate actions to address and mitigate any risks that may arise from an institution's business line and to file any necessary reports, such as Suspicious Activity Reports (SARs).

For example, for Money Services Businesses (MSBs), principal MSBs often derive a significant percentage of their revenue from the activity of their agents. When principal MSBs learn of possible inappropriate activity by an agent, the activity should be investigated thoroughly and appropriate action taken regardless of the impact on revenue. The findings from the investigation should be considered when determining whether an agent is terminated, and the sales unit should not have express or implied authority to veto the decision because of the agent's sales activity.

Information Should Be Shared Throughout the Organization

Several recent enforcement actions noted that the subject institution had relevant information in its possession that was not made available to BSA/AML compliance staff. This may have resulted from a lack of an appropriate mechanism for sharing information, a lack of appreciation of the significance or relevance of the information to BSA/AML compliance or an intentional decision to prevent compliance officers or staff from having access to the information.

There is information in various departments within a financial institution that may be useful and should be shared with the compliance staff. For example, information developed by those in the organization combating and preventing fraud could also assist a financial institution in complying with its BSA/AML obligations. Similarly, legal departments should alert compliance departments to subpoenas received issued by government agencies to trigger reviews of related customers' risk ratings and account activity for suspicious transactions. Additionally, in a larger organization there may be multiple affiliated institutions that could benefit from sharing of relevant information across the organization.²

For instance, in the gaming sector, this principle can be applied to casinos that develop significant information on their gaming customers for purposes of marketing or extending credit. However that information is derived, it should be provided to the compliance staff to assist in conducting customer due diligence and monitoring customers for suspicious activity. This principle can also be applied to mutual funds that receive transaction information about their customers through a frequent trading monitoring program, or other similar efforts. In those cases, information that could further the BSA/AML compliance efforts of the mutual fund should also be shared with mutual fund staff engaged in BSA/AML compliance.

Leadership Should Provide Adequate Human and Technological Resources

A required element of any BSA/AML compliance program is the designation of an individual responsible for coordinating and monitoring day-to-day compliance with the BSA. The individual should be knowledgeable of the BSA and have sufficient authority to administer the program. For the program to be effective, the institution should devote appropriate support staff to its BSA/AML compliance program based on its risk profile.

The failure of an institution's leaders to devote sufficient staff to the BSA/AML compliance function may lead to other failures. For example, depository institutions, as well as other types of financial institutions, generally have staff that review alerts generated by transaction monitoring systems. Devoting insufficient staff or other resources to this function may result

2. Likewise, information sharing between financial institutions can often result in a more comprehensive picture of suspicious activity and more useful reporting to law enforcement. For additional information about the benefits of the 314(b) information sharing program, see the [Section 314\(b\) Fact Sheet](#).

FINCEN ADVISORY

in alerts not being reasonably designed to capture appropriate risks or being dismissed improperly, or create a backlog of alerts that may result in the untimely reporting of suspicious activity.

Appropriate technological resources should also be allocated to BSA/AML compliance. Institutions with higher risk profiles, including those with substantially higher volumes of activity, may need to utilize automated systems for identifying and monitoring suspicious activity.

The Program Should Be Effective and Tested By an Independent and Competent Party

Appropriate involvement of a financial institution's leadership should be, at a minimum, commensurate with the institution's level of BSA/AML risk exposure. Appropriate leadership involvement allows the BSA/AML function to implement an effective compliance program. Components of an effective BSA/AML compliance program additionally include a proper ongoing risk assessment, sound risk-based customer due diligence, appropriate detection and reporting of suspicious activity and independent program testing.³

While recognizing that all the components of an effective compliance program are important, FinCEN stresses the independence that the testing of a compliance program should have. A financial institution's leadership should ensure that the party testing the program (whether internal or external) is independent, qualified, unbiased and does not have conflicting business interests that may influence the outcome of the compliance program test. Safeguarding the integrity and independence of the compliance program testing enables an institution to locate and take appropriate corrective actions to address BSA/AML deficiencies.

Leadership and Staff Should Understand How Their BSA Reports are Used

Finally, leadership and staff at all levels in a financial institution should understand that they are not simply generating reports for the sake of compliance, but rather recognize the purpose that BSA reports serve and how the information is used. The reporting and the transparency that financial institutions provide under FinCEN's regulations result in some of the most important information available to law enforcement and others safeguarding the nation. It is used to confront serious threats, including terrorist organizations, rogue nations, weapons of mass destruction (WMD) proliferators, foreign corruption and, increasingly, some cyber related threats. The reporting that financial institutions provide also assists in the fight against transnational criminal organizations including those involved in drug trafficking and massive fraud schemes targeting the U.S. government, our businesses and our people.

3. BSA/AML compliance professionals should be familiar with the guidance that has been made available by the federal functional regulators, SROs and FinCEN to assist financial institutions with developing an effective compliance program. Such guidance includes, but is not limited to, industry specific examination manuals and other regulatory guidance.

FINCEN ADVISORY

That same information may also help an institution protect itself and aid law enforcement in protecting the institution from bad actors, including insider threats, frauds and cyber-related threats such as spear phishing, account takeovers and distributed denial of service attacks, when such reports are filed.

Additionally, the very existence of BSA regulations has a deterrent effect on those who would abuse the financial system. The certainty of a Currency Transaction Report (CTR) filing and the mere possibility of a SAR filing force illicit actors to behave in ways that expose them to scrutiny and capture.

The reporting that financial institutions provide is used to:

- **Serve as tips to initiate investigations:** BSA reports contribute critical information that is routinely analyzed, resulting in the identification of suspected criminal activity and the initiation of investigations. For instance, approximately 100 SAR review teams across the country bring together investigators and prosecutors from different governmental agencies to review reports related to their geographic area of responsibility and use the information therein to initiate criminal investigations, where appropriate.
- **Expand existing investigations:** The reporting aids in expanding the scope of ongoing investigations by pointing to the identities of previously unknown subjects, exposing accounts and hidden financial relationships, or revealing other information such as common addresses or phone numbers that connect seemingly unrelated participants in a criminal or terrorist organization and, in some cases, even confirming the location of suspects. Nearly 11,000 federal, state and local law enforcement and regulatory users conduct roughly 30,000 searches per day of the reporting using FinCEN's information technology tool for making queries about known subjects.
- **Promote international information exchange:** The Egmont Group has developed mechanisms for the rapid exchange of sensitive information between 146 Financial Intelligence Units (FIUs) around the world. In FY 2014, based on current trends, it is estimated that FinCEN will receive approximately 1,300 incoming Egmont requests from foreign FIUs seeking information derived from BSA reporting and make approximately 700 outgoing Egmont requests on behalf of U.S. law enforcement agencies seeking similar information from foreign FIUs.
- **Identify significant relationships, trends and patterns:** BSA reports unmask the relationships between illicit actors and their financing networks, enabling law enforcement to target the underlying conduct of concern, and to use forfeiture and sanctions to disrupt their ability to operate and finance their illicit conduct. BSA reports also reveal trends and patterns on criminal, terrorist and other emerging threats that enable law enforcement to focus limited resources.

EXHIBIT 1-B

F I N C E N A D V I S O R Y

Understanding and communicating the context and the purpose of FinCEN's BSA/AML regime is as important to a financial institution's culture as understanding its underlying requirements, and financial institutions should consider including such information as part of their ongoing training requirement. Information on how BSA reports are used can be found on FinCEN's website and is routinely shared through numerous public-private training events involving FinCEN and its many law enforcement partners.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at (800) 767-2825 or (703) 905-3591. *Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).* The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

EXHIBIT 1-B

Prepared Remarks of FinCEN Director Kenneth A. Blanco, deliv...

<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-d...>

Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered virtually at the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference

December 10, 2020

Prepared Remarks

Kenneth A. Blanco

Director

Financial Crimes Enforcement Network

American Bankers Association/American Bar Association

Financial Crimes Enforcement Conference

December 10, 2020

VIRTUAL

Thank you, Rob, for that kind and generous introduction. Good morning, everyone. I am delighted to be joining you all again for the ABA/ABA's annual Financial Crimes Enforcement Conference. While so much has changed since last year, I am grateful to be able to join you virtually. One thing I will certainly miss is being on stage with Rob Rowe, something we have done together for the past several years.

I think it is always important to remind all of you that the work you do every day protects our national security; it keeps us, our families, and our communities safe from harm—especially the most vulnerable in our society. To be clear, this has never been more true than it is now in the face of this global pandemic—where we see so many bad actors taking advantage of (or trying to take advantage of) this world crisis—just shameful and despicable.

I know you all have been working tirelessly to serve your customers and keep your workforce safe in this unprecedented environment. We are doing the same at FinCEN. So today, I would like to discuss our COVID-19 response, as well as the ANPRM on effectiveness, and touch on some other important work FinCEN has accomplished this year, all of which impacts you in your important work.

But before I do that, I would like to announce some important guidance that FinCEN is issuing today which represents much needed clarity regarding how financial institutions may fully utilize FinCEN's 314(b) information sharing program.

Information Sharing

Information sharing among financial institutions through 314(b) is critical to identifying, reporting, and preventing crime and bad acts. It is an important part of how we protect our national security. It can also help financial institutions enhance compliance with their AML/CFT requirements.

EXHIBIT 1-B

Prepared Remarks of FinCEN Director Kenneth A. Blanco, deliv...

<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-d...>

Frankly, many have been calling for clarity in this area for a long time—I have been one of those most vocal about this needed change. In fact, I have spoken directly to several of you in attendance today and your perspectives have informed our work quite a bit. Thank you for your contributions to this effort.

The guidance we are announcing today, in a new 314(b) Fact Sheet (<https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf>), is the result of the feedback provided by financial institutions and through our own experiences at FinCEN. It is intended to clarify in greater detail the circumstances where 314(b) applies, with the hope of enhancing participation and utility of the 314(b) program.

The main themes of today's 314(b) Fact Sheet are as follows:

1. Financial institutions may share under Section 314(b) information relating to activities that they suspect may involve possible terrorist financing or money laundering. This includes, but is not limited to, information about activities they suspect involve the proceeds of a specified unlawful activity (SUA). Importantly, our guidance clarifies that:
 - Financial institutions do not need to have specific information that these activities directly relate to proceeds of an SUA, or to have identified specific proceeds of an SUA being laundered.
 - Financial institutions do not need to have made a conclusive determination that the activity is suspicious.
 - Financial institutions may share information about activities as described, even if such activities do not constitute a "transaction." This includes, for example, an attempted transaction, or an attempt to induce others to engage in a transaction. This clarification is significant and addresses some uncertainty with sharing incidents involving possible fraud, cybercrime, and other predicate offenses when financial institutions suspect those offenses may involve terrorist acts or money laundering activities.
 - In addition, the guidance notes that there is no limitation under Section 314(b) on the sharing of personally identifiable information, or the type or medium of information that can be shared (to include sharing information verbally).

We also offer some important clarification regarding who may register as an association of financial institutions and under what terms. This includes:

2. An entity that is not itself a financial institution may form and operate an association of financial institutions whose members can use 314(b). Notably, this includes compliance service providers; and
3. An unincorporated association of financial institutions, governed by a contract between its financial institutions' members, may engage in information sharing under Section 314(b).

We are incredibly excited about this guidance and we hope you all see it as a noteworthy example of FinCEN finding ways to work directly with industry to make our regulatory framework more efficient and effective.

When it comes to protecting our communities and preventing crimes and bad acts, we are all partners in the fight. FinCEN is committed to seeking ways to make that fight more effective and efficient for us all. I hope you view today's announcement as making good on that commitment.

The new 314(b) Fact Sheet is available on FinCEN's website. I ask that all financial institutions take the time to review the Fact Sheet, and let us know if they have any questions. And, of course, FinCEN strongly encourages financial institutions to participate in the 314(b) program.

Advance Notice of Proposed Rulemaking (ANPRM)

Now, let us turn to FinCEN's ANPRM (<https://www.fincen.gov/news/news-releases/fincen-seeks-comments-enhancing-effectiveness-anti-money-laundering-programs>) on effectiveness, which represents a significant achievement in our collective anti-money laundering/counter-financing of terrorism (AML/CFT) efforts over the past year. The ANPRM, issued on September 17, is the result of some really important work done by the Bank Secrecy Act Advisory Group's (BSAAG's) Anti-Money-Laundering Effectiveness Working Group.

This group worked collaboratively—really long hours (10 hour days, sometimes back to back), many commuting to DC from across the country—throughout 2019 and 2020—to identify regulatory initiatives that would allow financial institutions to reallocate resources to better focus on national AML priorities set by government authorities, increase information sharing and public-private partnerships, and leverage new technologies and risk-management techniques—and thus increase the

EXHIBIT 1-B

Prepared Remarks of FinCEN Director Kenneth A. Blanco, deliv...

<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-d...>

effectiveness and efficiency of the nation's AML regime.

The ANPRM is an outgrowth of their recommendations and was a meaningful, public invitation to all of you to weigh in, provide your perspectives, your experience, and your insights on questions such as:

How do we achieve, measure, and examine for, effectiveness in our AML regime? How do we work together to adequately provide the flexibility industry needs to allocate resources according to risk and priorities to help government authorities with actionable information? How do we communicate our needs and information to each other and feel confident that something will come of it?

And on a tactical level with respect to the ANPRM, does it help our collective mission if we provide an explicit definition of effectiveness? We know many of you already conduct risk assessments on a regular basis—but is it significant if we make it an explicit requirement? Will it help you if FinCEN provides you with strategic AML priorities? Will strategic AML priorities help you allocate your resources most effectively and efficiently? What considerations are specific to your institution or your industry?

But beyond these formal questions at the end of the ANPRM, we also invited you to think about the modernization of the AML regime in general and provide us with that feedback too. There is a lot of ongoing work, and this ANPRM is but one component. We talk about developing and focusing on priorities, reallocating compliance resources, modernizing and streamlining monitoring and reporting practices, enhancing information sharing, and advancing and maximizing regulatory and technological innovations.

The effectiveness ANPRM is just the beginning. Much more work needs to be done and we all know that it will be challenging. These things are not easy. But we need your insight and thoughtful consideration. Since the comment period closed on November 16, FinCEN has been busy going through the 108 comments received.

COVID-19 Response

I would now like to turn to FinCEN's COVID-19 response. As the pandemic began to unfold, we all had to pivot, and quickly. As many of you know, FinCEN has an incredibly important mission—one that profoundly impacts people's lives, and we cannot stop in the face of crisis or challenges.

We remain laser-focused on the effects COVID-19 has had on a range of illicit threats across the world. With businesses and individuals in our country and across the globe facing new and challenging circumstances, the entire AML community has had to adapt in real time.

FinCEN immediately aligned several strategic efforts to assist financial institutions and others impacted by the pandemic.

Expansion of Rapid Response Program

FinCEN quickly expanded its Rapid Response Program. Under the program, when U.S. law enforcement receives a business email compromise (BEC) complaint from either a victim or an interested third party like a financial institution, the relevant information is forwarded to FinCEN, where we move quickly to track and make contact with foreign jurisdictions to assist in recovering the funds.

Our efforts now support law enforcement and financial institutions in the recovery of funds stolen via fraud and other crimes related to COVID-19. Since the beginning of the pandemic, FinCEN has supported several requests from federal, state, and even international law enforcement agencies, and our contributions have aided in the successful recovery of almost \$325 million stolen in COVID-19 related fraud.

The work we are doing together with our law enforcement authorities in real-time is making a difference. In one publicized case, authorities of a foreign government were defrauded into purchasing COVID-19 related personal protective equipment from a small medical company for over \$300 million.

Financial institutions became suspicious of the account activity and alerted the United States Secret Service, who began its investigation. Working together with FinCEN and foreign law enforcement authorities, the investigation revealed that the company never had any masks to sell and that the deal was fraudulent.

EXHIBIT 1-B

Prepared Remarks of FinCEN Director Kenneth A. Blanco, deliv...

<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-d...>

Due to the quick actions by all involved, there was a 100% recovery of the total amount of the wired funds.

Guidance to Financial Institutions

FinCEN also issued Notices to financial institutions—one on March 16, one on April 3, and another on May 18—advising them to remain alert to fraudulent, COVID-19 related transactions, and providing instructions on BSA filing requirements.

FinCEN worked hard on the Coronavirus Aid, Relief, and Economic Security (CARES) Act with other Treasury components as it relates to our area, the BSA, and we are committed to promoting the success of the CARES Act, including the need to facilitate expeditious disbursement of CARES Act funds.

The mission for all of us in the financial space is to get funds to the intended recipients—many who badly need it for their financial survival—not to criminals and fraudsters.

FinCEN's Regulatory Support Section has responded to more than 550 inquiries relating to BSA obligations during COVID-19 and the Paycheck Protection Program (PPP) under the CARES Act.

More specifically, these inquiries included notifications from institutions on delays in filing of BSA reports; requests for additional clarification on the SAR filing expectations in accordance with FinCEN's COVID-19 advisories; and questions on how to return relief funds to the issuing government agencies after determining the funds were obtained fraudulently.

In addition, immediately after the PPP was established, FinCEN received many inquiries from institutions seeking clarification on their Customer Due Diligence - Beneficial Ownership requirements for new accounts.

In response, FinCEN issued FAQs (https://www.fincen.gov/sites/default/files/2020-04/Paycheck_Protection_Program_FAQs.pdf) to answer these questions, which greatly reduced the number of inquiries on this topic.

FinCEN Advisories

FinCEN immediately started tracking and publishing trends on COVID-19 fraud and financial crime based on BSA data, while working with our law enforcement partners.

Since May, we have published multiple advisories related to COVID-19 medical fraud, imposter scams, cyber-enabled crime, and defrauding of the unemployment insurance system that has been such a lifeline to so many over the past eight months. Let me mention them briefly, as they are very important.

Medical Fraud: Our first advisory, issued May 18, described **medical fraud** (<https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf>) in the wake of the pandemic—criminals selling fake vaccines and cures, price gouging on medical equipment, and the fraudulent collection of medical donations that criminals divert to their personal use, among other typologies.

For instance, non-delivery scams, where a customer pays a company for goods the customer will never receive, became prevalent. In these schemes, fraudulent companies advertise test kits, masks, drugs, and other goods they never intend to deliver, and sometimes never possess at all. Victims can include unsuspecting companies, hospitals, governments, and consumers. These fraudulent transactions occur through websites, robocalls, or on the Darknet.

Imposter Scams and Money Mules: On July 7, FinCEN issued its second advisory, alerting financial institutions to financial red flags of **imposter scams and money mules** (https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf).

In imposter scams, individuals pose as officials or representatives from government agencies or non-profit groups, like the Internal Revenue Service, the Centers for Disease Control and Prevention, or the World Health Organization to try to elicit personal information to defraud victims.

EXHIBIT 1-B

Prepared Remarks of FinCEN Director Kenneth A. Blanco, deliv...

<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-d...>

In money mule schemes, victims can be wittingly or unwittingly recruited to be “money mules” through romance, good-Samaritan, work-from-home, and unemployment insurance schemes. For instance, recruiters from a seemingly legitimate charity approach victims with an offer of work-from-home employment. Once “employed,” the money mule is asked to solicit donations for the charity, and send and receive funds from personal accounts to a fraudulent organization.

In other variations, criminals seek out individuals who are not looking for employment, but are tricked into becoming a money mule through romance scams or helping someone overseas, such as a U.S. service member, a U.S. citizen living abroad, or a U.S. citizen who cannot return to the United States because of COVID-19 travel restrictions. In these schemes, the scammers ask targets to send or receive money on the scammer’s behalf.

Cybercrime and Cyber-Enabled Crime: On July 30, FinCEN issued a third advisory to help financial institutions identify cybercrime and cyber-enabled crime (<https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf>) exploiting the COVID pandemic.

FinCEN and its law enforcement partners have seen thousands of reports of cybercrimes exploiting COVID-19, oftentimes targeting vulnerable individuals, such as the elderly, as well as companies. Leveraging COVID-19 lures, cyber-criminals and malicious state actors are using wide-scale phishing campaigns, malware, extortion, BEC, and other exploits against remote platforms to steal credentials, conduct fraud, and spread disinformation.

FinCEN also has observed ransomware incidents likely exploiting the significant transition to remote operations across organizations providing critical services, which have been growing in scope and severity since even before the pandemic. These risks are growing and becoming more prevalent during the pandemic. For example, fraudsters are advertising services instructing individuals on how to apply for unemployment insurance, the PPP, and the Small Business Administration’s Economic Injury Disaster Loan (EIDL) program on social media platforms often for a fee.

Dark web vendors are selling similar data, instructions, and complete packages of personally identifiable information (PII) to apply for PPP and EIDL funds. Cyber threat actors also are leveraging BEC attacks to defraud businesses and redirect small business loan stimulus disbursements to bank accounts belonging to the attackers.

We also see an increase in cybercriminals’ targeting of vulnerabilities in remote applications and functions—including virtual private networks (VPNs) and remote desktop protocol (RDP) exploits—to steal sensitive information, compromise transactions, and more.

We highlighted for financial institutions to remain vigilant against attacks that target their onboarding and authentication processes, including “deepfakes” that manipulate digital images or videos, or account takeovers that are facilitated by credential stuffing attacks. We see criminal activity seeking to undermine critical parts of the AML/CFT framework, including the regulatory obligations generally referred to as the “know your customer” process, especially in increasingly remote work environments.

We also see illicit actors using virtual currency to launder proceeds and buy and sell cyber tools and services on Darknet marketplaces, such as exploit kits or hacking services. Cybercriminals also have advertised illicit wares for virtual currency on the dark web, such as fraudulent COVID-19 cures, and live virus samples.

Unemployment Insurance Fraud: On October 13, FinCEN issued its advisory on pandemic-related unemployment insurance (UI) fraud (<https://www.fincen.gov/sites/default/files/shared/Advisory%20Unemployment%20Insurance%20COVID%2019%20508%20Final.pdf>), which contains financial red flag indicators and information on reporting suspicious activity.

FinCEN is observing numerous forms of UI fraud, including applicants falsely claiming that they work for a legitimate company or creating fictitious companies and then submitting UI claims, or applicants misrepresenting their income or claiming UI payments while receiving unreported wages. In identity fraud, fraudsters often use the dark web to execute their plans. They coordinate plans against various state unemployment programs on dark web forums, and discuss direct attacks on states with weaker controls.

Fraudsters also use dark web forums to sell previously hacked PII and share instructions on how to use the data to obtain

EXHIBIT 1-B

Prepared Remarks of FinCEN Director Kenneth A. Blanco, deliv...

<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-d...>

unemployment and other benefits. Law enforcement also has noted fake websites that appear legitimate to trick victims into making fraudulent donations or entering PII and confidential banking data. Fraud actors harvest and exploit this data to apply for unemployment benefits under the victims' names.

I encourage you to read these advisories. All of our advisories and guidance related to COVID-19 are housed prominently on a dedicated page on FinCEN's website (<https://www.fincen.gov/coronavirus>).

Charities Fact Sheet

On November 19, FinCEN and the Federal Banking Agencies issued a joint fact sheet (<https://www.fincen.gov/news/news-releases/fincen-and-federal-banking-agencies-clarify-ba-due-diligence-expectations>) to provide clarity to banks on how to apply a risk-based approach to charities and other non-profit organizations consistent with customer due diligence requirements.

The joint fact sheet highlights the importance of ensuring that legitimate charities have access to financial services and can transmit funds through legitimate and transparent channels, especially during the COVID-19 pandemic.

Banks are encouraged to manage customer relationships and mitigate risks on a case-by-case basis rather than declining to provide banking services to entire categories of customers. The joint fact sheet also reminds banks that the U.S. government does not view the charitable sector as a whole as presenting a uniform or unacceptably high risk of being used or exploited for money laundering, terrorist financing, or sanctions violations.

COVID-related SAR Filings

I do want to take a few moments to provide feedback on some of what we are seeing in your SAR reporting related to COVID-19 and the stimulus programs.

Your reporting is making a difference and has been incredibly helpful to us at FinCEN and to law enforcement working to combat the criminals trying to exploit this pandemic. Many of the trends below relate to the advisories I have already mentioned. We use SAR reporting as one way to identify prevalent typologies of illicit activity and ensure that information is broadly disseminated among financial institutions.

From February 1 to November 30, financial institutions have filed with FinCEN over 147,000 SARs referencing COVID-19 and the stimulus programs. Breaking this figure down by financial industry:

- **Depository Institutions (Banks):** almost 102,000 (69 percent)
- **Credit Unions:** 21,000 (about 14 percent)
- **Money Services Businesses:** almost 9,000 SARs (6 percent)
- **Securities/Futures industry:** 2,000 SARs (1 percent)
- **Casino/Card Clubs:** almost 750 SARs (less than 1 percent)

Different law enforcement teams are investigating fraud in the different government programs, and vague references to "stimulus" or "CARES Act" or "benefit" in SARs hinder our ability to get the information into the hands of the right team. The more specific you are in describing the suspicious activity you see in SARs that you submit to FinCEN, the more useful they are for our law enforcement partners, and the easier and faster it will be to get your SARs to the right investigative team. For example:

- If the suspicious activity is related to an ACH payment from a state unemployment insurance program, please clearly mention **COVID19 UNEMPLOYMENT INSURANCE FRAUD** in field 2 of the SAR (Filing Institution Note to FinCEN) as well as in the narrative. This will make it much easier for your SAR to get to law enforcement teams working with the states on unemployment fraud.
- Or if the activity involves a counterfeit check or ACH payment for the EIDL program, please clearly mention **COVID19 EIDL FUNDS FRAUD** in field 2 of the SAR and state this in the narrative, as there are specific prosecutorial teams working on EIDL fraud.

I want to thank each of you and encourage you to keep up the great work with your reporting. Your efforts are not going

EXHIBIT 1-B

Prepared Remarks of FinCEN Director Kenneth A. Blanco, deliv...

<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-d...>

unnoticed and they are helping to keep our nation, communities, and families safe from harm.

Rulemakings

I know I have already covered a great deal of ground today, but I wanted to briefly mention a few additional rulemakings that were issued this year.

Gap Rule: FinCEN published its **Final Rule** (<https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-require-customer-identification-program-anti-money>) on September 15, requiring minimum standards for banks lacking a federal functional regulator. Known as the “Gap rule,” this rulemaking closes a regulatory gap in AML coverage that presented a vulnerability to the U.S. financial system that could be exploited by bad actors.

The rulemaking requires AML standards for state-chartered, non-depository trust companies; non-federally insured credit unions; private banks; non-federally insured state banks and savings associations; and international banking entities. This rulemaking will help reduce the temptation for criminals to seek out and exploit banks subject to less rigorous AML requirements and will help keep our nation, communities, and families safe from harm.

Travel Rule NPRM: FinCEN and the Federal Reserve Board jointly issued a **Notice of Proposed Rulemaking** (<https://www.fincen.gov/news/news-releases/agencies-invite-comment-proposed-rule-under-bank-secrecy-act>) on October 27 that proposes to amend the recordkeeping threshold and travel rule regulations under the BSA.

Under the current recordkeeping and travel rule regulations, financial institutions must collect, retain, and transmit certain information related to transmittals of funds over \$3,000, such as the name and address of the transmitter, any payment instructions received from the transmitter with the transmittal order, the identity of the recipient’s financial institution, and, if provided, the name and address of the recipient.

The proposed rule lowers the applicable threshold from \$3,000 to \$250 for transactions that begin or end outside the United States. The threshold for domestic transactions remains unchanged at \$3,000. The proposed rule also further clarifies that those regulations apply to transactions above the applicable threshold involving convertible virtual currencies, as well as transactions involving digital assets with legal tender status, by clarifying the meaning of “money” as used in certain defined terms.

As described in the NPRM, criminals are using smaller value transfers and CVC to facilitate terrorist financing, narcotics trafficking, and other illicit activities. Defining the term money to explicitly cover CVC and lowering recordkeeping and reporting thresholds for international transactions will help law enforcement and national security authorities safeguard our financial system and protect our communities from harm.

The proposed definitional changes in this NPRM are consistent with existing FinCEN guidance, which makes clear that the regulations requiring the retention and transmittal of records related to transmittals of funds apply to transactions in CVC.

The comment period closed on November 27. FinCEN and our partners at the Federal Reserve Board are reviewing the roughly 2,900 comments received. We appreciate the very thoughtful and comprehensive feedback that industry and members of the public have submitted in response to this NPRM.

Stakeholder Engagement

Despite the pandemic, FinCEN continued its ongoing engagement with its stakeholders. FinCEN convened a virtual FinCEN Exchange on November 12 with representatives from financial institutions, technology firms, third-party service providers, and federal government agencies to discuss growing concerns regarding ransomware, as well as the efforts to curtail it. Topics discussed included ransomware detection and reporting, emerging trends and typologies, and recovery of victims’ funds.

And on October 1, FinCEN issued an advisory, entitled **Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments** (<https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>), providing information on the role of financial intermediaries in payments, ransomware trends and typologies, and related financial red flags. It also provides information on effectively reporting and

EXHIBIT 1-B

Prepared Remarks of FinCEN Director Kenneth A. Blanco, deliv...

<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-d...>

sharing information related to ransomware attacks. Most ransomware payments and associated laundering involve varieties of financial institutions, so you all are well-positioned to help us detect this activity.

The advisory provides useful information on specific types of technical indicators that are useful to investigators for financial institutions to include in their SAR reporting. Let me remind you that you are *required* to provide all relevant information available related to the suspicious activity, and that would include reporting any relevant technical cyber indicators related to a ransomware incident in the structured cyber indicator event fields on the SAR form.

FinCEN has observed underreporting of ransomware incidents, though we hope this advisory and our engagement with industry will improve that reporting and our investigations into this debilitating activity.

In addition, FinCEN's Innovation Hours marked its one-year milestone in July.

We have met with 43 different firms over the course of monthly sessions and another baker's dozen at a regional event held in New York City in partnership with the Office of the Comptroller of the Currency's Innovation Office. These firms have shared their solutions for:

- Tracing and analyzing virtual currency activity and solutions for meeting Funds Transfer and Travel Rule requirements;
- Detecting and responding to cyber incidents;
- Applying artificial intelligence and machine learning;
- Identifying suspicious transactions and activity;
- Creating confidential and secure digital identity solutions, corporate entity resolution, beneficial ownership solutions, and identifying synthetic identities; and
- Using anonymization technology to support the greater use of USA PATRIOT Act Section 314(b) information sharing authorities among banks and other financial institutions.

These are but a few examples of our ongoing efforts. At the end of the day, we all want the same thing: to be effective, to be efficient, to confront and address risk, to prioritize, to protect our national security, and to protect our families and communities from harm.

On a personal note, I hope you and your families have been safe and healthy during this time. Thank you for joining me today.

###

FinCEN Recognizes Law Enforcement Cases Significantly Impacted by Bank Secrecy Act Filings

Contact: Office of Strategic Communications, 703-905-3770

Immediate Release: May 19, 2020

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) announced today the award recipients of the 2020 FinCEN Director's Law Enforcement Awards Program. The annual program recognizes law enforcement agencies that used Bank Secrecy Act (BSA) reporting to successfully pursue and prosecute criminal investigations.

The program demonstrates the critical role that the financial industry's BSA filings play in criminal cases, and underscores the importance of a successful partnership between financial institutions and law enforcement agencies. The investigations being recognized are a key example of how vital BSA reporting is toward keeping our country strong, our financial system secure, and our families safe from harm.

The program is open to all Federal, state, local, and tribal law enforcement agencies. Due to current social distancing guidelines, Director Blanco will present the awards at an official ceremony on October 29, 2020 in Washington, DC.

The seven categories and redacted summaries of the recipients are listed below. The recipients will be publicly identified during the October 2020 ceremony.

SAR Review Task Force: *Federal Bureau of Investigation (FBI)*

Federal Bureau of Investigation (FBI) officials opened an investigation into suspected fraudulent activities of a law firm based on allegations that attorneys with the firm were targeting distressed homeowners with the false promise of loan modification and legal representation. A mortgage fraud task force was established by the FBI. The task force consisted of investigators from the Utah Department of Consumer Protection, the Utah Department Real Estate, the Utah Attorney General's Office, the Special Inspector General for the Troubled Asset Relief Program, the Internal Revenue Service, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the Federal Reserve Board, the Consumer Financial Protection Bureau, the Federal Housing Finance Agency, the United States Attorney's Office, and the FBI.

Employees at the law firm used mass mailings and call centers to attract customers, generating significant upfront fees. Unlicensed individuals and non-attorneys who made outrageous claims about their success rates and turnaround times in order to deceive customers completed the fraudulent loan modification documents. Complaints to state and Federal agencies throughout the country reflected a pattern of fraudulent activities conducted by this group of individuals.

Law enforcement officials' initial investigation led to a search warrant for the law office, resulting in the seizure of over 200 boxes of evidence and the indictment of six individuals on charges of mail fraud, wire fraud, telemarketing fraud, and money laundering. After an initial court hearing, the subjects were released pending trial. While the case was awaiting a trial date, the Fraud Manager at a Utah credit union contacted FBI investigators to inform them of a Bank Secrecy Act (BSA) filing regarding continued fraudulent activity by one of the subjects of this investigation.

As a result of several additional BSA filings by the credit union and information obtained through subsequent interviews, FBI investigators determined that the primary subject and several co-conspirators, while pending trial, had established and began carrying out a boiler-room telemarketing scam. The subjects convinced vulnerable victims, typically elderly individuals, that they would earn significant income by creating a website and advertising for products with an upfront investment of \$1,000 to \$3,000. When the marketing websites inevitably failed, the fraudsters would contact the victims to offer various services costing an additional \$4,000 to \$7,000 to build up the failed businesses. The services were not actually rendered, and were never intended to help the victims launch successful businesses.

The subjects of this investigation also operated a scheme to "sell" free, fictitious Federal grants. Victims of the scheme were convinced to create an LLC, for which they would later receive a \$300,000 to \$600,000 Federal business grant. The victims typically spent between \$30,000 to \$60,000 in business setup fees, educational material, and other dubious items to qualify for this "free" Federal grant. During this fraudulent process, the subjects convinced many victims to open merchant accounts to process credit card transactions on behalf of American businesses. These merchant accounts actually processed the proceeds of this very fraud and several others that the subjects were carrying out.

Throughout the investigation, task force officials analyzed approximately 100 BSA filings, often leading to new subjects and victims located throughout the United States. These filings allowed the task force to connect disparate pieces of information, identify additional subjects and merchant processors, and better understand the magnitude of the fraudulent activity.

The primary subject of this investigation was arrested a second time, his release pending trial was revoked. A second indictment was handed up by a grand jury at the request of the Assistant United States Attorneys prosecuting both cases. With the new charges and overwhelming amount of evidence, the subject reached an agreement to cooperate and agreed to a plea arrangement of 7 years' incarceration for his role in both schemes. This led to the confession and cooperation of several other co-conspirators.

EXHIBIT 1-B

Eight subjects were charged and convicted for conspiracy to commit wire fraud, mail fraud, and money laundering. Total losses exceeded \$42 million and approximately 15,000 victims nationwide were identified. Combined asset forfeiture exceeded \$3.2 million. The United States Attorney's Office-Utah prosecuted this case.

Significant Fraud: *Immigration and Customs Enforcement-Homeland Security Investigations (ICE-HSI)*

This investigation was conducted by Immigration and Customs Enforcement-Homeland Security Investigations, the Internal Revenue Service-Criminal Investigation, and the multi-agency Financial Investigations and Border Crimes Task Force. This investigation began with the analysis of Bank Secrecy Act (BSA) filings indicating activity occurring at the Calexico, California Ports of Entry. The goal was to identify the most active cash couriers repatriating U.S. currency from Mexico due to the change in Mexican banking laws in 2010. Once HSI officials identified the most active cash couriers, they used the information from the initial BSA filings to develop queries of additional BSA filings related to the couriers and the businesses for which they reportedly worked.

Investigators determined the most active cash courier was bringing on average approximately \$6 million per month into the United States from Mexico, and depositing the cash at a bank branch in California. Further analysis of BSA data identified a pattern of activity within this one bank that was similar to the activity of the cash courier already identified. Investigators identified a significant amount of structured cash transactions with minimal reporting or follow-up action taken by this bank.

Based on the apparent failures to report suspicious activity, as well as information that investigators obtained from bank employees regarding the bank's lax anti-money laundering (AML) controls, officials from HSI, Internal Revenue Service-Criminal Investigation (IRS-CI), United States Attorney's Office Southern District of California, DOJ Money Laundering and Asset Recovery Section and other law enforcement agencies began to examine the bank's criminal BSA/AML failures. These failures included money laundering, structuring, and other financial crimes committed by bank staff and customers. The criminal failures included the concealment of these deficiencies from, and false statements to, law enforcement and its primary regulator. This investigation occurred in parallel with regulatory investigations conducted by the Office of the Comptroller, Office of General Counsel, and the Financial Crimes Enforcement Network's Enforcement Division.

The prosecution team compared transactional activity in the accounts of the customers they identified as the most suspicious account holders against the bank's BSA filings. The review and analysis of the data revealed the bank had failed to monitor, review, investigate, and ultimately act on nearly one billion dollars of suspicious cash and wire transfer activity.

The bank's former Vice President (VP) of its BSA/AML unit acknowledged his criminal conduct in a deferred prosecution agreement. The financial institution ultimately pled guilty to conspiring to defraud the United States and to obstructing a financial exam by their Federal regulator. The criminal conviction of a financial institution was a first in BSA enforcement. At sentencing, the court imposed a historic penalty, comprised of the forfeiture of over \$368 million and a criminal fine of \$500,000.

This investigation was unique in that it involved transactions solely at U.S.-based banks, for transactions occurring on U.S. soil. It is also the first investigation to result in the criminal conviction of the financial institution for conspiring to defraud the United States and obstructing the functions of its regulator. The financial penalty imposed remains the largest in the history of the Southern District of California.

Cyber Threat: *Immigration and Customs Enforcement-Homeland Security Investigations (ICE-HSI)*

Investigators from Immigration and Customs Enforcement-Homeland Security Investigations (ICE-HSI), United States Postal Inspection Service, and United States Secret Service initiated this highly complex operation by analyzing Bank Secrecy Act (BSA) data to identify potential dark web vendors involved in narcotics sales. The BSA data provided a roadmap agents followed until the operation's conclusion, which resulted in tremendous criminal disruptions. The operation initially began in small-scale, but eventually evolved into an expansive operation using unique approaches to identify dark web narcotics dealers by targeting their illicit digital currency.

An analysis of BSA data provided investigators with the information necessary to subpoena a well-known cryptocurrency exchanger, resulting in the discovery of several related bank accounts with additional suspicious activity. Agents subsequently identified another subject who was importing large quantities of controlled substances via international mail from India. A search warrant carried out on the subject's property resulted in the seizure of several hundred thousand pharmaceutical pills and the discovery of \$600,000 in U.S. currency concealed within dozens of FedEx and U.S. Priority Mail envelopes. As agents continued this investigation, they discovered the vendor was purchasing U.S. currency from a very well-known dark web "cash-out" vendor, whom agents knew could lead to multiple targets nationwide.

Investigative results identified dark web vendors sending illicitly earned bitcoin with a physical receiving address via an encrypted email to conduct this cash-out scheme. This cash-out vendor charged anywhere from 12-16 percent depending on the amount of digital currency being cashed out. The investigators worked diligently to identify the individual operating the cash-out vendor's accounts. Agents relied heavily on BSA data, the results of a 314(a) request through FinCEN, and coordination with other law enforcement agencies to identify the individual and execute a search warrant and arrest. Agents seized over \$500,000 in U.S. currency and bitcoin valued at over \$800,000 USD at the time of the seizure.

Continued investigative efforts included extensive undercover operations and analysis of BSA data filed by various financial institution types, including virtual currency exchangers. This analysis led to the de-anonymization of over 80 additional dark web vendors selling illicit items, leading to the identification and arrest of numerous individuals. The operation concluded after the arrest of 42 individuals, the seizure of \$22 million in various digital currencies, \$3.5 million

EXHIBIT 1-B

in cash, 120 firearms, 15 pill press machines, and a wide range of controlled substances. This case was prosecuted by the United States Attorney's Office, Southern District of New York, and was coordinated by the Department of Justice's Money Laundering and Asset Forfeiture Section of the Criminal Division.

State and Local Law Enforcement: *New York State Police (NYSP)*

New York State Police (NYSP) investigators began this investigation after a New York-based bank representative contacted them to report an individual using counterfeit checks totaling over \$100,000 to complete a residential mortgage loan closing. The bank made this discovery after the deed and title to the property were transferred to the buyer.

The NYSP's Financial Crimes Unit conducted an analysis of Bank Secrecy Act (BSA) data that led to the discovery of a relationship between two individuals, including the primary subject of this investigation, working together on numerous fraud schemes to include the fraudulent real estate transaction that led to the investigation. Investigators identified BSA filings of multiple financial institutions involving the two individuals.

Investigators followed a complex trail of cash transactions, personal loans, mortgage loans, lines of credit, construction loans, cashier's checks, credit cards, and Automated Clearing House (ACH) transactions in order to trace the origin of the funds used in a series of fraudulent real estate transactions. Investigators determined that the subjects of this investigation submitted fraudulent information, including paystubs, bank account statements, tax documents, business proposals, invoices, and cashier's checks to the financial institutions to obtain these various products.

Investigators issued subpoenas to six different financial institutions and uncovered evidence of mortgage fraud, larceny, money laundering, falsifying business records, criminal possession of a forged instrument, and scheme to defraud. Through various schemes, the subjects defrauded the banks resulting in a loss in excess of \$170,000.

A grand jury indicted each of the two subjects on 19 fraud, larceny, money laundering, and criminal possession charges, both of whom were convicted at trial. One defendant was sentenced to 4-8 years in prison, while the other was sentenced to 2-6 years in prison. The Office of the New York State Attorney General prosecuted this case.

Third Party Money Launderers: *Internal Revenue Service-Criminal Investigation (IRS-CI)*

This investigation was led by the Internal Revenue Service-Criminal Investigation (IRS-CI) and the Drug Enforcement Administration (DEA). Bank Secrecy Act (BSA) reporting was crucial in identifying bank accounts and ultimately uncovering and substantiating multiple criminal violations.

This investigation focused on a transnational money laundering organization operating in the United States and Mexico through a complex trade-based money laundering (TBML) scheme.

This conspiracy involved couriers picking up drug proceeds in the form of U.S. currency from multiple cities in the United States and transporting it by various means to Texas. Once in Texas, the organization laundered the funds through commodities businesses, including perfume sellers, using a sophisticated TBML scheme. The drug proceeds collected in the United States were assigned by Mexico-based peso brokers to Mexican import businesses who owed U.S. currency to U.S. export businesses. Part of the proceeds were then delivered to the particular U.S. export businesses as payment for the purchase of goods, while the remainder of the proceeds were transferred through a series of additional transactions to Mexican drug cartels.

Investigative officials from several agencies analyzed a high volume of BSA data to identify the bank accounts of numerous individuals, as well as the money laundering activity occurring in these accounts. In some instances, officials were able to determine that certain BSA forms that should have been reported by the U.S.-based businesses involved had not been filed.

Following a 5-week jury trial, all of the defendants were convicted of various money laundering and conspiracy charges. In total, this organization laundered more than \$2.8 million. Approximately \$2.5 million was seized during the investigation, and over \$870,000 in money judgments were ordered after trial. The case was prosecuted by the United States Attorney's Office, Southern District of Texas-Laredo Division and the Department of Justice's Money Laundering and Asset Forfeiture Section of the Criminal Division.

Transnational Organized Crime: *Drug Enforcement Administration (DEA)*

This multi-year investigation led by Drug Enforcement Administration (DEA) agents focused on a narcotics trafficking and money laundering organization with ties to the Sinaloa and Jalisco New Generation cartels. The investigative efforts included the analysis of over 100 Bank Secrecy Act (BSA) records that helped lead to numerous arrests and the significant disruption of this criminal organization.

Utilizing various investigative techniques and strategies, DEA agents identified members of a global money laundering network that controls the flow of narcotics proceeds for Mexican cartels. Investigators leveraged this information to target the money laundering cells providing acquisition and processing of funds, and in under 9 months, investigators seized over \$2 million and the largest volume of fentanyl in U.S. history.

Investigators subsequently carried out numerous operations, which provided a plethora of new leads to DEA offices located domestically and internationally. These operations helped initiate a large-scale financial investigation into multiple companies based in the United States, Mexico, China, Taiwan, Hong Kong, Italy, and France. An analysis of the financial activity of these companies revealed that many of their accounts were utilized to transfer narcotics proceeds to various parts of the world before returning to the Mexican cartels. This financial investigation included an analysis of a high volume of BSA data, and resulted in the discovery of accounts holding hundreds of millions of dollars in forfeitable and verifiable narcotics proceeds intended to be used for real estate and

EXHIBIT 1-B

other investments in an attempt to legitimize the funds. Investigators subsequently seized over \$22 million from a Miami-based real estate investment firm that was using sophisticated trading techniques to repatriate narcotics proceeds to Mexico through U.S.-based real estate purchases. Investigators also discovered numerous accounts invested in corporate bonds, treasury notes, and various stock indexes. Seizures of these accounts totaled nearly \$85 million.

Investigators continue to develop the “end game” scenario involving the arrest of numerous money launderers and brokers working for the Mexican cartels as well as the global money laundering network. To date, the investigation has resulted in the combined seizure of 562 kilos of narcotics and \$165 million in criminal proceeds, as well as the execution of 162 arrests and indictments of 25 organization members. The United States Attorney’s Office, Southern District of New York prosecuted this case.

Transnational Security Threat Category: *Federal Bureau of Investigation (FBI)*

Federal Bureau of Investigation (FBI) officials initiated this investigation after Treasury’s Office of Foreign Assets Controls (OFAC) blocked approximately \$2 million USD in transit from a Hong Kong-based entity acting as a shell company for a North Korean bank known to be a proliferator of weapons of mass destruction (WMD). The Hong Kong based company operated in such a manner that allowed the North Korean bank to access the U.S. financial system illegally.

FBI investigators analyzed a large volume of Bank Secrecy Act (BSA) data to map out the scheme, identify previously unknown transactions, and confirm related transactions facilitated by the network. Investigators utilized the 314(a) Program and, also under the safe harbor of the 314(b) Program, interfaced with an established bank consortium group to produce an analysis that detailed transactions related to the Hong Kong shell company and its counterparties.

Law enforcement officials analyzed BSA, 314(a), and search warrant data to generate grand jury subpoenas to correspondent banks in order to obtain the shell company’s transaction history. Investigators were then able to ascertain the currency and amount of the transactions, the banking information of the beneficiaries, contact information, and any memos, such as invoice numbers, that the North Korean originator requested.

Using the data obtained from the various investigative techniques, FBI was able to demonstrate the Hong Kong-based company was used strictly as a shell company to clear funds for North Korea, both directly and indirectly. FBI, together with the U.S. Attorney’s Office in the District of Columbia, filed an affidavit to seize the blocked funds totaling \$1,902,976. Shortly after the seizure warrant was executed, a Chinese national used by the North Koreans as a bank liaison for the shell company was sanctioned, along with the Hong Kong-based company itself.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



[Home \(/\)](#)

[Resources \(/resources\)](#)

[Contact \(/contact\)](#)

[About \(/what-we-do\)](#)

[Careers \(/cutting-edge-opportunities\)](#)

[Newsroom \(/news-room\)](#)

[Site Map \(/sitemap\)](#)

[Contract Opportunities \(/about/contract-opportunities\)](#)

[USA.gov \(https://www.USA.gov\)](https://www.USA.gov) | [Regulations.gov \(https://www.Regulations.gov\)](https://www.Regulations.gov) | [Treasury.gov \(https://www.treasury.gov\)](https://www.treasury.gov) | [IRS.gov \(https://www.IRS.gov\)](https://www.IRS.gov) | [Freedom of Information Act \(FOIA\) \(/freedom-information-act-foia-and-guide-accessing-fincen-information\)](#) | [NO FEAR Act \(https://www.treasury.gov/No-Fear-Act/Pages/default.aspx\)](https://www.treasury.gov/No-Fear-Act/Pages/default.aspx) | [Accessibility \(/accessibility\)](#) | [EEO & Diversity Policy \(/equal-employment-opportunity-and-diversity-policy\)](#) | [Privacy Policy \(/privacy-security\)](#)

EXHIBIT 1-B

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Financial Crimes Enforcement Network
National Credit Union Administration
Office of the Comptroller of the Currency**

Interagency Statement on Sharing Bank Secrecy Act Resources

October 3, 2018

Introduction

The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) (collectively, the Agencies), are publishing this statement to address instances in which banks¹ may decide to enter into collaborative arrangements to share resources to manage their Bank Secrecy Act (BSA) and anti-money laundering (AML) obligations more efficiently and effectively. Collaborative arrangements as described in this statement generally are most suitable for banks with a community focus, less complex operations, and lower-risk profiles for money laundering or terrorist financing. The risk profile is bank-specific, and should be based on a risk assessment that properly considers all risk areas, including products, services, customers, entities, and geographic locations.²

Collaborative arrangements involve two or more banks with the objective of participating in a common activity or pooling resources to achieve a common goal. Banks use collaborative arrangements to pool human, technology, or other resources to reduce costs, increase operational efficiencies, and leverage specialized expertise.

Notably, this interagency statement does not apply to collaborative arrangements or consortia formed for the purpose of sharing information under Section 314(b) of the USA PATRIOT Act. Further, banks that form collaborative arrangements as described in this interagency statement are not an association for purposes of Section 314(b) of the USA PATRIOT Act.³ Banks should contact FinCEN for additional information concerning the 314(b) program and requirements.

All banks are required to establish and maintain procedures reasonably designed to ensure compliance with the BSA and to develop and implement BSA/AML programs.⁴ The BSA/AML compliance program must include the following: 1) a system of internal controls to ensure ongoing compliance; 2) independent testing of BSA/AML compliance; 3) designating an individual or individuals responsible for managing BSA compliance (BSA compliance officer);

¹ Under the BSA the term "bank" is defined in 31 CFR 1010.100(d) and includes each agent, agency, branch or office within the United States of banks, savings associations, credit unions, and foreign banks.

² See Federal Financial Institutions Examination Council (FFIEC) *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2014), at https://bsaaml.ffiec.gov/pages_manual/manual_online.htm

³ See *Voluntary Information Sharing Among Financial Institutions*, 31 CFR 1010.540.

⁴ See 31 U.S.C. 5311 *et seq.*, 31 U.S.C. 5318(h)(1), and the federal banking agencies' implementing BSA/AML compliance program regulations: 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (FRB); 12 CFR 326.8 (FDIC); 12 CFR 748.2 (NCUA); and 12 CFR 21.21 (OCC).

EXHIBIT 1-B

and 4) training for appropriate personnel.⁵ A bank is expected to have a BSA/AML compliance program commensurate with its respective risk profile.

Benefits of Sharing a Resource

The cost of meeting BSA requirements and effectively managing the risk that illicit finance poses to the broader U.S. financial system may be reduced through sharing employees or other resources in a collaborative arrangement with one or more other banks. These arrangements may also provide access to specialized expertise that may otherwise be challenging to acquire without the collaboration. The following examples describe situations in which the use of shared human, technology or other resources in a collaborative arrangement may be beneficial for banks. These examples are not intended to be exhaustive.

Internal Controls Example

Banks are required to provide for a system of internal controls to assure ongoing compliance with the BSA. A collaborative arrangement may be entered into by two or more banks to share resources between the respective banks to conduct internal control functions. Some examples of functions that may be conducted utilizing shared resources include: 1) reviewing, updating, and drafting BSA/AML policies and procedures; 2) reviewing and developing risk-based customer identification and account monitoring processes; and 3) tailoring monitoring systems and reports for the risks posed.

Independent Testing Example

Banks are required to provide for independent testing for compliance. That testing may be conducted by an outside party or bank personnel. Such testing should provide an evaluation of the adequacy and effectiveness of the bank's BSA/AML compliance program.

Some banks may have personnel that perform multiple job functions, making it difficult to identify an employee within the bank to conduct an independent test of the BSA/AML compliance program. Personnel at one bank may be utilized to conduct the BSA/AML independent test at another bank within a collaborative arrangement. The shared resource may, for example, be utilized in the scoping, planning, and performance of the BSA/AML compliance program independent test with appropriate safeguards in place to ensure the confidentiality of sensitive business information. The banks involved in the collaborative arrangement need to ensure that the shared resource conducting the BSA/AML independent testing is qualified and not involved in other BSA/AML functions at the bank being reviewed, such as training or developing policies and procedures that may present a conflict of interest or lack of independence.

⁵ See 31 CFR 1020.210 and 1010.230 – Under the Customer Due Diligence rule, banks are required to develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence, to include, but not be limited to (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information (including beneficial owners of legal entity customers).

EXHIBIT 1-B

BSA/AML Training Example

Banks must ensure that appropriate personnel are trained in BSA regulatory requirements and in internal BSA/AML policies, procedures, and processes.

It may be challenging to acquire personnel with BSA/AML expertise in some communities. It may also be cost prohibitive to attract a qualified outside BSA/AML trainer. A collaborative arrangement between two or more banks may provide the latitude to hire a qualified instructor to conduct the BSA/AML training, allowing the bank to share the cost. Examples of basic BSA/AML training topics that may be covered by shared resources include: alert analysis and investigation techniques, alert trends and money laundering methods, and regulatory updates.

Other Considerations

The bank's board of directors must designate a qualified individual or individuals to serve as the BSA compliance officer.⁶ The sharing of a BSA officer among banks could be challenging due to the confidential nature of suspicious activity reports filed and the ability of the BSA officer to effectively coordinate and monitor each bank's day-to-day BSA/AML compliance. In addition, the sharing of a BSA officer may create challenges with effective communication between the BSA officer and each bank's board of directors and senior management. Accordingly, it may not be appropriate for banks to enter into a collaborative arrangement to share a BSA officer.⁷

Risk Considerations and Mitigation

The use of collaborative arrangements to manage BSA/AML obligations requires careful consideration regarding the type of collaboration in relation to the bank's risk profile, adequate documentation, consideration of legal restrictions, and the establishment of appropriate oversight mechanisms; and should be consistent with sound principles of corporate governance. For example, a bank's board of directors should provide for appropriate oversight of BSA/AML collaborative arrangements in advance. As is standard, a collaborative arrangement should be supported by a contractual agreement between the banks, with the performance reviewed by management and evaluated on a periodic basis. Banks should refer to their respective regulator's existing guidance regarding third-party relationships.

A collaborative arrangement for sharing employees or other resources to manage BSA/AML obligations is similar to using dual-employees. Guidance in this area could be relevant to contractual agreements between banks sharing BSA/AML resources.⁸ Banks must also comply with all applicable legal restrictions, including limitations on the disclosure of confidential supervisory information, confidential financial and business information, individual customer

⁶ See 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (FRB); 12 CFR 326.8 (FDIC); 12 CFR 748.2 (NCUA); and 12 CFR 21.21 (OCC).

⁷ Although it may not generally be appropriate to share a BSA officer through a collaborative arrangement, it may be more appropriate between affiliated banks.

⁸ See e.g., FDIC's *Risk Management Manual of Examination Policies*, Chapter 4.3 *Related Organizations, Dual Employees* Section at <https://www.fdic.gov/regulations/safety/manual/section4-3.pdf>.

EXHIBIT 1-B

data, and trade secrets, as well as restrictions governing collaborative arrangements among competitors generally, such as rules designed to limit conflicts of interest.

As is usual and customary when a bank enters into an arrangement with a third-party, a collaborative arrangement should be appropriately documented to define the nature and type of resources to be shared, define each institution's rights and responsibilities, establish procedures for protecting customer data and confidential information, and develop a framework to manage risks associated with the sharing of resources. Reasonable systems should be established to ensure that bank management adequately oversees the activities of shared resources. Banks should devote sufficient resources for monitoring services performed under the collaborative arrangement. Periodic reports related to BSA/AML collaborative arrangements should be provided to senior management and reported to the board of directors as appropriate in conjunction with their regular oversight of bank activities.

It is important that collaborative arrangements be designed and implemented in accordance with the bank's risk profile for money laundering and terrorist financing. Ultimately, each bank is responsible for ensuring compliance with BSA requirements. Sharing resources in no way relieves a bank of this responsibility. Nothing in this interagency statement alters a bank's existing legal and regulatory requirements.

Conclusion

Banks may benefit from using shared resources to manage certain BSA/AML obligations more efficiently and effectively. However, banks should approach the establishment of collaborative arrangements like other business decisions, with due diligence and thorough consideration of the risks and benefits. Banks are encouraged to contact their primary federal regulator regarding sharing BSA resources, and should refer to other relevant guidance.⁹

⁹ See e.g., OCC's "[An Opportunity for Community Banks: Working Together Collaboratively](https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-community-banks-working-collaborately.PDF)" (January 13, 2015), at <https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-community-banks-working-collaborately.PDF>.

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Financial Crimes Enforcement Network
National Credit Union Administration
Office of the Comptroller of the Currency**

**Joint Statement on Innovative Efforts to Combat Money Laundering
and Terrorist Financing**

December 3, 2018

The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Financial Crimes Enforcement Network (FinCEN), the National Credit Union Administration, and the Office of the Comptroller of the Currency (collectively, the Agencies) are issuing this joint statement to encourage banks¹ to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their Bank Secrecy Act/anti-money laundering (BSA/AML) compliance obligations, in order to further strengthen the financial system against illicit financial activity.

The Agencies recognize that private sector innovation, including new ways of using existing tools or adopting new technologies, can help banks identify and report money laundering, terrorist financing, and other illicit financial activity by enhancing the effectiveness and efficiency of banks' BSA/AML compliance programs. To assist banks in this effort, the Agencies are committed to continued engagement with the private sector and other interested parties.

The Agencies will not penalize or criticize banks that maintain effective BSA/AML compliance programs commensurate with their risk profiles but choose not to pursue innovative approaches. While banks are expected to maintain effective BSA/AML compliance programs, the Agencies will not advocate a particular method or technology for banks to comply with BSA/AML requirements.

Innovative Approaches to Combat Money Laundering, Terrorist Financing, and Other Illicit Financial Activity

Innovation has the potential to augment aspects of banks' BSA/AML compliance programs, such as risk identification, transaction monitoring, and suspicious activity reporting. Some banks are becoming increasingly sophisticated in their approaches to identifying suspicious activity, commensurate with their risk profiles, for example, by building or enhancing innovative internal financial intelligence units devoted to identifying complex and strategic illicit finance

¹ Under the Bank Secrecy Act, the term "bank" is defined in 31 CFR 1010.100(d) and includes each agent, agency, branch, or office within the United States of banks, savings associations, credit unions, and foreign banks.

vulnerabilities and threats. Some banks are also experimenting with artificial intelligence and digital identity technologies applicable to their BSA/AML compliance programs. These innovations and technologies can strengthen BSA/AML compliance approaches, as well as enhance transaction monitoring systems. The Agencies welcome these types of innovative approaches to further efforts to protect the financial system against illicit financial activity. In addition, these types of innovative approaches can maximize utilization of banks' BSA/AML compliance resources.

Pilot programs undertaken by banks, in conjunction with existing BSA/AML processes, are an important means of testing and validating the effectiveness of innovative approaches. While the Agencies may provide feedback, pilot programs in and of themselves should not subject banks to supervisory criticism even if the pilot programs ultimately prove unsuccessful. Likewise, pilot programs that expose gaps in a BSA/AML compliance program will not necessarily result in supervisory action with respect to that program. For example, when banks test or implement artificial intelligence-based transaction monitoring systems and identify suspicious activity that would not otherwise have been identified under existing processes, the Agencies will not automatically assume that the banks' existing processes are deficient. In these instances, the Agencies will assess the adequacy of banks' existing suspicious activity monitoring processes independent of the results of the pilot program. Further, the implementation of innovative approaches in banks' BSA/AML compliance programs will not result in additional regulatory expectations.

At the same time, compliance with the BSA and its regulations is critically important in protecting the U.S. financial system, and banks that fail to comply with BSA/AML requirements expose the financial system to abuse by illicit actors. Accordingly, banks must continue to meet their BSA/AML compliance obligations, as well as ensure the ongoing safety and soundness of the bank, when developing pilot programs and other innovative approaches. Bank management should prudently evaluate whether, and at what point, innovative approaches may be considered sufficiently developed to replace or augment existing BSA/AML processes. In making these evaluations, bank management should also consider and address other factors including, but not limited to, information security issues, third-party risk management, and compliance with other applicable laws and regulations, such as those related to customer notifications and privacy. Bank management should also discuss their evaluations with the bank's respective regulators.

Commitment to Continued Private Sector Engagement

The Agencies are open to engaging with bank management to discuss pilot programs for innovative BSA/AML approaches. As banks pursue innovative change, early engagement can promote a better understanding of these approaches by the Agencies, as well as provide a means to discuss expectations regarding compliance and risk management. In addition, the Agencies will clarify supervisory expectations, as appropriate and necessary.

The Agencies will continue to monitor industry developments and encourage responsible innovative approaches in BSA/AML compliance programs that help protect the financial system against illicit financial activity. To this end, the Agencies are exploring additional methods to encourage innovation, including through FinCEN's Bank Secrecy Act Advisory Group. Also, to

the extent necessary and appropriate, FinCEN will consider requests for exceptive relief under 31 CFR 1010.970 to facilitate the testing and potential use of new technologies and other innovations, provided that banks maintain the overall effectiveness of their BSA/AML compliance programs. FinCEN is launching an innovation initiative to foster a better understanding of the opportunities and challenges of BSA/AML-related innovation in the financial services sector. As part of this initiative, FinCEN will engage in outreach efforts that include dedicated times for financial institutions, technology providers, and other firms involved in financial services innovations to discuss the implications of their products and services, and their future applications or next steps.

Similarly, each of the other Agencies has, or will establish, projects or offices that will work to support the implementation of responsible innovation and new technology in the financial system. While bank management should continue to follow existing protocols for communication with their respective regulators, these projects or offices may also serve as central points of contact to facilitate communication related to innovation and new technology. In addition, they are intended to enhance the other Agencies' ability to respond to innovation and new technology, understand the related risks, and encourage discussion of regulatory principles, processes, and expectations.

The Agencies also welcome industry's feedback on how the Agencies can best support innovative efforts through explanations of, or updates to, supervisory processes, regulations, and guidance. Those wishing to share such feedback in writing may do so by sending their submission electronically to FinCEN at FRC@fincen.gov.

EXHIBIT 1-B



Financial Crimes Enforcement Network
U.S. Department of the Treasury

Washington, D.C. 20220

Financial Crimes Enforcement Network (FinCEN) Statement on Enforcement of the Bank Secrecy Act

This statement describes FinCEN's approach to enforcing the Bank Secrecy Act (BSA).¹ FinCEN uses the factors described in this statement to determine the appropriate enforcement response when it identifies actual or possible violations of the BSA. FinCEN is issuing this statement as administrator of the BSA.²

Background

Most BSA requirements apply by their terms only to "financial institutions," as defined in the BSA and its implementing regulations. The definition of financial institution encompasses a wide variety of institutions, including banks, broker-dealers in securities, money services businesses, and casinos and card clubs, among others.³ The BSA, in more limited circumstances, prescribes rules of conduct for nonfinancial trades and businesses and individuals. FinCEN may take enforcement actions, to include imposing civil money penalties on financial institutions, nonfinancial trades or businesses, and other persons that violate the BSA, and in a number of instances may take enforcement actions, to include imposing civil money penalties on partners, directors, officers, or employees who participate in these violations.⁴

When FinCEN takes an enforcement action, it will seek to establish a violation of law based on applicable statutes and regulations. FinCEN will not treat noncompliance with a standard of conduct announced solely in a guidance document as itself a violation of law. Regulated parties will be afforded an opportunity to respond to and contest factual findings or legal conclusions underlying any FinCEN enforcement action.

1. The BSA is codified at 12 U.S.C. §§ 1829b, 1951-1959, and 31 U.S.C. §§ 5311-5314, 5316-5332. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.
2. 31 C.F.R. § 1010.810(a) (2019) (delegating to FinCEN "overall authority for enforcement and compliance").
3. See, e.g., 31 U.S.C. § 5312(a)(2)(A)–(F) (2012) and 31 C.F.R. § 1010.100(d), (t)(1) (2019) (banks); 31 U.S.C. § 5312(a)(2)(G) (2012) and 31 C.F.R. § 1010.100(h), (t)(2) (2019) (broker-dealers in securities); 31 U.S.C. § 5312(a)(2)(R) (2012) and 31 C.F.R. § 1010.100(t)(3), (ff) (2019) (money services businesses); and 31 U.S.C. § 5312(a)(2)(X) (2012) and 31 C.F.R. § 1010.100(t)(5), (t)(6) (2019) (casinos and card clubs).
4. 31 U.S.C. §§ 5321, 5324 and 5330(e) (2012); 12 U.S.C. §§ 1829b(j) and 1955 (2012). FinCEN has the authority to examine financial institutions and, in addition, relies on examinations conducted by Federal functional regulators and the Internal Revenue Service. 31 U.S.C. § 5318(a)(3) and (b) (2012); 31 C.F.R. § 1010.810 (2019). Federal functional regulators, which may have their own enforcement authority, include the Securities and Exchange Commission, the Commodity Futures Trading Commission, the National Credit Union Administration, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Board of Directors of the Federal Deposit Insurance Corporation. 31 C.F.R. § 1010.100(r) (2019).

EXHIBIT 1-B

Enforcement Approach

FinCEN has authority to take the following actions when it identifies an actual or possible violation of the BSA or any BSA regulation or order:

1. No Action. FinCEN may close a matter with no additional action. FinCEN may reopen the matter if FinCEN obtains new material information concerning the matter or becomes aware of additional or subsequent violations.
2. Warning Letter. FinCEN may issue a warning through a supervisory letter or similar communication.
3. Equitable Remedies. FinCEN may seek an injunction or equitable relief to enforce compliance when FinCEN believes an entity or individual has violated, is violating, or will violate the BSA or any BSA regulation or order.
4. Settlements. As part of a settlement, FinCEN may require both remedial undertakings and civil money penalties.
5. Civil Money Penalties. FinCEN may assess a civil money penalty.
6. Criminal Referral. If circumstances warrant, FinCEN may refer a matter to appropriate law enforcement agencies for criminal investigation and/or criminal prosecution.

In all matters, FinCEN will consider the need to impose compliance commitments deemed necessary and appropriate to ensure that financial institutions are fully complying with their BSA obligations.

FinCEN considers a range of factors when evaluating an appropriate disposition upon identifying actual or possible violations of the BSA. FinCEN considers both compliance with specific BSA requirements—such as registration, recordkeeping, and reporting requirements—as well as the adequacy of an anti-money laundering (AML) program, including the extent of the AML program's compliance with pillar requirements.⁵ FinCEN strives for proportionality, consistency, and effectiveness. The weight given to any factor in contemplation of the potential dispositions identified above may change based on the relevant facts and circumstances of a case. The factors FinCEN considers include, but are not limited to, the following:

1. Nature and seriousness of the violations, including the extent of possible harm to the public and the amounts involved.
2. Impact or harm of the violations on FinCEN's mission to safeguard the financial system from illicit use, combat money laundering, and promote national security.
3. Pervasiveness of wrongdoing within an entity, including management's complicity in, condoning or enabling of, or knowledge of the conduct underlying the violations.
4. History of similar violations, or misconduct in general, including prior criminal, civil, and regulatory enforcement actions.
5. Financial gain or other benefit resulting from, or attributable to, the violations.

5. "Pillar violations" would include the lack of one or more required elements of an AML program. Although AML program requirements may vary among categories of financial institution, all financial institutions that are subject to AML program requirements must implement a set of internal controls, conduct training and independent testing, and designate one or more individuals to assure day-to-day compliance with the BSA. *See, e.g.*, 31 C.F.R. § 1022.210 (AML program requirements for money services businesses).

EXHIBIT 1-B

6. Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures.
7. Timely and voluntary disclosure of the violations to FinCEN.
8. Quality and extent of cooperation with FinCEN and other relevant agencies, including as to potential wrongdoing by its directors, officers, employees, agents, and counterparties.
9. Systemic nature of violations. Considerations include, but are not limited to, the number and extent of violations, failure rates (*e.g.*, the number of violations out of total number of transactions), and duration of violations.
10. Whether another agency took enforcement action for related activity. FinCEN will consider the amount of any fine, penalty, forfeiture, and/or remedial action ordered.

EXHIBIT 1-B

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency**

August 13, 2020

JOINT STATEMENT ON ENFORCEMENT OF BANK SECRECY ACT/ ANTI-MONEY LAUNDERING REQUIREMENTS¹

The Board of Governors of the Federal Reserve System (“Federal Reserve”), the Federal Deposit Insurance Corporation (“FDIC”), the National Credit Union Administration (“NCUA”), and the Office of the Comptroller of the Currency (“OCC”), (an “Agency” or collectively the “Agencies”), are issuing this statement to set forth the Agencies’ policy on the circumstances in which an Agency will issue a mandatory cease and desist order to address noncompliance with certain Bank Secrecy Act/anti-money laundering (“BSA/AML”) requirements,² particularly in light of the specific BSA/AML compliance provisions in section 8(s) of the Federal Deposit Insurance Act (“FDIA”) and section 206(q) of the Federal Credit Union Act (“FCUA”) (hereafter referred to as “sections 8(s) and 206(q)”).³ This interagency statement also describes the circumstances in which an Agency may use its discretion to issue formal or informal enforcement actions or use other supervisory actions to address BSA-related violations or unsafe or unsound banking practices or other deficiencies. This statement does not create new

¹ This statement supersedes the Interagency Statement on Enforcement of BSA/AML Requirements issued by the Agencies in July 2007 and is intended to set forth general policy guidance. It does not compel or preclude an enforcement or other supervisory action as appropriate in a specific factual situation.

² This statement does not address the assessment of civil money penalties for violations of the BSA or its implementing regulations. The Agencies have such authority under their general enforcement statutes. 12 U.S.C. §§ 1786(k)(2) and 1818(i)(2). Likewise, the Financial Crimes Enforcement Network (“FinCEN”) has independent authority to assess civil money penalties under the BSA.

³ 12 U.S.C. §§ 1786(q), 1818(s).

EXHIBIT 1-B

expectations or standards. Rather, it is intended to further clarify the Agencies' enforcement of the BSA and the conditions that require the issuance of a mandatory cease and desist order under sections 8(s) and 206(q). Whenever the Agencies undertake an enforcement action, whether mandatory under sections 8(s)(3) and 206(q)(3) or otherwise, they will tailor that action to address the deficiencies that are specific to the institution,⁴ as identified during the supervisory process.⁵

I. Background.

BSA/AML Compliance Program Requirement.

Under section 8(s) of the FDIA and section 206(q) of the FCUA, each of the Agencies is directed to prescribe regulations requiring each insured depository institution to establish and maintain procedures reasonably designed to assure and monitor the institution's compliance with the requirements of the BSA (collectively, these procedures form the basis of each institution's "BSA/AML compliance program"). Sections 8(s) and 206(q) require that each Agency's examination of an institution include a review of the institution's BSA/AML compliance program and that reports of examination describe any problem with the BSA/AML compliance program. Finally, sections 8(s) and 206(q) state that if an institution has failed to establish and maintain a BSA/AML compliance program or has failed to correct any problem with the BSA/AML compliance program

⁴ The term "institution" refers to banks, as defined in 31 C.F.R. § 1010.100(d), and includes each agent, agency, branch or office within the United States of banks, savings associations, credit unions, and foreign banks.

⁵ It should also be noted that BSA/AML enforcement actions can have a significant impact on an institution's ability to engage in certain corporate activities and expansion since the effectiveness of an institution's efforts in combating money laundering are expressly required to be considered by the Agencies when evaluating proposals subject to the Bank Merger Act, 12 U.S.C. § 1828(c)(11), and the Bank Holding Company Act, 12 U.S.C. § 1842(c)(6).

EXHIBIT 1-B

previously reported to the institution by the appropriate Agency, the appropriate Agency shall issue a cease and desist order against the institution.

As required by sections 8(s) and 206(q), each of the Agencies has issued regulations that require any institution it supervises or insures to establish and maintain a BSA/AML compliance program. Each of these regulations imposes substantially the same requirements.⁶ Specifically, under each Agency's regulations, a BSA/AML compliance program must: (1) be reasonably designed to assure and monitor the institution's compliance with the requirements of the BSA and its implementing regulations and (2) have, at a minimum, the following components or pillars:

- a system of internal controls to assure ongoing compliance with the BSA;
- independent testing for BSA/AML compliance;
- a designated individual or individuals responsible for coordinating and monitoring BSA/AML compliance; and
- training for appropriate personnel.

A BSA/AML compliance program must include a Customer Identification Program with risk-based procedures that enable the institution to form a reasonable belief that it knows the true identity of its customers.⁷

⁶ 12 C.F.R. §§ 21.21 (OCC); 208.63 (Federal Reserve); 326.8(c) (FDIC); 748.2 (NCUA). The provisions of section 8(s) are also made applicable to certain banking organizations other than insured depository institutions. 12 U.S.C. §§ 1818(b)(3), (b)(4). The OCC's regulations also apply to Federal branches and agencies of foreign banks. 12 U.S.C. § 3102(b); 12 C.F.R. § 28.13. The Federal Reserve's regulations also apply to Edge Act and agreement corporations, and branches, agencies, and other offices of foreign banking organizations. 12 C.F.R. §§ 211.5, 211.24. BSA/AML compliance programs that comply with these Agency regulations are also deemed to comply with the Treasury Department's regulations issued pursuant to the BSA, which separately require that financial institutions establish AML programs. *See*, 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210.

⁷ 12 C.F.R. §§ 21.21(c)(2) (OCC); 208.63(b)(2), 211.5(m)(2), 211.24(j)(2), (Federal Reserve); 326.8(b)(2) (FDIC); 748.2(b)(2) (NCUA); 31 C.F.R. § 1020.220 (Treasury Department).

EXHIBIT 1-B

A BSA/AML compliance program must also include appropriate risk-based procedures for conducting ongoing customer due diligence as set forth in regulations issued by the U.S. Department of the Treasury (“Treasury Department”),⁸ including, but not limited to:

- understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.

In addition to these customer due diligence requirements, a reasonably designed BSA/AML compliance program must include procedures to address other BSA reporting and recordkeeping requirements set forth in regulations issued by the Treasury Department including, among others, beneficial ownership, foreign correspondent banking, and currency transaction reporting requirements.⁹ For the purposes of sections 8(s) and 206(q), the Agencies evaluate customer due diligence and other BSA reporting and recordkeeping requirements as a part of the internal controls component of the bank’s BSA/AML compliance program.

Communication of Supervisory Concerns about BSA/AML Compliance Programs.

Sections 8(s) and 206(q) require that each Agency examine the institution’s BSA/AML compliance program, and that reports of examination describe any problem with that BSA/AML compliance program. When an Agency identifies supervisory concerns relating to an institution’s BSA/AML compliance program in the course of an examination or otherwise, the Agency may communicate those concerns by various

⁸ 31 C.F.R. § 1020.210(b)(5).

⁹ See 31 C.F.R. Parts 1010 and 1020.

EXHIBIT 1-B

formal and informal means. The particular method of communication used typically depends on the seriousness of the concerns and each Agency's policies. These methods may include, but are not limited to:

- informal discussions by examiners with an institution's management during an examination or ongoing supervision processes;
- formal discussions by examiners with the board of directors as part of or following an examination, or as part of the ongoing supervision processes;
- written communications from examiners or the Agency to an institution's board of directors or senior management that communicate concerns regarding the implementation of its BSA/AML compliance program;
- a finding contained in the report of examination or in other formal communications from an Agency to an institution's board of directors or senior management indicating deficiencies or weaknesses in the BSA/AML compliance program; or
- a finding contained in the report of examination or in other formal communications from the Agency to an institution's board of directors or senior management of a violation of the regulatory requirement to implement and maintain a reasonably designed BSA/AML compliance program.

As explained below, for section 8(s) or 206(q) to apply, the deficiencies in the compliance program must be identified in a report of examination or other written document reported to an institution's board of directors or senior management as a violation of law or a matter that must be corrected. Certain isolated or technical violations of law and other issues or suggestions for improvement may be communicated through other means.

II. Enforcement Actions for BSA/AML Compliance Program Failures.

In accordance with sections 8(s)(3) and 206(q)(3), the appropriate Agency shall issue a cease and desist order against an institution for noncompliance with BSA/AML

EXHIBIT 1-B

compliance program requirements in the following situations, based on a careful review of all the relevant facts and circumstances.

Failure to establish and maintain a reasonably designed BSA/AML Compliance Program.

The appropriate Agency shall issue a cease and desist order based on a violation of the requirement in sections 8(s) and 206(q) to establish and maintain a reasonably designed BSA/AML compliance program where the institution:¹⁰

- fails to have a written BSA/AML compliance program, including a customer identification program, that adequately covers the required program components or pillars (internal controls, independent testing, designated BSA/AML personnel, and training); or
- fails to implement a BSA/AML compliance program that adequately covers the required program components or pillars (institution-issued policy statements alone are not sufficient; the program as implemented must be consistent with the institution's written policies, procedures, and processes); or
- has defects in its BSA/AML compliance program in one or more program components or pillars that indicate that either the written BSA/AML compliance program or its implementation is not effective, for example, where the deficiencies are coupled with other aggravating factors, such as (i) highly suspicious activity creating a potential for significant money laundering, terrorist financing, or other illicit financial transactions, (ii) patterns of structuring to evade reporting requirements, (iii) significant insider complicity, or (iv) systemic failures to file currency transaction reports ("CTRs"), suspicious activity reports ("SARs"), or other required BSA reports.

For example, an institution would be subject to a cease and desist order if its system of internal controls (such as customer due diligence, procedures for monitoring suspicious activity or an appropriate risk assessment) fails with respect to either a high-risk area or multiple lines of business that significantly impact the institution's overall

¹⁰ The examples in this document do not in any way limit the ability of an Agency to bring an enforcement action under sections 8(s) and 206(q) where the failure to have or implement a BSA/AML compliance program is demonstrated by other deficiencies. The examples are included for illustrative purposes only and do not set any thresholds or precedent for future enforcement actions.

EXHIBIT 1-B

BSA/AML compliance program, even if the other components or pillars are satisfactory. Similarly, a cease and desist order would be warranted if, for example, an institution has deficiencies in the required independent testing component or pillar of the BSA/AML compliance program and those deficiencies are coupled with evidence of highly suspicious activity, creating a potential for significant money laundering, terrorist financing, or other illicit financial transactions in the institution.

An institution would also be subject to a cease and desist order if the institution fails to implement a BSA/AML compliance program that adequately covers the required program components or pillars. For example, an institution rapidly expands its business relationships through its foreign affiliates and businesses:

- without identifying its money laundering and other illicit financial transaction risks;
- without an appropriate system of internal controls to verify customers' identities, conduct customer due diligence, or monitor for suspicious activity related to its products and services;
- without providing sufficient authority, resources, or staffing to its designated BSA officer to properly oversee its BSA/AML compliance program;
- with deficiencies in independent testing that caused it to fail to identify problems; and
- with inadequate training exemplified by relevant personnel not understanding their BSA/AML responsibilities.

However, other types of deficiencies in an institution's BSA/AML compliance program or in implementation of one or more of the required BSA/AML compliance program components or pillars, including violations of the individual component or pillar requirements, will not necessarily result in the issuance of a cease and desist order, unless the deficiencies are so severe or significant as to render the BSA/AML compliance

EXHIBIT 1-B

program ineffective when viewed as a whole. For example, an institution that has deficiencies only in its procedures for providing BSA/AML training to appropriate personnel ordinarily may be subject to examiner criticism and/or supervisory action other than the issuance of a cease and desist order, unless the training program deficiencies, viewed in light of all relevant circumstances, are so severe or significant as to result in a finding that the organization's BSA/AML compliance program, taken as a whole, is not effective.

In determining whether an institution has failed to implement a BSA/AML compliance program, an Agency will also consider the application of the institution's BSA/AML compliance program across its business lines and activities. In the case of institutions with multiple lines of business, deficiencies affecting only some lines of business or activities would need to be evaluated to determine if the deficiencies are so severe or significant in scope as to result in a conclusion that the institution has not implemented an effective overall BSA/AML compliance program.

Failure to correct a previously reported problem with the BSA/AML Compliance Program.

An Agency shall, in accordance with sections 8(s) and 206(q), and based on a careful review of the relevant facts and circumstances, issue a cease and desist order whenever an institution fails to correct a previously reported problem with its BSA/AML compliance program identified during the supervisory process. However, in order to be considered a "problem" within the meaning of sections 8(s)(3)(B) and 206(q)(3)(B), a problem reported to the institution ordinarily would involve substantive deficiencies in one or more of the required components or pillars of the institution's BSA/AML compliance program or implementation thereof that is reported to the institution's board

EXHIBIT 1-B

of directors or senior management in a report of examination or other supervisory communication as a violation of law or regulation that is not isolated or technical, or as a matter that must be corrected. For example, failure to take any action in response to an express criticism in a report of examination regarding a failure to appoint a qualified and effective BSA compliance officer could be viewed as an uncorrected previously reported problem that would result in a cease and desist order. Violations or deficiencies in an institution's BSA/AML compliance program communicated to the institution in a report of examination or through other written means that are determined to be isolated or technical are generally not considered problems that would result in a mandatory cease and desist order.

An Agency will ordinarily not issue a cease and desist order under sections 8(s) or 206(q) for failure to correct a BSA/AML compliance program problem unless the problems subsequently found by the Agency are substantially the same as those previously reported to the institution. For example, during a previous examination, an institution's system of internal controls was considered inadequate as a result of substantive deficiencies related to customer due diligence and suspicious activity monitoring processes. Specifically, the institution had not developed customer risk profiles to identify, monitor, and report suspicious activities related to the institution's higher-risk businesses lines. These substantive deficiencies were identified in the previous report of examination as a problem requiring board attention and management's correction. The subsequent report of examination determined that management had not addressed the previously reported problem with the institution's BSA/AML compliance program. Customer risk profiles remained undeveloped to identify, monitor, and report

EXHIBIT 1-B

suspicious activity related to the institution's higher-risk business lines. As a result, the institution would be subject to a cease and desist order for failure to correct a previously reported problem with its BSA/AML compliance program.

In contrast, if an Agency notes in a previous report of examination that an institution's training program was inadequate because it was out of date (for instance, if it did not reflect changes in the law, and at the next examination the training program is adequately updated, but flaws are discovered in the internal controls for the BSA/AML compliance program) the Agency would not issue a cease and desist order under sections 8(s) or 206(q) for failure to correct a previously reported problem and will consider the full range of potential supervisory responses. Similarly, if a violation is cited in a previous report of examination for failure to designate a qualified BSA compliance officer, and the institution has appointed an otherwise qualified person to assume that responsibility by the next examination, but the examiners recommend additional training for the person, an Agency may determine not to issue a cease and desist order under sections 8(s) or 206(q) based solely on that deficiency. Additionally, statements in a report of examination or other written document reported to the board of directors or senior management suggesting areas for improvement, identifying less serious issues, or identifying isolated or technical violations or deficiencies would generally not be considered problems for purposes of sections 8(s) and 206(q).

The Agencies also recognize that certain types of problems with an institution's BSA/AML compliance program may not be fully correctable before the next examination or within the planned timeframes for corrective actions due to unanticipated or other issues. Remedial actions involving multiple lines of business within an institution or the

EXHIBIT 1-B

adoption or conversion of automated systems may take more time to implement than initially anticipated. In these types of situations, a cease and desist order is not required, provided the Agency determines that the institution has made acceptable substantial progress toward correcting the problem.

III. Other Enforcement Actions for BSA/AML Compliance Program Component or Pillar Deficiencies.

As noted above, in addition to the situations described in this statement where an Agency will issue a cease and desist order for a violation of the BSA/AML compliance program regulation or for failure to correct a previously reported BSA/AML compliance program problem, an Agency may also take formal or informal enforcement actions against an institution for other types of BSA/AML compliance program concerns or deficiencies separate from enforcement actions taken under the authorities referred to in sections 8(s) and 206(q).¹¹ In these situations, depending upon the particular facts involved, an Agency may pursue enforcement actions based on individual component or pillar violations or BSA-related unsafe or unsound practices that may impact individual components or pillars. The form and content of the enforcement action in a particular case will depend on the severity of the concerns or deficiencies, the capability and cooperation of the institution's management, and the Agency's confidence that the institution's management will take appropriate and timely corrective action.

IV. Enforcement Actions for Other BSA/AML Requirements.

In appropriate circumstances, an Agency may take formal or informal enforcement actions to address violations of BSA/AML requirements other than the BSA

¹¹ See, e.g., 12 U.S.C. §§ 1786(b); 1818(b).

EXHIBIT 1-B

compliance program or the individual component or pillar requirements. These other requirements include, for example, customer due diligence, beneficial ownership, foreign correspondent banking, and suspicious activity reporting and currency transaction reporting requirements. Also, consistent with the treatment of violations of isolated or technical compliance program requirements, violations of these non-program requirements that are determined by the Agency to be isolated or technical are generally not considered the kinds of problems that would result in an enforcement action.

Suspicious Activity Reporting Requirements.

Under regulations of the Agencies and the Treasury Department, institutions subject to the Agencies' supervision are required to file a SAR when they detect certain known or suspected criminal violations or suspicious transactions.¹² Suspicious activity reporting forms the cornerstone of the BSA reporting system, and is critical to the United States' ability to utilize financial information to combat money laundering, terrorist financing, and other illicit financial activity. The regulations require institutions to file SARs with respect to the following general types of activities:

- known or suspected criminal violations involving insider activity in any amount;
- known or suspected criminal violations aggregating \$5,000 or more when a suspect can be identified;
- known or suspected criminal violations aggregating \$25,000 or more, regardless of potential suspects; or
- suspicious transactions of \$5,000 or more that involve potential money laundering or BSA violations.

¹² 12 C.F.R. §§ 21.11; 163.180(d) (OCC); 208.62, 211.5(k), 211.24(f), 225.4(f) (Federal Reserve); Part 353 (FDIC); 748.1(c) (NCUA); 31 C.F.R. § 1020.320 (Treasury Department).

EXHIBIT 1-B

The SAR must be filed within 30 days of detecting facts that may constitute a basis for filing a SAR (or within 60 days if there is no subject).

The Agencies will cite a violation of the SAR regulations, and will take appropriate supervisory action, if the institution's failure to file a SAR (or SARs) evidences a systemic breakdown in its policies, procedures, or processes to identify and research suspicious activity, involves a pattern or practice of noncompliance with the filing requirement, or represents a significant or egregious situation.

Other BSA Reporting and Recordkeeping Requirements.

Institutions also are subject to other BSA reporting and recordkeeping requirements set forth in regulations issued by the Treasury Department.¹³ These requirements are reviewed in detail in the *FFIEC BSA/AML Examination Manual*; they include, among other things, requirements applicable to cash and monetary instrument transactions and funds transfers, CTR filing and exemption rules, due diligence, certification, and other requirements that may be applicable to customer accounts and foreign correspondent and private banking accounts. As previously noted, the Agencies evaluate these additional regulatory requirements as a part of the internal control component or pillar of the institution's BSA/AML compliance program.

¹³ 31 C.F.R. Part 1010.

Bank Secrecy Act / Anti-Money Laundering Questions

True or False

- _____ 1. The Anti-Drug Abuse Act was the statute that “introduced” what has become known as the Bank Secrecy Act.
- _____ 2. The U.S. Treasury has codified the implementing regulations for BSA at 31 CFR 103, et/seq.
- _____ 3. The U.S. Treasury Bureau charged with managing the Bank Secrecy Act is named CENTIF.
- _____ 4. The Money Laundering Control Act of 1986 not only made structuring a Federal crime, but also stimulated the banking regulatory agencies to implement regulations requiring banks, savings and loans, and credit unions to formally establish a BSA program.
- _____ 5. The Federal bank regulatory agencies are required by statute to examine financial institutions for BSA on a Bi-annual basis.
- _____ 6. Independent testing is not part of the required tenets, or “pillars” of BSA.
- _____ 7. \$100,000,000 is the maximum criminal penalty which can be imposed on a financial institution under the Bank Secrecy Act.
- _____ 8. Hiding lawfully acquired money to avoid the payment of taxes thereon is one example of money laundering currently underway in this country.
- _____ 9. The three stages of money laundering include placement, layering, and interrogation.
- _____ 10. It is widely understood that the largest single generator of illicit proceeds in this country is Las Vegas Casino gaming.
- _____ 11. Only the Federal Deposit Insurance Corporation can bring both informal and formal enforcement actions against financial institutions for BSA failures.
- _____ 12. Although the BSA E-Filing system is safe, secure, and reliable, it does not provide an acknowledgement of filed reports when received.
- _____ 13. The electronic filing of all BSA reports became mandatory on July 1, 2019.
- _____ 14. You not only know the name of, but you personally know, the board appointed BSA Officer for your organization.

CUSTOMER DUE DILIGENCE (CDD)/ ENHANCED DUE DILIGENCE (EDD)

I. CUSTOMER DUE DILIGENCE PROGRAM – Firm Customer Due Diligence (CDD) programs, which encompass and expand on the previous “know your customer” effort, provide the critical framework that enables an institution to comply with regulatory requirements and report suspicious activities. Requiring financial institutions to perform effective CDD so that they understand who their customers are, and what transactions they conduct, is a critical aspect of combatting all forms of illicit financial activity, from terrorist financing and sanctions evasion to more traditional financial crimes including money laundering, fraud, and tax evasion. CDD advances the purposes of the BSA by enhancing the availability to law enforcement agencies of beneficial ownership information, increases the ability of law enforcement and the intelligence community to identify assets and accounts of terrorist organizations, corrupt actors, drug kingpins, and other national security threats, helps financial institutions access and mitigate risk, facilitates improved tax compliance, and advances the Treasury Department’s broad strategy to enhance financial transparency of legal entities.

A. Regulation – The Federal Reserve Board (Fed), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), and the Office of Comptroller of the Currency (OCC) published in December of 1998 proposed regulations which would have required specific “know your customer” policies and procedures. With the withdrawal of the proposal in April of 1999, the regulatory agencies began to encourage financial institutions to establish and maintain “customer due diligence” programs as well as “know your customer” procedures. Enforcement actions issued in 4th quarter 2004 presented the agencies current position on CDD, wherein a financial institution that has failed to conduct a risk assessment of its customer base to identify high-risk customers, products, and geographic locations may be found to have an inadequate system of internal controls that is required under the BSA.

On 03/05/12, FinCEN published an Advanced Notice of Proposed Rulemaking (ANPRM – press release dated 02/29/12) to solicit public comment on a wide range of questions pertaining to the possible application of an explicit customer due diligence (CDD) obligation on financial institutions, including a requirement for financial institutions to identify beneficial ownership of their accountholders. An express CDD program rule is one key element of a broader Treasury strategy to enhance financial transparency in order to strengthen efforts to combat financial crime. On 08/04/14, FinCEN published the formal proposed Rule on Customer Due Diligence Requirements for Financial Institutions, which includes a new regulatory requirement to identify beneficial owners of legal entity customers. On 05/11/16, FinCEN issued final Rules to clarify and strengthen existing CDD requirements and added a new requirement to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exemptions. The effective date of the final Rules is 07/11/2016, with the “Applicability Date” being 05/11/2018 (81FR28398-29458).

B. CDD Elements – The key elements of CDD include:

1. Identifying and verifying the identity of customers;
2. Identifying and verifying the identity of beneficial owners of legal entity customers (i.e. the natural persons who own or control legal entities);

3. Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
4. Conducting on-going monitoring to identify and report suspicious transactions, and on a risk basis, to maintain and update customer information.

Collectively, these elements comprise the minimum standards of CDD, which FinCEN believes are fundamental to an effective AML/BSA program.

NOTE: For FinCEN, the term “customer” includes customers and members. The term “Bank” includes banks, savings associations, and credit unions.

C. Customer Identification Program – The first element of CDD is already a program requirement of an institution’s AML program, and is discussed in Chapter 2 of this manual.

D. Beneficial Ownership – Covered financial institutions (CFI) are required to establish and maintain written procedures that are reasonably designed to identify and verify the beneficial owners of legal entity customers. Financial institutions are also required to include such procedures in their anti-money laundering compliance programs. These procedures shall enable the financial institution to:

1. Identify the beneficial owner(s) of each legal entity at the time a new account is opened, unless the customer is otherwise excluded. A CFI may complete such identification by obtaining from the individual who opens the new account on behalf of the legal entity, either the Certification Form supplied in the regulation, or by some other means provided the individual opening the account certifies, to the best of the individual’s knowledge, the accuracy of the information; (FinCEN believes that the beneficial ownership information must be, at the time of account opening, both (1) current, and (2) certified by an individual authorized by the legal entity customer to open accounts at financial institutions to be accurate to the best of his or her knowledge); and
2. Verify the identity (the existence of, not the status) of each beneficial owner presented to it according to risk based procedures to the extent reasonable and practical. At a minimum, the identification procedures must contain the elements required for verifying the identity of customers that are individuals under the CFI’s Customer Identification Program (CIP). CFIs may use both documentary (E.g. unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a drivers license or passport) and/or non-documentary verification procedures (E.g., contacting the beneficial owner, and/or check references with other financial institutions), assuming such procedures are covered in the CFI’s CIP program.

In the case of documentary verification, the CFI may use photocopies or other reproductions of the documents utilized, though given the vulnerabilities inherent in the reproduction process, CFIs should conduct their own risk-based analyses of the types of photocopies or reproductions that they will accept in accordance with this section so that such reliance is reasonable. (For example, the CFI will not accept reproductions below a

certain optical resolution, or that it will not accept reproductions transmitted via facsimile, or that it will only accept digital reproductions transmitted in certain file formats).

In the case of non-documentary verification, for beneficial owners who are NOT signers on the business account, affirmative consent must be obtained before “pulling” a consumer report under the Fair Credit Reporting Act (FCRA). The verification must be completed within a reasonable period of time after the account is opened. In addition, the developed procedures must address situations in which the CFI cannot form a reasonable belief that it knows the true identity of the beneficial owner(s) of the customer following the required procedures.

NOTE: If the individual identified as a beneficial owner is an existing customer of the financial institution, and is subject to the financial institution’s CIP, a financial institution MAY rely on the information in its possession to fulfill the identification and verification requirements, providing the existing information is up-to-date, accurate, and the legal entity customer’s representative certifies or confirms the accuracy of the pre-existing CIP information. The covered institution’s records of beneficial ownership for the new account could (should) cross-reference the relevant CIP records and the verification of information would not need to be repeated. (Source – FAQ # 7 – April 03, 2018).

3. A CFI may rely on the information supplied by the legal entity customer regarding the identity of its beneficial owner or owners, provided that it has no knowledge of facts that would reasonably call into question the reliability of such information. However, financial institution staff who know, suspect, or have reason to suspect that the customer’s equity holders are attempting to avoid the reporting threshold may, depending on the circumstances, be required to file a SAR.

NOTE: The term covered financial institution (CFI) means an insured bank, a commercial bank, an agency or branch of a foreign bank in the United States, a federally insured credit union, a savings association, et al.

NOTE: The term account means a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit. Account also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, and custodian services. (The term account does not include an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974, as these types of accounts are of extremely low money laundering risk).

NOTE: The term “New Account” means each account opened at a CFI by a legal entity on or after the applicability date (NO “grandfathering”). FinCEN has concluded that while it is not requiring periodic updating of the beneficial ownership information of all legal entity customers at specified intervals, the opening of a new account (even for an existing customer) is a relatively convenient and otherwise appropriate occasion to obtain current information regarding an existing customer’s beneficial owners.

NOTE: When a legal entity customer has previously provided the Certification Form for the beneficial owner(s) of the legal entity customer, the covered institution MAY rely on that information to fulfill the beneficial ownership requirement for subsequent accounts, provided the legal entity customer certifies or confirms that such information is up-to-date and accurate at the time each subsequent account is opened and the financial institution has no knowledge of facts that would reasonably call into question the reliability of such information. The covered institution would need to maintain a record of such certification or confirmation. (Source = FAQ Question # 10 – April 03, 2018)

NOTE: On September 07, 2018, FinCEN issued Ruling FIN-2018-R003, granting exceptive relief to covered financial institutions from the obligations of the Beneficial Ownership Rule and its requirement to identify and verify the identity of the beneficial owner(s) when a legal entity customer opens a new account as a result of the following:

- A rollover of a certificate of deposit (CD);
- A renewal, modification, or extension of a loan (e.g. setting a later payoff date) that does not require underwriting review and approval;
- A renewal, modification, or extension of a commercial line of credit or credit card account (e.g. later payoff date is set) that does not require underwriting review and approval; and
- A renewal of a safe deposit box rental.

The exception only applies to the rollover, renewal, modification, or extension of any of the types of accounts listed above occurring on or after May 11, 2018, and does not apply to the initial opening of such account. Covered institutions must continue to comply with all other applicable anti-money laundering (AML) requirements under the Bank Secrecy Act and its implementing regulations, including program, recordkeeping, and reporting requirements. (This exceptive relief was issued in response to the industry concerns surrounding FAQ # 12 in the April 03, 2018 FAQ document (FIN 2018-G001)).

This exception relieves financial institutions from treating rollovers, loan or safe deposit rental renewals, modifications, or extensions described in this Ruling as new accounts for purposes of the Beneficial Ownership Rule, but it does not relieve financial institutions from their obligation to collect sufficient information to understand the nature and purpose of the customer relationships in order to develop a customer risk profile, as needed as part of the AML program requirement. Regardless of whether an account described in this Ruling was established before or after May 11, 2018, a financial institution has an obligation under its AML program requirement to “conduct ongoing monitoring to identify and report suspicious transactions and on a risk basis, to maintain and update customer information.

For accounts with rollover, renewal, modification, or extension features opened after May 11, 2018, financial institutions must collect the beneficial ownership information as part of the account opening process. Financial institutions will no longer be required however to collect beneficial ownership information for these accounts at each rollover, renewal, extension, or modification for products described in this Ruling.

4. Beneficial Owner is defined using two “prongs”:
- a. Each individual, if any, who directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise, owns 25 percent or more of the equity interests of a legal entity customer (Ownership Prong); AND
 - b. A single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (E.g. CEO, CFO, COO, Managing Member, General Partner, President, Vice President or Treasurer) or any other individual who regularly performs similar functions (Control Prong).

NOTE: The Ownership and Control Prongs, although related, are independent requirements. Thus, satisfaction of, or exclusion from, regulatory obligations under one prong does not mean a covered financial institution’s obligations under the other prong are also satisfied or excluded.

NOTE: The term “equity interests” should be interpreted broadly to apply to a variety of different legal structures and ownership situations. In short, “equity interests” refers to an ownership interest in a business entity. Examples of “equity interests” includes shares of stock in a corporation, membership interests in a limited liability company, and other similar ownership interests in a legal entity.

NOTE: If a trust owns directly or indirectly, 25% or more of the equity interests of a legal entity customer, the beneficial owner under the Ownership Prong is the trustee. Where there are multiple trustees or co-trustees, financial institutions are expected to collect and verify the identity of, at a minimum, one co-trustee of a multi-trustee trust which owns 25 percent or more of the equity interests of the legal entity customer. A covered institution MAY choose to identify additional co-trustees as part of its CDD program.

NOTE: Each prong is intended to be an “independent test” Under the Ownership Prong, up to four individuals may need to be identified and verified. Under the Control Prong, only one individual must be identified. It is possible in some circumstances that the same person or persons may be identified under both prongs.

NOTE: FinCEN reiterates that the 25% threshold is the baseline regulatory benchmark, but CFIs may establish a lower percentage threshold based on their own assessment of risk. CFIs may also determine pursuant to a risk-based approach for their institution, that certain higher risk circumstances may warrant the collection of beneficial ownership information for at least one natural person under the Ownership Prong, even if no beneficial owner meets the 25% threshold. The legal entity customer must provide identifying information for one person with significant managerial control under the Control Prong. CFIs have the discretion to identify additional beneficial owners as appropriate based on risk.

5. Legal Entity Customer is defined to include:

- a. Corporation;
- b. Limited Liability Company;

NOTE: When a legal entity is identified as owning 25 percent or more of the legal entity customer that is opening an account, it **IS** necessary for a covered institution to request beneficial ownership information on the legal entity identified as an owner. Covered institutions must obtain from their legal entity customers, the identities of individuals who satisfy the definition of a legal entity customer either directly or INDIRECTLY through multiple corporate structures. (A covered institution need not independently investigate the legal entity customer's ownership structure and may accept and reasonably rely on the information regarding the status of beneficial owners presented to it by the legal entity customer's representative. (Source - FAQ Question # 3, 04/03/18).

- c. Any other entity that is created by the filing of a public document with the Secretary of State, or similar office – though this definition does not include sole proprietorships or unincorporated associations, even though such businesses may file with the Secretary of State in order to register a trade name or establish a tax account;
- d. General, and Limited Partnerships;
- e. Business trusts that are created through the filing with a State Office; and
- f. Any similar entity formed under the laws of a foreign jurisdiction that opens a new account.

NOTE: Attorney escrow and client trust accounts are treated as intermediary accounts for purposes of beneficial ownership requirements, and the intermediary (not the intermediary's customers) is the customer for purposes of beneficial ownership identification and verification.

6. The following legal entity customers are subject to only the Control Prong of the beneficial ownership requirement:

- a. A pooled investment vehicle that is operated or advised by a financial institution not regulated by a Federal functional regulator or a bank not regulated by a State bank regulator; and
- b. Any legal entity that is established as a nonprofit corporation or similar entity and has filed its organizational documents with the appropriate State authority as necessary. (A nonprofit corporation or similar entity would include, among others, charitable, nonprofit, not-for-profit, nonstock, public benefit or similar corporations, whether or not formally tax-exempt under the internal revenue code. Such an organization could establish that it

is a qualifying entity by providing a certified copy of its Certificate of Good Standing from the appropriate State authority).

7. The term legal entity customer does not include:
- a. Sole Proprietorships;
 - b. Unincorporated Associations – (FinCEN notes that small local community organizations, such as Scout Troops and youth sports leagues, are unincorporated associations rather than legal entities, and therefore not subject to the beneficial ownership requirements);
 - c. Trusts (other than statutory trusts created by the filing with a Secretary of State or similar office) – FinCEN’s understanding is that CFIs are already taking a risk-based approach to collecting information with respect to various persons associated with trusts in order to know the customer and FinCEN expects CFIs to continue these practices as part of overall efforts to safeguard against money laundering and terrorist financing;
 - d. A financial institution regulated by a Federal functional regulator or a bank regulated by a State bank regulator;
 - e. A department or agency of the United States, or any State, or of any political subdivision of any State;
 - f. Any entity established under the laws of the United States, of any State, or of any political subdivision of any State, that exercises governmental authority on behalf of the United States, or any such political subdivision;
 - g. Any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange, or the American Stock Exchange or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (except stocks listed under the separate “NASDAQ Capital Markets Companies” heading). Companies listed on foreign exchanges are NOT excluded from the definition of legal entity customer;
 - h. Any subsidiary, other than a bank, or any entity described in (d) above that is organized under the laws of the United States, or of any State, and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity;
 - i. An issuer of a class of securities registered under Section 12 of the Securities and Exchange Act of 1934;
 - j. An investment company as defined in section 3 of the Investment Company Act of 1940 that is registered with the Securities and Exchange Commission;

- k. An investment adviser, as defined in section 202(a)(11) of the Investment Advisors Act of 1940 and is registered with the Securities and Exchange Commission;
 - l. An exchange or clearing agency as defined in section 3 of the Securities Exchange Act of 1934;
 - m. A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant each as defined in section 1a of the Commodity Exchange Act that is registered with the Commodity Futures Trading Commission;
 - n. A public accounting firm registered under section 102 of the Sarbanes-Oxley Act;
 - o. A bank holding company, as defined in section 2 of the Bank Holding Company Act of 1956, or savings and loan holding company as defined in section 10(n) of the Home Owners' Loan Act;
 - p. A pooled investment vehicle that is operated or advised by a financial institution regulated by a Federal functional regulator or by a State bank regulator;
 - q. An insurance company that is regulated by a State;
 - r. A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010;
 - s. A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
 - t. A non-U.S. governmental department, agency, or political subdivision that engages only in governmental rather than commercial activities; and
 - u. Any legal entity only to the extent that it opens a private banking account subject to the due diligence requirements for private banking accounts found within the BSA. (Private banking for non-U.S. Citizens found within Section 312 of the USA PATRIOT Act.)
8. CFIs are exempt from the requirements to identify and verify the identity of beneficial owners of a legal entity customer that is established:
- a. To provide at the point-of-sale, credit products, including commercial private label credit cards, solely for the purchase of retail goods and/or services at these retailers, up to a limit of \$50,000. (On the other hand, legal entities that issue co-branded credit cards that can be used at any outlet or ATM are not excluded from the definition of legal entity customer, and beneficial ownership information must be obtained by the CFI when opening new accounts for these entities);

- b. To finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of postage products;
- c. To finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker; or
- d. To finance the purchase or leasing of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

NOTE: The exemptions above do not apply to transactions through transaction accounts which a legal entity customer can make payments to, or receive payments from third parties. If there is a possibility of a cash refund on the account activity described above, then beneficial ownership of the legal entity customer must be identified and verified by the CFI either at the time of the initial remittance, or at the time such refund occurs.

- 9. A CFI must establish procedures for making and retaining a record of information obtained under the Beneficial Ownership requirement including:
 - a. The identification information, including the Certification Form (in whatever format is utilized), and the information contained thereon, for five years after the account is closed; and
 - b. The verification information, including a description of any document relied on (noting the type, any identification number, place of issuance, and if any, date of issuance and expiration) and of any non-documentary methods and the results of such methods undertaken, and the resolution of each substantive discrepancy for five years after the record is made.

NOTE: FinCEN expects financial institutions to protect the sensitive personal information collected and retained about the beneficial owners of legal entity customers just as they do CIP information. CFIs are also expected to comply with all applicable Federal and State privacy laws, including but not limited to, the Right to Financial Privacy Act and the Gramm-Leach Bliley Act.

NOTE: These recordkeeping requirements apply to both the information obtained when opening new accounts, and to the information obtained when updating customer and beneficial ownership information on existing accounts.

- 10. A CFI may rely on the performance by another financial institution (including an affiliate) of the identification and verification of beneficial owners of legal entity customers provided that:
 - a. Such reliance is reasonable under the circumstances;
 - b. The other financial institution is subject to BSA and is regulated by a Federal functional regulator; and

- c. The other financial institution enters into a contract requiring it to certify annually to the CFI that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) the specified requirements of the CFI's procedures that comply with the requirements to identify and verify the beneficial owners of legal entity customers.
- 11. FinCEN generally expects the beneficial ownership information to be treated like CIP and related information, and accordingly used to ensure that CFIs comply with other requirements including:
 - a. OFAC – CFIs should use beneficial ownership information to help ensure that they do not open or maintain an account or otherwise engage in prohibited transactions or dealings involving individuals or entities subject to OFAC administered sanctions. (OFAC requires the blocking of accounts of among others, persons appearing on the SDN list, which includes any entity that is 50% or more owned, in the aggregate, by one or more blocked persons, regardless of whether the entity itself is formally listed on the SDN list);
 - b. “Negative Media” searches -- CFIs should also develop risk-based procedures to determine whether and when additional screening of the names of beneficial owners through negative media searches would be appropriate; and
 - c. CTR Aggregation expectations – FinCEN expects CFIs to apply existing procedures consistent with CTR regulations and FinCEN Guidance 2012 – G001 (CTR Aggregation for Businesses with Common Ownership).

A covered financial institution is not required to list the beneficial owners of a business when completing a CTR as a matter of course, unless a beneficial owner was the “person conducting the transaction for another” (Part 1 Box 2b – FinCEN Form 112). (Source - FAQ Question # 33, 04/03/18).

NOTE: FinCEN does not expect the information obtained pursuant to the beneficial ownership information to add additional requirements with respect to Section 314(a) searches performed by CFIs.

- E. Customer Risk Profile** – The third element of CDD requires banks to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. The existing regulations covering suspicious activity reporting require among other things, that banks obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. With that information, transactions that have no business or apparent lawful purpose or are not the sort in which that particular customer would normally be expected to engage in can be identified and reviewed for possible SAR reporting. Developing a customer risk profile by understanding the types of transactions in which a customer would normally be expected to engage forms the baseline against which aberrant suspicious transactions are identified. The addition of this third element into the CDD requirement seeks to merely clarify and explicitly state existing expectations and requirements and is not intended to lower, reduce, or limit the due diligence

expectations of the Federal functional regulators or limit their existing regulatory discretion, nor create any new obligations.

In some circumstances, an understanding of the nature and purpose of a customer relationship can also be developed by inherent or self-evident information about the product or customer type, such as the type of customer, the type of account opened, or the service or product offered, or other basic information about the customer. Such information may be sufficient to understand the nature and purpose of the relationship. Depending on the facts and circumstances, other relevant facts could include basic information about the customer, such as annual income, net worth, domicile, or principle occupation or business as well as, in the case of long standing customers, the customer's history of activity.

- F. Conduct ongoing monitoring to identify and report suspicious transactions, and on a risk basis, to maintain and update customer information.** As SAR reporting actually began in April 1996, banks are already expected to have in place internal controls to provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity. This fourth element simply codifies existing supervisory and regulatory expectations for banks as explicit requirements with FinCEN's AML program requirements in order to make clear that the minimum standards of CDD include ongoing monitoring of ALL transactions by, at, or through, the financial institution. FinCEN clarified that the previous phrase of "monitoring ALL transactions" does not mean that FinCEN expects all accounts to be the subject to a uniform level of scrutiny. Rather, FinCEN expect banks to apply a risk-based approach in determining the level of monitoring to which each account will be subjected. Thus, consistent with current practice, FinCEN would expect the level of monitoring to vary across accounts based on the bank's assessment of the risk associated with the customer and the account. (FinCEN noted that all account relationships would be subject to this requirement merely to reflect the fact that all accounts must necessarily be monitored in some form in order to comply with existing SAR requirements, and not just accounts subject to the CIP Rule).

FinCEN emphasizes that the obligation to update customer information, including beneficial ownership information is triggered only when in the course of normal monitoring, the bank detects information relevant to assessing the risk posed by the customer. This updating customer information requirement is not intended to impose a categorical requirement to update customer or beneficial ownership information on a continuous or ongoing basis. "Monitoring-triggered" updating of beneficial ownership information (as with other customer information) should only occur on a risk basis when material information about a change in beneficial ownership information is uncovered during the course of the bank's normal monitoring, whether at the customer or transaction level. Such "monitoring-triggered" activity could include:

- a. Significant and unexplained change in customer activity; or
- b. Information indicating a possible change in beneficial ownership, such as an unexpected transfer of all of the funds in a legal entity's account to a previously unknown individual.

In addition, the following events should at least trigger a discussion on the change in beneficial ownership:

- c. Change in signers on business account;
- d. Known death of a beneficial owner;
- e. Change of address of business (especially to out-of-state location);
- f. Change in phone number of business;
- g. Known sale of company through media sources; and
- h. Limited Partnership between spouses – Divorce;
- i. Cash Management Agreement Updates;
- j. Phase 2 CTR Exemption annual reviews;
- k. Annual review of credit facility;
- l. SAR Filings – Be Very Careful though;
- m. “Special Circumstances” elevate internally to relationship managers.

FinCEN believes that the updating requirement will apply not only to new customers with new accounts, but to existing customers with existing accounts. Should a CFI learn as a result of its normal monitoring that the beneficial owner of a legal entity customer with an existing account may have changed, the CFI should identify the “new” beneficial owner of such customer.

G. AML Program Updates – By 05/11/2018, CFIs must update their existing AML program requirements to add a fifth “pillar” or “tenet” which states the CFI will have:

- 1. Appropriate risk-based procedures for conducting ongoing customer due diligence, to include, but not be limited to:
 - a. Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
 - b. Conducting ongoing monitoring to identify and report suspicious transactions, and on a risk basis, to maintain and update customer information. Customer information shall include information regarding the beneficial owners of legal entity customers.

The Board of Directors will be expected to approve the updated Anti-money laundering program.

H. Exam Procedures – Beneficial Ownership – On May 11, 2018, the agencies released exam procedures covering the Beneficial Ownership program. Highly qualitative and totally subjective in nature, the Federal examiner will:

- 1. Determine whether the bank has **adequate** written procedures for gathering and verifying information required to be obtained, and retained (including name, physical address, taxpayer identification number, and date of birth) for beneficial owners of legal entity customers who open an account after May 11, 2018.

2. Determine whether the bank has **adequate** risk-based procedures for updating customer information, including beneficial owner information, and maintaining current customer information; and
3. On the basis of examination procedures completed, including transaction testing, **form a conclusion** about the adequacy of procedures for complying with the Beneficial Ownership Rule.

I. Customer Due Diligence (CDD)

The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of risk-based CDD policies, procedures, and processes for ALL customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD is to enable the bank to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious. In accordance with regulatory requirements, all banks must develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence, including but not limited to:

- Obtaining and analyzing sufficient customer information to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile (this concept is commonly referred to as the customer risk rating); and
- Conduct ongoing monitoring to identify and report suspicious transactions, and on a risk basis, maintain and update information, including information regarding the beneficial ownership of legal entity customers.

In addition, the bank's risk-based CDD policies, procedures, and processes should:

- Be commensurate with the bank's BSA/AML risk profile, with increased emphasis on higher risk customers;
- Contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable; and
- Provide standards for conducting and documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

The factors the bank should consider when assessing a customer risk profile are substantially similar to the risk categories considered when determining the bank's overall risk profile. The bank should identify the specific risks of the customer or category of customers, and then conduct analysis of all pertinent information in order to develop the customer's risk profile.

The requirement to update customer information is event-driven and occurs as a result of normal monitoring. Should the bank become aware as a result of its ongoing monitoring that customer information, including beneficial ownership information, has materially changed, it should update the customer information

accordingly. The bank's procedures should establish criteria for when and by whom customer relationships will be reviewed, including updating customer information and reassessing the customer's risk profile. The procedures should indicate who in the organization is authorized to change a customer's risk profile.

- J. Enhanced Due Diligence** – Clients that pose higher money laundering or terrorist financing risks present increased exposure to institutions and as such, due diligence procedures and processes should be enhanced as a result. Higher-risk clients and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship. Institutions may determine that a client poses a higher risk because of the client's business activity, ownership structure, anticipated or actual volumes and types of transactions. In those instances, the following information could be collected on the client including:

1. Purpose of the account;
2. Source of funds and wealth;
3. Occupation or type of business (of the client or other individuals with ownership or control over the account);
4. Financial; statements;
5. Location where the business is organized and where they maintain their principal place of businesses;
6. Proximity of the client's residence, place of employment, or place of business to the financial institution;
7. Description of the client's primary trade area and whether international transactions are expected to be routine;
8. Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and
9. Explanations for changes in account activity.

Financial institutions should take measures to ensure that account profiles are current and monitoring should be risk-based. Institutions must consider whether the risk profiles should be adjusted versus suspicious activity reported when the actual activity is inconsistent with the client's profile.

- K. Exam Procedures – Customer Due Diligence (CDD)** – On May 11, 2018, the agencies released exam procedures covering the Customer Due Diligence requirements. Highly qualitative and totally subjective in nature, the Federal examiner will:

1. Determine whether the bank has developed appropriate written risk-based procedures for conducting ongoing CDD and that they:
 - Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile;
 - Enable the bank to conduct ongoing to monitoring for the purpose of identifying and reporting suspicious transactions and on a risk basis, maintain and update customer information including beneficial ownership information; and
 - Enable the bank to use customer information and the customer risk profile to understand the types of transactions a particular customer

would be expected to engage in and as a baseline against which suspicious transactions are identified.

2. Determine whether the bank has effective processes to develop customer risk profiles that identify the specific risks of individual customers or categories of customers;
3. Determine whether the CDD procedures are commensurate with the bank's BSA/AML risk profile with increased focus on higher risk customers;
4. Determine whether policies procedures, and processes contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable;
5. Determine that the bank has policies, procedures, and processes to identify customers that may pose a higher risk for money laundering or terrorist financing that include whether and/or when, on a risk basis, it is appropriate to obtain and review additional customer information (EDD);
6. Determine whether the bank provides guidance for documenting analysis associated with the due diligence process;
7. Determine whether the bank has defined in its policies, procedures, and processes how customer information, including beneficial ownership information is used to meet other regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties; and
8. Perform transaction testing to determine whether the bank collects appropriate information sufficient to understand the nature and purpose of the customer relationship and effectively incorporates customer information, including beneficial ownership information in the customer risk profile.

On the basis of the examination procedures completed, the examiner will **form a conclusion** about the adequacy of policies, procedures, and processes associated with CDD.

- II. IDENTIFYING SUSPICIOUS TRANSACTIONS** – Money laundering schemes come in a wide variety of forms. As law enforcement efforts have intensified, methods of money laundering have become more sophisticated. Appendix F (Money Laundering and Terrorist Financing Red Flags) in the interagency *Bank Secrecy Act/Anti-Money Laundering Examination Manual (2010)* presents multiple situations that may indicate money laundering and/or terrorist financing. However, just because a transaction appears on the list does not mean that it involves illicit activity, it only means that the transaction requires closer scrutiny. Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime. Many of these activities are suspicious only because they are inconsistent with normal client behavior. Upon closer examination, many may be found to result from legitimate business activity. Similarly, other transactions not mentioned in the Appendix may be suspicious if they

are inconsistent with the normal activity of a particular client or clients of that same type within the DFI's organizational structure.

III. MONEY SERVICES BUSINESSES (MSB) – In August 1999, FinCEN issued regulations which revised the definition of certain non-bank financial institutions, designated those businesses as money services businesses, and required those businesses to “expand” their compliance with the BSA. In July 2011, FinCEN released updated definitions that more clearly delineate the scope of the entities regulated as MSBs so that determining which entities are obligated to comply with the MSB requirements was more straightforward and predictable (76 FR 43585 – 43597). Financial institutions maintaining account relationships with MSBs are exposed to higher risk for potential money laundering and terrorist financing as these entities are less regulated and may have little or no documentation on their clients.

A. Definition – A money services business is defined as a person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the following capacities :

1. Dealer in Foreign Exchange – A person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency of one or more other countries, in an amount greater than \$1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery.
2. Check Cashier – A person that accepts checks (as defined in the Uniform Commercial Code), or monetary instruments (as defined at 31 CFR 1010.100) in return for currency or a combination of currency and other monetary instruments or other instruments in an amount greater than \$1,000 for any person on any day in one or more transactions. Whether a person is a “check cashier” is a matter of facts and circumstances. The term check cashier SHALL include:
 - a. A person engaged in redeeming monetary instruments (including travelers checks and money orders) is a check cashier if it redeems checks for currency or a combination of currency and monetary or other instruments. (This revision does not capture activity that is tantamount to merely exchanging one monetary instrument for another monetary or other instrument, and accordingly requires currency to be included in the redeeming);
 - b. An entity that accepts payment for goods or services with a check and returns more than \$1,000 in currency or a combination of currency and other monetary instruments regardless of the value of the goods or services.

The term check cashier SHALL NOT include:

- a. A person that sells prepaid access in exchange for a check, monetary instrument, or other instrument;

- b. A person that solely accepts monetary instruments as payment for goods and services other than check cashing services;
 - c. A person that engages in check cashing for the verified maker of the check who is a customer otherwise buying goods and services;
 - d. A person that redeems its own checks; or
 - e. A person that only holds a customer's check as collateral for repayment by the customer of a loan.
3. Issuer or Seller of Traveler's Checks or Money Orders – A person that:
- a. Issues traveler's checks or money orders that are sold in an amount greater than \$1,000 to any person on any day in one or more transactions; or
 - b. Sells traveler's checks or money orders in an amount greater than \$1,000 to any person on any day in one or more transactions.
4. Money Transmitter – A person that provides money transmission services. Money transmission services means the acceptance of currency, funds, or other value that substitutes for currency from one person, and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means. "Any means" includes but is not limited to through a financial agency or institution; a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both; an electronic funds transfer system; or an informal value transfer system. Whether a person is a money transmitter is a matter of facts and circumstances and the term "money transmitter" SHALL NOT include a person that only:
- a. Provides the delivery, communication, or network access services used by a money transmitter to support money transmission services;
 - b. Acts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller;
 - c. Operates a clearance and settlement system or otherwise acts as an intermediary solely between BSA regulated institutions. (This includes but is not limited to the Fedwire system, et al).
 - d. Physically transports currency, other monetary instruments, other commercial paper, or other value that substitutes for currency as a person primarily engaged in such business (such as an armored car), from one person to the same person at another location or to an account belonging to the same person at a financial institution;
 - e. Provides prepaid access; or

- f. Accepts and transmits funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds.

NOTE: FinCEN Guidance FIN-2019-G001 (May 09, 2019) provided interpretive guidance to remind persons subject to BSA how FinCEN regulations relating to Money Services Businesses (MSBs) apply to certain business models involving money transmission denominated in value that substitutes for currency, specifically, convertible virtual currencies (CVCs). Exchangers (persons engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency) and administrators (persons engaged as a business in issuing (putting into circulation) and/or have the authority to redeem (withdrawing from circulation) such virtual currency) are considered MSBs. A user of virtual currency, a person that obtains virtual currency to purchase goods or services on the user's own behalf is not considered an MSB.

5. Provider of Prepaid Access – A participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. (The participants in each prepaid access program must determine a single participant within the prepaid program to serve as the provider of prepaid access).
6. Seller of Prepaid Access - Any person that receives funds or the value of funds in exchange for an initial loading or subsequent loading of prepaid access, if that person sells prepaid access offered under a prepaid program that can be used before verification of customer identification, or sells prepaid access (including closed loop prepaid access) to funds that exceed \$10,000 to any person during any one day, and has not implemented policies and procedures reasonably adapted to prevent such sale.
7. United States Postal Service – except with respect to the sale of postage or philatelic products.

FinCEN clarified that whether a person is an MSB depends on the person's activities, and does not depend on whether the person is licensed by the state, whether the person is engaged in a for-profit venture, or whether the person has employees.

B. Exclusions/Inclusions – An MSB is NOT:

1. A bank or a foreign bank;
2. A person registered with a functionally regulated or examined by the SEC or the CFTC, or a foreign financial agency that engages in activities that if were conducted in the United States would cause that foreign agency to be registered with the SEC or CFTC;
3. A natural person who engages in an MSB activity on an infrequent basis and not for gain or profit; or
4. A person that sells prepaid access “outside” of a prepaid program, so long as such sale does not exceed \$10,000 to any person during any one day.

An MSB does INCLUDE:

1. A “foreign-located” MSB, as they now have the same reporting and recordkeeping and other requirements as MSBs with a physical presence in the United States with respect to their activities in the U.S. Foreign-located MSBs are subject to the same civil and criminal penalties as domestic MSBs, and they are also be required to designate a person who resides in the U.S. to function as an agent to accept service of legal process, including with respect to BSA compliance. (This designation is due by 01/23/2012).

- C. Registration and Licensing** - A person that is an MSB solely because that person serves as an agent of another MSB is not required to register, but an MSB that engages in MSB activities on its own behalf, and as an agent for another must register with FinCEN. The registration form for the initial registration period must be filed on or before the end of the 180-day period beginning on the day following the date the business is established. The registration form for the renewal period (each two-calendar-year-period) must be filed on or before the last day of the calendar year preceding the renewal period. Each provider of prepaid access must identify each prepaid program for which it is the provider of prepaid access. Each MSB must maintain a list of its agents (where applicable).

NOTE: State law may also require a MSB to obtain a license to operate from the state.

- D. Currency Transaction Reports** – MSBs must file a report of any transaction which involves currency of more than \$10,000. (The Postal Service is exempt from this requirement in connection with the purchase of postage or philatelic products).
- E. Suspicious Activity Reporting** – MSBs with the exception of check cashers, must file a SAR when the transaction is suspiciously reportable, and is of at least \$2,000. (In special circumstances where the identification of suspicious transactions to be reported is derived from a review of clearance records, an issuer of money orders or traveler’s checks is only required to report a transaction or pattern of transactions that involves or aggregates funds or other assets of at least \$5,000). Note: Now that FinCEN has included the redemption of monetary instruments within the definition of check casher, the SAR filing exclusion for check cashers is being reviewed and could possibly change in the future.
- F. Anti-Money Laundering Programs** – Each MSB shall develop, implement, and maintain an effective anti-money laundering program reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activity. The AML program for MSBs should consist of a system of internal controls, a designated person to assure day-to-day compliance with the program, training for appropriate personnel, and an independent review to monitor and maintain an adequate program. The MSB should also perform a risk assessment in connection with the development of its AML program.
- G. Prepaid Access** – Final Regulations issued 07/29/2011 imposed SAR reporting, and client, and transactional information collection requirements for non-bank providers and sellers of prepaid access, similar to those imposed on other categories of MSBs (76 FR 45403 – 45420). Critical definitions and requirements for these MSBs include:

1. Prepaid Access – defined as access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number. Prepaid access is not a device or a vehicle, but that such a device or vehicle is a means through which prepaid funds are accessed.
2. Closed Loop Prepaid Access – defined as prepaid access to funds or the value of funds that can be used only for goods or services in transactions involving a defined merchant or location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system.
3. Prepaid program – defined as an arrangement under which one or more persons acting together provide(s) prepaid access. An arrangement is NOT a prepaid access program if it:
 - a. provides closed loop prepaid access to funds not to exceed \$2,000 maximum value on any day;
 - b. provides access solely to employment benefits, incentives, wages or salaries, or access to funds not to exceed \$1,000 maximum value and from which no more than \$1,000 maximum value can be initially or subsequently loaded, used, or withdrawn on any day and it does NOT permit:
 - i. funds or value to be transmitted internationally;
 - ii. transfers between or among users within a prepaid program; or
 - iii. loading additional funds or the value of funds from non-depository sources.
 - c. provides prepaid access solely to funds provided by Federal, State, local, or Tribal government agencies;
 - d. provides prepaid access solely to funds from pre-tax flexible spending arrangements for health care or dependent care expenses.
4. Customer Identification – Providers and Sellers of prepaid access must establish procedures to verify the identity of a person who obtains prepaid access under a prepaid program, and obtain identifying information concerning such a person. Such information will be retained for a period of five years from the last use of the device (provider) or from the sale of the device (seller).
5. Additional Records – A provider of prepaid access is required to maintain access to transactional records generated in the ordinary course of business that would be needed to reconstruct prepaid access activation, loads, reloads, purchases, withdrawals, transfers, or other prepaid-related transactions.

H. Federal Guidance – On April 26, 2005, FinCEN and the Agencies released *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States*. The guidance set forth the minimum steps that banking organizations were to take when providing banking services to money services businesses (MSBs). Most importantly, the guidance specifically stated that banking organizations are not expected to act as the *de facto* regulator of the MSB industry, and that banking organizations will not be held responsible for their customers' compliance with the Bank Secrecy Act and other applicable federal and state law regulations. The guidance also clarified that banking organizations have the flexibility to provide services to a wide range of money services businesses while remaining in compliance with the Bank Secrecy Act. The Guidance further indicated that it was essential that banking organizations neither defined nor treated all money services businesses as posing the same level of risk.

1. Registration with FinCEN, if required, and compliance with any state-based licensing requirements represent the most basic of compliance obligations for MSBs, as an MSB operating in contravention of registration or licensing requirements would be violating Federal and possibly state laws. As a result, FinCEN and the Agencies find that it is reasonable and appropriate for a banking organization to insist that an MSB provide evidence of compliance with such requirements or demonstrate that it is not subject to such requirements.
2. At a minimum, the due diligence expectations associated with opening and maintaining accounts for MSBs include:
 - a. Apply CIP at account opening;
 - b. Confirm FinCEN registration if required.
(<https://www.fincen.gov/msb-state-selector>)
 - c. Confirm compliance with state and local licensing requirements, if applicable;
 - d. Confirm agent status, if applicable; and
 - e. Conduct risk assessment to determine whether further due diligence is necessary.
3. Risk Assessment of an MSB client should consider the:
 - a. Types of products and services offered by the MSB;
 - b. Location(s) and market(s) served by the MSB;
 - c. Anticipated account activity; and
 - d. Purpose of the account.
4. The Guidance provided, and the Interagency BSA/AML Examination Guide provides examples of lower risk indicators for an MSB, such as when the MSB:
 - a. Primarily markets to customers that conduct routine transactions with moderate frequency in low amounts;

- b. Offers only a single line of MSB product;
 - c. Check casher that does not accept out of state checks;
 - d. Check casher that does not accept third-party checks or only cashes payroll or government checks;
 - e. Established business with an operating history;
 - f. Only provides services to local residents;
 - g. Only transmits funds to domestic entities;
 - h. Only facilitates domestic bill payments;
 - i. Exhibits expected transaction activity consistent with the profile created at account opening and/or consistent with ongoing expectations;
 - j. Registers and is licensed when required;
 - k. Confirms it is the subject of an AML exam by the IRS or the appropriate state agency; or
 - l. Affirms the existence of a written BSA/AML program and provides the BSA officer's name and contact information.
5. The Guidance also provided examples of higher risk indicators for an MSB, such as when an MSB:
- a. Allows customers to conduct higher-amount transactions with moderate to high frequency;
 - b. Offers multiple types of MSB products;
 - c. Check casher that cashes any third-party check and/or cashes checks for commercial businesses;
 - d. Offers only, or specializes in cross-border transactions;
 - e. A currency dealer/exchanger for currencies of jurisdictions posing heightened risk for money laundering or the financing of terrorism;
 - f. New business without an established operating history; or
 - g. Business located in a HIFCA or HIDTA.
 - h. Provider and seller of prepaid access.
6. For a higher risk MSB, the Guidance suggested banking organizations may pursue some or all of the following as part of an appropriate due diligence/risk management process for these clients:
- a. Review the MSB's AML program;
 - b. Review the results of the MSB's independent test results;
 - c. Conduct on-site visits;
 - d. Review the list of agents that will be receiving services directly or indirectly through the MSB's account;
 - e. Review the MSB's written procedures;

- f. Review the agent management and termination practices for the MSB; or
- g. Review the written employee screening practices for the MSB.

The Guidance also stated the banking organization should decide whether to inquire about the existence and operation of the AML program of a particular MSB.

- 7. The Guidance reminded financial institutions that the identification and reporting of known or suspected violations of law and/or suspicious transactions relevant to possible violations of law or regulation extends to MSB relationships. The Guidance explicitly stated that given the importance of the licensing and registration requirement of an MSB, a banking organization should file a SAR if it becomes aware that a customer is operating in violation of the registration or state licensing requirements. A banking organization is not expected to terminate existing accounts of MSBs based solely on the discovery that the customer is an MSB that has failed to comply with the licensing and registration requirements. The decision to maintain or close an account should be made by a banking organization's management under standards and guidelines approved by the board of directors.

Ongoing monitoring of the MSB relationship should include periodic confirmation that initial projections of account activity have remained reasonably consistent over time, and the Guidance did clarify that risk-based monitoring did not generally include "real-time" monitoring of all transactions flowing through the account of an MSB.

- 8. The Guidance contained an appendix with a set of "Frequently Asked Questions", and is available at: www.fincen.gov.
- 9. On November 10, 2014, FinCEN published "*FinCEN Statement on Providing Banking Services to Money Services Businesses*" reiterating the fact that banking organizations can serve the MSB industry while meeting their Bank Secrecy Act obligations. The statement is available at: www.fincen.gov/news_room/nr/pdf/20141110.pdf.

I. Identifying MSBs - Some of the ways depository financial institutions (DFI) can identify their clients who are MSBs include:

- 1. Asking/probing at the time the relationship is established to determine the MSB status (if any);
- 2. Observe multiple third-party checks being deposited and/or numerous currency withdrawals being made – (RDC is going to make such identification more "challenging");
- 3. Recognize ACH debit settlements originated from major funds transfer, money order, or stored value providers (E.g. Western Union, Amex);
- 4. Client initiates outbound wire transfers going to major funds transfer, money order, or stored value providers; and

5. Personal observations or knowledge of the MSB existence/activities by DFI personnel.
6. Once identified, then the risk assessment can be performed and the appropriate level of due diligence can be applied.

J. Exam Procedures – Contained within the current interagency BSA/AML examination manual are the expanded examination procedures covering the adequacy of the institution's systems to manage the risks associated with the accounts of non-bank financial institutions (NBFIs), including MSBs. Highly qualitative and subjective in nature, the Federal examiner will evaluate the program and assess management's ability to implement effective monitoring and reporting systems by completing a number of reviews that include, but are not limited to:

1. Determining that the institution has policies, procedures, and processes in place for accounts opened or maintained for MSBs;
2. Determining whether the institution assesses the risks posed by MSB clients and is effectively identifying higher-risk accounts and the amount of further due diligence necessary.
3. Determining whether the institution's system for monitoring NBFI accounts for suspicious activities, and the reporting of suspicious activities, is adequate given the nature of the institution's client relationships.

Federally Defined Categories High-Risk Clients and Entities

In identifying those clients who present a “heightened risk” from the BSA/AML perspective, financial institutions could begin with the Federally defined categories of high-risk clients found in the *SAR Activity Reviews*, the *FFIEC BSA/AML Examination Manual*, and the Treasury Department’s National Money Laundering Strategy documents. “High-risk” clients can include customers/members who either are or who:

1. Send money to or from any of the HRNCJ Countries;
2. Located in or are conducting major business transactions in either High Risk Money Laundering and Related Financial Crimes Areas (HIFCAs) or High Intensity Drug Trafficking Areas (HIDTAs) or Narcotics and Bulk Currency Corridors;
3. 314(a) “hits” – assuming the relationship remains;
4. Clients upon whom SARs have been filed upon;
5. Clients upon whom subpoenas or summonses have been received from law enforcement, or IRS garnishments have been processed thereon;
6. IBCs and PICs – International Business Corporations and Private Investment Companies, offshore corporations, domestic shell corporations and foreign corporations;
7. NRAs – non-resident aliens and foreign individuals;
8. Cash-intensive clients (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, vending machine operators, and parking garages.)
9. PSPs – Professional Service Providers – intermediaries between its client and the financial institution – attorneys, accountants, doctors, investment brokers, or real estate brokers, and other third parties, especially those that act as financial liaisons for their clients.
10. Non-Profit Organizations (NPO) (FATF statement July 2014) and Non-Governmental Organizations (NGO), especially those tied to Charities both foreign and domestic;
11. PEPs – Politically Exposed Persons, especially Embassy and Foreign Consulate personnel (On 08/21/20, the Agencies issued a joint statement to address due diligence questions related to the BSA/AML regulatory requirements for clients whom financial institutions may consider PEPs. The Agencies do not interpret the

Federally Defined Categories High-Risk Clients and Entities, Continued

term “politically exposed persons” to include U.S. public officials. Also, the term PEP should not be confused with the term senior foreign political figure (SFPF) as defined under §1010.620 – Due Diligence programs for Private Banking Accounts);

12. MSBs and other NBFIs – Money Services Businesses, and Non-Bank Financial Institutions. (e.g., Casinos and card clubs, brokers and dealers in securities, and dealers in precious metals, stones, or jewels.).
13. Foreign Financial Institutions, including banks and foreign money services providers, especially those dealing in bulk currency shipments.
14. Deposit Brokers, particularly foreign deposit brokers and Ponzi schemes.
15. Privately owned ATMs – Both retail stores and Independent Service Organizations (ISO).
16. Third-Party Payment Processors (TPPP) – See FDIC FIL 41-2014 (07/28/14), FDIC FIL 43-2013 (09/27/13), FinCEN Advisory 2012-A010, and FDIC FIL 3-2012.
17. Real Estate Title and Escrow Companies – Geographic targeting orders in 2016, 2017, 2018, and 2019 and FinCEN Advisory 2017-A003 (08/2017).
18. Statement of Providing Banking Services (FDIC FIL -5-2015) – Dated January 28, 2015, the FDIC wrote that the agency “encourages insured depository institutions to serve their communities and recognizes the importance of the services they provide. Individual customers within broader customer categories present varying degrees of risk. Accordingly, the FDIC encourages institutions to take a risk-based approach in assessing individual customer relationships rather than declining to provide banking services to entire categories of customers, without regard to the risks presented by an individual customer or the financial institutions ability to manage the risk. Financial institutions that can properly manage customer relationships and effectively mitigate risks are neither prohibited nor discouraged from providing services to any category of customer accounts or individual customer operating in compliance with applicable state and federal law..... (Any FDIC-supervised institution concerned that FDIC personnel are not following the policies laid out in this statement may contact the FDIC’s Office of Ombudsman (OO) at 800-756-8854, or via e-mail at bankingservicesOO@fdic.gov).”

HIGH-RISK CATEGORIES/FACTORS

In addition to the Federal “suggestions” on what makes a client “high-risk”, other attendees have shared some of the other factors they have used to identify and create their matrix of “high-risk” clients.

- ♦ Accountants/Tax Preparers
- ♦ Adoption Agencies
- ♦ Adult Book Stores/Massage Parlor
- ♦ Antique Dealers & Antique Cars
- ♦ Animal Sales (e.g., Teddy Bear Puppies)
- ♦ Appraisers/Real Estate Property Managers
- ♦ Aqua Farmers/Hydroponics
- ♦ Arms Dealers
- ♦ Art Dealers (high-end)
- ♦ ATM Servicing Company/ATM Owners
- ♦ Attorneys
- ♦ Auctioneers
- ♦ Auto Salvage/Collision Repair Yard
- ♦ Bait Shops
- ♦ Boat Captains/Boat Dealers/Fishing Vessels
- ♦ Border Trucking Companies
- ♦ Bowling Alley/Pool League/Card Tournament
- ♦ Brothels (Nevada)
- ♦ Bus Companies
- ♦ Campground
- ♦ Car Wash
- ♦ Card Clubs – Legal in some states
- ♦ Carnival
- ♦ Caterer
- ♦ Cattle Buyers
- ♦ Cell Phone Operator (Small)/Mobile Phone Store
- ♦ Charities/Churches
- ♦ Christmas Tree Farms
- ♦ Cigarette Outlets
- ♦ Cleaning Services
- ♦ Collection Agencies
- ♦ Construction Companies/Contractors
- ♦ Cosmetic Surgeons
- ♦ Credit-Repair “Business”
- ♦ Cultural Folk Dancing
- ♦ Day-Care Centers
- ♦ Debt Collection Agency
- ♦ Diamond Merchants
- ♦ Drug Stores
- ♦ Escort Services – Traveling
- ♦ Ethnic Groceries/Bakeries
- ♦ Extended Car–Warranty Companies
- ♦ FBO Centers/Private Aircraft
- ♦ Firewood Sales
- ♦ Fireworks Stands
- ♦ Flea Markets
- ♦ Florist
- ♦ Foreign Accounts/Foreign College Students
- ♦ Freight-Forwarder
- ♦ Fruit Stands – Ethnic and Generic
- ♦ Furniture Rental Stores/Sales Stores
- ♦ FX Dealers
- ♦ Gambler (Professional)
- ♦ Game Processors (Taxidermy)
- ♦ Gas Stations
- ♦ Gun Dealers and On-Line Ammo
- ♦ Herbal Medicine Shops
- ♦ High Wire Transfer Activity
- ♦ Home Health Agency/Cash Only Medical Outlets
- ♦ Honey merchants/jewelry merchants
- ♦ Horse Ranch – Cash Livestock Sales
- ♦ Hot Dog Stands/Lunch Trucks
- ♦ Ice Cream Trucks
- ♦ Import/Export – especially Art Dealers
- ♦ “In the Headlines”
- ♦ Inmate Accounts
- ♦ Investment Club
- ♦ Laundromats/Dry Cleaners
- ♦ Lawn Mowing and Landscaping
- ♦ Leather Goods Store
- ♦ Liquor Stores
- ♦ LLCs – at times associated with shell companies – understand purpose
- ♦ Medical Billing Service
- ♦ MMD- Medical Marijuana Dispensaries/“Potpourri” Shops
- ♦ Mortuaries
- ♦ Movie Theaters
- ♦ Nail Salons/Hair Salons
- ♦ Newsstand
- ♦ Night Clubs/Bars/Bartenders/Dancers
- ♦ No-Name Motels
- ♦ Oil and Gas Brokers
- ♦ Pain Medication Canters/Clinics
- ♦ Painters, Plumbers, Physicians, Preachers, & Policeman
- ♦ Palm-Tree Salesman
- ♦ Parking Structures – looking at where located and how much charged
- ♦ Pawn Shops/Bail Bond Companies
- ♦ Pay-Day Lenders
- ♦ Phone-Card Salespersons
- ♦ Pizza Shops
- ♦ Political P.R. Firms/PACs
- ♦ Psychic
- ♦ Rare Coin Dealers/Bullion Dealers
- ♦ Recycling Centers/Scrap Metal/On-Site Shredding
- ♦ Rehab Centers
- ♦ Restaurants (Ethnic)/Fast Food Outlets
- ♦ Seafood Distributor/Shrimp Boats
- ♦ Self-Storage Facilities
- ♦ Slaughterhouse/Butcher Shop
- ♦ “Soil Company” – “Organic Farming”
- ♦ Sovereign Citizen “crazies”
- ♦ Tanning Booths
- ♦ Tattoo/Piercing
- ♦ Sub-Prime Lenders
- ♦ Taxi Cabs/Uber/Lyft
- ♦ Telemarketers
- ♦ Ticket Broker/Event Promoter
- ♦ Trade-Show Operators
- ♦ Travel Agents
- ♦ Trucking Company
- ♦ Undercover Agents (Rotten)
- ♦ Uninsurable Insurance Company/Insurance Agency
- ♦ Used Car Dealers/ATV Dealers/New Car Dealers
- ♦ “Vape” Shops
- ♦ Used Clothing and textile stores
- ♦ Video Gaming/Poker
- ♦ Wireless Phone Company
- ♦ Worm Farms – Cannabis “Soil”
- ♦ Yacht Builders and Sales
- ♦ Zoo

Below is one example of one format that an FI could use to numerically assign risk-weighting factors to its client base. Factors and Values are presented for example purposes only. FIs must determine their own “factors” and “values” based on local market and industry knowledge.

HIGH-RISK ANALYSIS FACTORS BANK SECRECY ACT

RETAIL / CONSUMER CLIENTS

FACTOR	VALUE
“Normal” Consumer – derived using institutional profile of the “normal consumer” – (E.g. Average Consumer has 4.0 ACH credits, writes 12 physical checks, makes 6 ATM withdrawals, and uses their debit card 8 times/month).	- 0 -
“Not – Normal” consumer	+ 3
Non-U.S. Citizen	+ 3
Politically Exposed Person (PEP)	+ 10
SAR previously filed on consumer	+ 10
Subpoena / summons received from law enforcement	+ 10
Account opened > 10 years	- 2
Loans borrowed and repaid within original terms	- 2
Account opened < 1 year	+ 3
Purchase recordable monetary instruments	+ 3
Utilize Fedwire services (inbound and/or outbound)	+3
Significant Cash Activity	+ 3
Private Banking Client	+ 3
“Out of Market” Client	+ 3
“Other” factors the institution identifies	+ ?

WEIGHTING	RISK RATING
- 4 to + 2	Low
+ 3 to + 8	Medium
+ 9 and >	High

**HIGH-RISK ANALYSIS FACTORS
BANK SECRECY ACT**

BUSINESS / COMMERCIAL CLIENTS

FACTOR	VALUE
Money Services Business – High Risk	+ 15
Money Services Business – Low Risk	+ 5
SAR Previously Filed on Client	+ 15
Charged-Off Loan	+15
Foreign Correspondent Bank	+ 15
Client upon whom subpoenas and summonses have been received from Federal Government and/or law enforcement	+ 15
Account opened > 10 Years	- 5
Account opened > 5 Years	- 3
Loan(s) repaid successfully within original terms and conditions	- 3
Account opened < 1 year	+ 1
Deposit Account Only relationship	+ 1
Located “outside” of market area	+ 1
“High-Risk” Industry – Institutionally defined based on understanding of local industries, markets, and geographies. (E.g. Tobacco Farmer) – Federal Agency guidance utilized as well.	+ 5
Cash Intensive Client	+ 1
Cash Intensive Client – Non Exemptible	+ 5
Utilize Fedwire Services	+ 1
Utilize SWIFT Services	+ 5
ACH Originator	+ 1
Doing Business in a HIFCA and/or HIDTA	+ 1
Business physically located in a HIFCA/HIDTA	+ 5
(Other Factors the institution identifies....)	+ ?

WEIGHTING	RISK RATING
- 5 to +4	Low
+5 to +14	Medium
+ 15 and >	High

RISK ASSESSMENT FORMAT

As the Agencies examine financial institutions for compliance with EDD, documentation of the risk assessment process will be critical to determining the success of the review. Assessments should cover:

- Reasonably foreseeable internal and external threats that lead to the financial institution being used by criminal elements.
- Determine the likelihood and potential damage from each of these threats.
- Identify and consider the sufficiency of existing policies, procedures, systems and other arrangements intended to control the identified risks.

Below is one example of a documentation format that might be utilized to document the efforts:

Client Name/ Account Number(s)	Assigned Officer	Client Type	Risk Type	Risk Weight	Monitoring Process	Training / Development Needed.
Piggly Wiggly #3201 123-4567-8	Branch 47	Retail Grocery	MSB – Checks, Money Orders, Funds Transfers- International, Global Prepaid Access	High – (Federal Definition)	Specific Acct Monitoring; Large Dollar Cash Report; Annual verification documentation request from client.	Relationship Manager – Annual documentation request.
Atta's Import and Export 987-6543-2	Comm. Officer # 2712	International Trader of Silks and Honey	Potential Hawalla & terrorist financier.	High	Review monthly SWIFT and Fedwire Logs & Watch for International ACH activity.	Develop systematic "feeds" from funds transfer systems – perform tracking.
Jefferson County Sheriff's Office 456-7891-2	Comm. Officer # 0001	Public Tax Collector	Received Subpoena for records in connection with Public Fraud case.	High	Review Lockbox Receipts and Account Disbursements to assure consistency.	Develop systematic "feed" from Lockbox system.
Church of St. Mark the Humble. 555-7777-8	Branch # 05	New Religion – Account just opened.	Extremely Cash Intensive Business – Physical building only has three rows of pews.	High	Review Large Cash Transaction Reports – plot cash inflows and map to expectations.	Ensure Branch officer is receiving proper information for monitoring.

Documentation in a format such as above will assist the examiners in understanding the due diligence efforts expended by the financial institution in response to the Process.

Signature: _____ Date: _____

¹ In lieu of a passport number, foreign persons may also provide an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

Legal Entity Identifier _____ (Optional)

PART 1020—RULES FOR BANKS

■ 3. The authority citation for part 1020 continues to read as follows:

Authority: 12 U.S.C. 1829b and 1951–1959; 31 U.S.C. 5311–5314 and 5316–5332; title III, sec. 314 Pub. L. 107–56, 115 Stat. 307.

■ 4. Revise § 1020.210 to read as follows:

§ 1020.210 Anti-money laundering program requirements for financial institutions regulated only by a Federal functional regulator, including banks, savings associations, and credit unions.

A financial institution regulated by a Federal functional regulator that is not subject to the regulations of a self-regulatory organization shall be deemed to satisfy the requirements of 31 U.S.C. 5318(h)(1) if the financial institution implements and maintains an anti-money laundering program that:

(a) Complies with the requirements of §§ 1010.610 and 1010.620 of this chapter;

(b) Includes, at a minimum:

(1) A system of internal controls to assure ongoing compliance;

(2) Independent testing for compliance to be conducted by bank personnel or by an outside party;

(3) Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance;

(4) Training for appropriate personnel; and

(5) Appropriate risk-based procedures for conducting ongoing customer due diligence, to include, but not be limited to:

(i) Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and

(ii) Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. For purposes of this paragraph (b)(5)(ii), customer information shall include information regarding the beneficial owners of legal

entity customers (as defined in § 1010.230 of this chapter); and

(c) Complies with the regulation of its Federal functional regulator governing such programs.

PART 1023—RULES FOR BROKERS OR DEALERS IN SECURITIES

■ 5. The authority citation for part 1023 continues to read as follows:

Authority: 12 U.S.C. 1829b and 1951–1959; 31 U.S.C. 5311–5314 and 5316–5332; title III, sec. 314 Pub. L. 107–56, 115 Stat. 307.

■ 6. Revise § 1023.210 to read as follows:

§ 1023.210 Anti-money laundering program requirements for brokers or dealers in securities.

A broker or dealer in securities shall be deemed to satisfy the requirements of 31 U.S.C. 5318(h)(1) if the broker-dealer implements and maintains a written anti-money laundering program approved by senior management that:

(a) Complies with the requirements of §§ 1010.610 and 1010.620 of this chapter and any applicable regulation of its Federal functional regulator governing the establishment and implementation of anti-money laundering programs;

(b) Includes, at a minimum:

(1) The establishment and implementation of policies, procedures, and internal controls reasonably designed to achieve compliance with the applicable provisions of the Bank Secrecy Act and the implementing regulations thereunder;

(2) Independent testing for compliance to be conducted by the broker-dealer's personnel or by a qualified outside party;

(3) Designation of an individual or individuals responsible for implementing and monitoring the operations and internal controls of the program;

(4) Ongoing training for appropriate persons; and

(5) Appropriate risk-based procedures for conducting ongoing customer due

diligence, to include, but not be limited to:

(i) Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and

(ii) Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. For purposes of this paragraph (b)(5)(ii), customer information shall include information regarding the beneficial owners of legal entity customers (as defined in § 1010.230 of this chapter); and

(c) Complies with the rules, regulations, or requirements of its self-regulatory organization governing such programs; provided that the rules, regulations, or requirements of the self-regulatory organization governing such programs have been made effective under the Securities Exchange Act of 1934 by the appropriate Federal functional regulator in consultation with FinCEN.

PART 1024—RULES FOR MUTUAL FUNDS

■ 7. The authority citation for part 1024 continues to read as follows:

Authority: 12 U.S.C. 1829b and 1951–1959; 31 U.S.C. 5311–5314 and 5316–5332; title III, sec. 314 Pub. L. 107–56, 115 Stat. 307.

■ 8. Revise § 1024.210 to read as follows:

§ 1024.210 Anti-money laundering program requirements for mutual funds.

(a) Effective July 24, 2002, each mutual fund shall develop and implement a written anti-money laundering program reasonably designed to prevent the mutual fund from being used for money laundering or the financing of terrorist activities and to achieve and monitor compliance with the applicable requirements of the Bank Secrecy Act (31 U.S.C. 5311, *et seq.*), and the implementing regulations promulgated thereunder by the



Ruling

Financial Crimes Enforcement Network / U.S. Department of the Treasury

FIN-2018-R003

Issued: September 7, 2018

Subject: **Exceptive Relief from Beneficial Ownership Requirements for Legal Entity Customers of Rollovers, Renewals, Modifications, and Extensions of Certain Accounts**

The Financial Crimes Enforcement Network (FinCEN) grants exceptive relief under the authority set forth in 31 U.S.C. § 5318(a)(7) and 31 CFR § 1010.970(a) to covered financial institutions from the obligations of the Beneficial Ownership Requirements for Legal Entity Customers (Beneficial Ownership Rule)¹ and its requirement to identify and verify the identity of the beneficial owner(s) when a legal entity customer opens a new account as a result of the following:

- A rollover of a certificate of deposit (CD) (as defined below);
- A renewal, modification, or extension of a loan (e.g., setting a later payoff date) that does not require underwriting review and approval;
- A renewal, modification, or extension of a commercial line of credit or credit card account (e.g., a later payoff date is set) that does not require underwriting review and approval; and
- A renewal of a safe deposit box rental.

The exception only applies to the rollover, renewal, modification or extension of any of the types of accounts listed above occurring on or after May 11, 2018, and does not apply to the initial opening of such accounts.² Notwithstanding this exception, covered financial institutions must continue to comply with all other applicable anti-money laundering (AML) requirements under the Bank Secrecy Act (BSA) and its implementing regulations, including program, recordkeeping, and reporting requirements.

1. 31 CFR §1010.230. "Covered financial institutions" are banks, brokers or dealers in securities, mutual funds, futures commission merchants, and introducing brokers in commodities.
2. Covered financial institutions are not excepted from the obligation to identify and verify the identity of the beneficial owner(s) of legal entity customers at the initial account opening for such accounts occurring on or after May 11, 2018.

Background

In its response to Question Number 12 in the April 3, 2018 Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (FAQs),³ FinCEN stated “[c]onsistent with the definition of ‘account’ in the CIP [Customer Identification Program] rules and subsequent interagency guidance, each time a loan is renewed or a certificate of deposit is rolled over, the bank establishes another formal banking relationship and a new account is established.”⁴ FinCEN therefore noted that because CD rollovers (or certain loan renewals) are the establishment of a new account relationship and covered financial institutions are required to obtain information on the beneficial owners of a legal entity that opens a new account, even for existing customers, covered financial institutions must obtain the required information at the first renewal following the applicability date of the Beneficial Ownership Rule. Since the FAQs were issued, financial institutions represented that it is industry practice not to treat such rollovers and renewals as the opening of a new account, because, among other factors, there is generally no change to account information. Accordingly, industry representatives requested that FinCEN either except these accounts from the obligations of the Beneficial Ownership Rule or delay the implementation of the Rule for the products and services referenced in the FAQ to allow the industry adequate time to come into compliance.

In response, on May 16, 2018, FinCEN issued a 90-day temporary and limited exceptive relief, retroactive to May 11, 2018, and which FinCEN extended an additional 30 days, to covered financial institutions from the obligations of the Beneficial Ownership Rule in order to determine whether, and to what extent, a further exception would be appropriate for certain products and services. The exception applied to covered financial products and services that automatically rollover or renew (i.e., CD or loan accounts) and were established before the Beneficial Ownership Rule’s Applicability Date of May 11, 2018. This exceptive relief replaces and supersedes the May 16, 2018, 90-day limited exceptive relief, as well as the August 8, 2018, 30-day extension.

Since May 11, 2018, FinCEN has met with stakeholders, including representatives from financial institutions, trade associations, regulators, and law enforcement to obtain feedback on implementation of the Beneficial Ownership Rule for CDs and loans, including rollovers and renewals, established before May 11, 2018 and that are expected to rollover or renew after that date. FinCEN also received feedback from stakeholders through the FinCEN Resource Center.

-
3. See, “Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions,” (April 3, 2018), https://www.fincen.gov/sites/default/files/2018-04/FinCEN_Guidance_CDD_FAQ_FINAL_508_2.pdf.
 4. See, “Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act, FAQs: Final CIP Rule,” p. 8 (April 28, 2005) <https://www.fincen.gov/sites/default/files/guidance/faqsfinalciprule.pdf>.
-

Based on those discussions and feedback, FinCEN obtained additional information on the characteristics and the money laundering risks posed by those products and the practical impact the Beneficial Ownership Rule had on those products.

COVERED PRODUCT DESCRIPTIONS AND CHARACTERISTICS

Certificates of Deposit

For purposes of this Ruling, a certificate of deposit (CD) is a deposit account that has a specified maturity date, but cannot be withdrawn before that date without incurring a penalty.⁵ During the term of the CD, a customer cannot add additional funds to the CD. The term of a CD may vary from a week to several years. At the end of the term, when the CD matures, the customer is entitled to the amount deposited and any interest that has accrued; the customer may also have the ability to elect to either renew or close the account. Typically, the account will automatically renew absent affirmative action by the customer to close the account.

Loan Renewals, Modifications, and Extensions

Generally, a loan account is an account created to track transactions related to a loan that has terms and conditions tailored to the needs and circumstances of the customer, such that the issuance of a new loan would result in a new account relationship. However, once a loan application process is finalized and a loan approved, a financial institution may renew, extend, or otherwise modify the loan without substantively changing the terms or requiring additional underwriting. Industry has also represented that, as with CDs, some loans are subject to automatic renewal, modification, or extension within a specified time and require no action from the customer for that renewal, modification, or extension to take effect.

Commercial Lines of Credit and Credit Cards

A commercial line of credit account is a type of revolving loan account that allows a commercial enterprise to draw upon a predetermined amount of funds and generally use those funds only for specified business purposes. Small businesses rely on this mode of financing to cover short-term needs such as paying suppliers and addressing payroll needs. A business customer can repay the line at any time by making payment to the financial institution through the account, at which point those funds become available for borrowing again. Credit card accounts are revolving

5. The definition of “CD” for the purposes of this Ruling differs from the definition of “time deposit” in Regulation D of the Board of Governors of the Federal Reserve System (Reserve Requirements of Depository Institutions, 12 CFR Part 204); see 12 CFR 204.2(c)(i).

accounts, similar to commercial line of credit accounts, that grant the customer a maximum credit limit, which can generally be used repeatedly so long as the limit is not exceeded. The financial institution may change certain terms of a commercial line of credit or of a credit card, such as the credit limit, without requiring the affirmative assent of the customer.

Safe Deposit Boxes

Financial institutions maintain safe deposit boxes within their institutions that they rent to individuals and legal entities to store valuables such as collectibles, documents, and jewelry. While financial institutions do not have access to the contents of a safe deposit box rented to a customer, under the terms of the rental agreement, customers are not permitted to store money or dangerous substances in them. In exchange for the use of the safe deposit box, the customer generally pays a rental fee that is electronically deducted from an account provided to the financial institution. During the rental period, the financial institution has minimal or no communication with the customer, so long as the rental payment is made.

ANALYSIS

Additional Information from Industry

After FinCEN issued the temporary exception on May 16, 2018, covered financial institutions explained that the burden of complying with the Beneficial Ownership Rule with respect to renewals of CDs, certain loan and credit accounts, and safe deposit box rentals was not, in their view, commensurate with the low money laundering risks associated with the renewal of these particular products. They indicated that applying the Beneficial Ownership Rule, with its requirement to collect certain information before account rollover, renewal, modification, or extension, would be costly, burdensome, and would have a significant impact on financial products and services that many small businesses rely upon to manage their cash flow and liquidity. The current industry practice for renewing or extending these types of account relationships is generally automated and does not require an affirmative action from the customer. Any delay by the customer in providing the required beneficial ownership information could result in account closure and a corresponding loss of needed liquidity or financial stability (in the case of a loan account) or loss of investment benefit (in the case of a CD).

Furthermore, financial institutions indicated that implementation of the Beneficial Ownership Rule for these accounts would require information technology (IT) system upgrades as some of these accounts, such as a CD, might renew every week or month. Moreover, in the case of a CD, the financial institution's IT operation systems may

automatically roll over the CD if the customer does not communicate to the financial institution that the customer will remove the funds and close the CD. Similarly, a safe deposit box rental may automatically renew through an institution's IT systems, provided that the customer pays the renewal or rental fee, or such fee is available for automatic deduction from an account the customer has provided to the financial institution. The automated rollover or renewal characteristics of these products have therefore presented certain implementation challenges for financial institutions.

Money Laundering and Terrorist Financing Risks

Each of the account relationships described in this exceptive relief presents low risks for money laundering and terrorist financing (ML/TF) because the features of the account make their use for ML/TF activity impractical. For example, CDs and safe deposit boxes are non-transactional, that is, customers cannot use either of them to pay or receive payments from a third party. In addition, funds cannot be transferred into or out of the CD during the term of the account relationship. Moreover, customer information, including beneficial ownership information, is collected about the customer at account opening in order to understand the nature and purpose of the customer relationship, create a customer risk profile, monitor account activity, and report suspicious activity, when appropriate. A financial institution providing a loan or line of credit to a customer must collect customer identification and other background information to determine the creditworthiness of the customer to assess against the institution's risk tolerance. This customer information obtained at the establishment of the relationship, which often includes information on the customer's beneficial owner(s), would generally be sufficient for covered financial institutions to understand who their customers are and the type of transactions they conduct in order to assess ML/TF risks and identify suspicious activity.

Information Available to Law Enforcement

FinCEN also considered the extent to which the application of the Beneficial Ownership Rule would provide information that is of a high degree of usefulness to law enforcement and other FinCEN stakeholders. The exception affects the accounts described in this Ruling in two ways: by removing the obligation to collect beneficial ownership information when an account opened before May 11, 2018 rolls over or renews after May 11, 2018, as if it were a new account, and by removing that same obligation for rollovers, modifications, extensions, and renewals of such accounts opened after May 11, 2018. However, the removal of these obligations does not have a significant impact on the information available and useful to law enforcement.

This exception relieves financial institutions from treating rollovers, loan or safe deposit rental renewals, modifications, or extensions described in this Ruling as new accounts for purposes of the Beneficial Ownership Rule, but it does not relieve

financial institutions from their obligation to collect sufficient information to understand the nature and purpose of customer relationships in order to develop a customer risk profile, as needed as part of the AML program requirement. Regardless of whether an account described in this Ruling was established before or after May 11, 2018, a financial institution has an obligation under its AML program requirement to “conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.”⁶

For accounts with rollover, renewal, modification or extension features opened after May 11, 2018, financial institutions must collect the beneficial ownership information, as part of the account opening process. Financial institutions will no longer be required, however, to collect beneficial ownership information for these accounts at each rollover, renewal, extension, or modification for products described in this Ruling.

CONCLUSION

Under 31 U.S.C. § 5318(a)(7) and 31 CFR § 1010.970(a), FinCEN has the authority to grant exceptions to the requirements of 31 CFR Chapter X. Such exceptions may be either conditional or unconditional and may apply to particular persons or classes of persons, but only to the extent that such limits are expressly stated in the order of authorization. Exceptions may be revoked at FinCEN’s discretion.

Accordingly, FinCEN is granting exceptive relief to covered financial institutions from the Beneficial Ownership Rule’s requirement to identify and verify beneficial ownership information on or after May 11, 2018, as a result of the following: (1) CD rollovers; (2) loan renewals, modifications, and extensions (e.g., setting a later payoff date) that do not require underwriting review and approval; (3) commercial line of credit or credit card account renewals, modifications, or extensions (e.g., setting a later payoff date) that do not require underwriting review and approval; and (4) safe deposit box rental renewals. This exceptive relief does not apply to the initial opening of any of the types of accounts listed above, nor does it apply to relieve any covered financial institution of its customer due diligence requirements under AML program rules. Notwithstanding this permanent excepted relief, covered financial institutions must comply with all other applicable AML requirements under the BSA, such as maintaining an AML program and reporting suspicious activity.

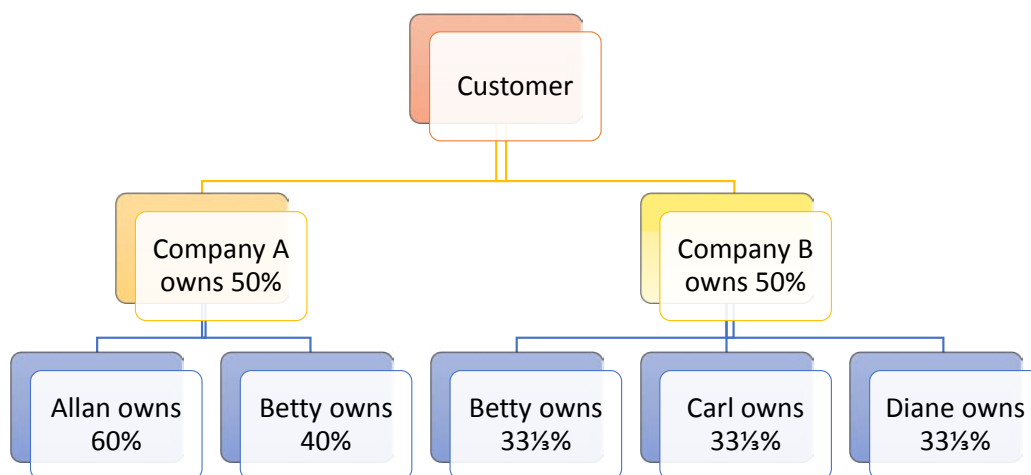
6. See, 31 CFR § 1020.210(b)(5) regarding AML program requirements for banks, savings associations, and credit unions.

Question 3: Collection of beneficial ownership information for direct and indirect owners: Legal entity customers with complex ownership structures

When a legal entity is identified as owning 25 percent or more of a legal entity customer that is opening an account, is it necessary for a covered financial institution to request beneficial ownership information on the legal entity identified as an owner?

- A. Under the Rule's beneficial ownership identification requirement, a covered institution must collect, from its legal entity customers, information about any individual(s) that are the beneficial owner(s) (unless the entity is excluded or the account is exempted). Therefore, covered financial institutions must obtain from their legal entity customers the identities of individuals who satisfy the definition, either directly or indirectly through multiple corporate structures, as illustrated in the following example.

For purposes of the Rule, Allan is a beneficial owner of Customer because he owns indirectly 30 percent of its equity interests through his direct ownership of Company A. Betty is also a beneficial owner of Customer because she owns indirectly 20 percent of its equity interests through her direct ownership of Company A plus $16\frac{2}{3}$ percent through Company B for a total of indirect ownership interest of $36\frac{2}{3}$ percent. Neither Carl nor Diane is a beneficial owner because each owns indirectly only $16\frac{2}{3}$ percent of Customer's equity interests through their direct ownership of Company B.



A covered financial need not independently investigate the legal entity customer's ownership structure and may accept and reasonably rely on the information regarding the status of beneficial owners presented to the financial institution by the legal entity customer's representative, provided that the institution has no knowledge of facts that would reasonably call into question the reliability of the information.

Question 4: Identification and Verification: Methods of verifying beneficial ownership information

What means of identity verification are sufficient to reliably confirm beneficial ownership under the CDD Rule?

- A. Covered financial institutions must verify the identity of each beneficial owner according to risk-based procedures that contain, at a minimum, the same elements financial institutions are required to use to verify the identity of individual customers under applicable Customer Identification Program ("CIP") requirements. This includes the requirement to address situations in which the financial institution cannot form a reasonable belief that it knows the true identity of the legal entity customer's beneficial owners.² Although the CDD Rule's beneficial ownership verification procedures must contain the same elements as existing CIP procedures, they are not required to be identical to them.³ For example, a covered financial institution's policies and procedures may state that the institution will accept photocopies of a driver's license from the legal entity customer to verify the beneficial owner(s)' identity if the beneficial owner is not present, which is not permissible in the CIP rules. (See Question 6.)

A financial institution's CIP must contain procedures for verifying customer identification, including describing when the institution will use documentary, non-documentary, or a combination of both methods for identity verification.⁴ Covered financial institutions may use the same methods to verify the identity of the beneficial owner of a legal entity customer. In addition, in contrast to the CIP rule, the CDD Rule expressly authorizes covered financial institutions to use photocopies or other reproduction documents for documentary verification.⁵

-
2. Under the CIP rules, a financial institution's CIP must include procedures for responding to circumstances in which the financial institution cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe: (1) when the institution should not open an account; (2) the terms under which a customer may use an account while the institution attempts to verify the customer's identity; (3) when it should close an account, after attempts to verify a customer's identity have failed; and (4) when it should file a Suspicious Activity Report in accordance with applicable laws and regulations. *See, e.g.,* 31 CFR 1020.220(a)(2)(iii).
3. *See* 31 CFR 1020.220(a)(2); 31 CFR 1023.220(a)(2); 31 CFR 1024.220(a)(2); or 31 CFR 1026.220(a)(2).
4. *See* 31 CFR 1020.220 (a)(2)(ii).
5. *See* 31 CFR 1010.230(b)(2).
-

Beneficial Ownership Requirements for Legal Entity Customers – Overview

Objective. *Assess the bank's written procedures and overall compliance with regulatory requirements for identifying and verifying beneficial owner(s) of legal entity customers.*

Under the Beneficial Ownership Rule,¹ a bank must establish and maintain written procedures that are reasonably designed to identify and verify beneficial owner(s) of legal entity customers and to include such procedures in its anti-money laundering compliance program.

Legal entities, whether domestic or foreign, can be used to facilitate money laundering and other crimes because their true ownership can be concealed. The collection of beneficial ownership information by banks about legal entity customers can provide law enforcement with key details about suspected criminals who use legal entity structures to conceal their illicit activity and assets. Requiring legal entity customers seeking access to banks to disclose identifying information, such as the name, date of birth, and Social Security number of natural persons who own or control them will make such entities more transparent, and thus less attractive to criminals and those who assist them.

Similar to other customer information that a bank may gather, beneficial ownership information collected under the rule may be relevant to other regulatory requirements. These other regulatory requirements include, but are not limited to, identifying suspicious activity, and determining Office of Foreign Assets Control (OFAC) sanctioned parties. Banks should define in their policies, procedures, and processes how beneficial ownership information will be used to meet other regulatory requirements.

Legal Entity Customers

For the purposes of the Beneficial Ownership Rule,² a legal entity customer is defined as a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or other similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account. A number of types of business entities are excluded from the definition of legal entity customer under the Beneficial Ownership rule. In addition, and subject to certain limitations, banks are not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens certain types of accounts. For further information on exclusions and exemptions to the Beneficial Ownership Rule, see Appendix 1. These exclusions and exemptions do not alter or supersede other existing requirements related to BSA/AML and OFAC sanctions.

Beneficial Owner(s)

Beneficial ownership is determined under both a control prong and an ownership prong. Under the control prong, the beneficial owner is a single individual with significant

¹ See 31 CFR 1010.230

² See 31 CFR 1010.230(e)(1)

responsibility to control, manage or direct a legal entity customer.³ This includes, an executive officer or senior manager (Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, President), or any other individual who regularly performs similar functions. One beneficial owner must be identified under the control prong for each legal entity customer.

Under the ownership prong, a beneficial owner is each individual, *if any*, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer.⁴ If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, the beneficial owner is the trustee.⁵ Identification of a beneficial owner under the ownership prong is *not required* if no individual owns 25 percent or more of a legal entity customer. Therefore, all legal entity customers will have a total of between one and five beneficial owner(s) – one individual under the control prong and zero to four individuals under the ownership prong.

Banks may rely on the information supplied by the legal entity customer regarding the identity of its beneficial owner or owners, provided that it has no knowledge of facts that would reasonably call into question the reliability of such information.⁶ However, bank staff who know, suspect, or have reason to suspect that equity holders are attempting to avoid the reporting threshold may, depending on the circumstances, be required to file a SAR.⁷ More information on filing of SARs may be found in the “Suspicious Activity Reporting Overview” section on page 60 of the *FFIEC BSA/AML Examination Manual*.

Identification of Beneficial Ownership Information

A bank must establish and maintain written procedures detailing the identifying information that must be obtained for each beneficial owner of a legal entity customer opening a new account after May 11, 2018. At a minimum, the bank must obtain the following identifying information for each beneficial owner of a legal entity customer:

- Name.
- Date of birth.
- Address.⁸

³ See 31 CFR 1010.230(d)(2)

⁴ See 31 CFR 1010.230(d)(1)

⁵ See 31 CFR 1010.230(d)(3)

⁶ See 31 CFR 1010.230(b)(2)

⁷ Department of the Treasury, Financial Crimes Enforcement Network (2016), “Customer Due Diligence Requirements for Financial Institutions,” final rules (RIN 1506-AB25), *Federal Register*, vol. 81 (May 11), p. 29410.

⁸ For an individual: a residential or business street address, or if the individual does not have such an address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer’s physical location. For a person other than an individual (such as a corporation, partnership, or trust): a principal place of business, local office, or other physical location. See 31 CFR 1010.220(a)(2)(i)(3)

- Identification number.⁹

A bank may obtain identifying information for beneficial owner(s) of legal entity customers through a completed certification form¹⁰ from the individual opening the account on behalf of the legal entity customer, or by obtaining from the individual the information required by the form by another means, provided the individual certifies, to the best of the individual's knowledge, the accuracy of the information. A bank may rely on the information supplied by the individual opening the account on behalf of the legal entity customer regarding the identity of its beneficial owner(s), provided that it has no knowledge of facts that would reasonably call into question the reliability of such information. If a legal entity customer opens multiple accounts a bank may rely on the pre-existing beneficial ownership records it maintains, provided that the bank confirms (verbally or in writing) that such information is up-to-date and accurate at the time each account is opened.¹¹

Banks must have procedures to maintain and update customer information, including beneficial ownership information for legal entity customers, on the basis of risk. Additionally, banks are not required to conduct retroactive reviews to obtain beneficial ownership information on legal entity customers that were existing customers as of May 11, 2018. However, the bank may need to obtain (and thereafter update) beneficial ownership information for existing legal entity customers based on its ongoing monitoring. For further guidance on maintaining and updating of customer information including beneficial ownership information, please see the “Ongoing Monitoring of Customer Relationship” section of the “Customer Due Diligence Overview” section of the *FFIEC BSA/AML Examination Manual*.¹²

Verification of Beneficial Owner Information

A bank must establish and maintain written risk-based procedures for verifying the identity of each beneficial owner of a legal entity customer within a reasonable period of time after the account is opened. These procedures must contain the elements required for verifying the identity of customers that are individuals under 31 CFR 1020.220(a)(2), provided, that in the case of documentary verification, the bank may use photocopies or other reproductions of the documents listed in paragraph (a)(2)(ii)(A)(I) of 31 CFR 1020.220. Guidance on documentary and non-documentary verification methods may be found in the core overview section “Customer Identification Program,” of the *FFIEC BSA/AML Examination Manual*.

⁹ An identification number for a U.S. person is a taxpayer identification number (TIN) (or evidence of an application for one), and an identification number for a non-U.S. person is one or more of the following: a TIN; a passport number and country of issuance; an alien identification card number; or a number and country of issuance of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. TIN is defined by section 6109 of the Internal Revenue Code of 1986 (26 USC 6109) and the IRS regulations implementing that section (e.g., Social Security number (SSN) or individual taxpayer identification number (ITIN), or employer identification number (EIN)). See 31 CFR 1010.220(a)(2)(i)(4).

¹⁰ See 31 CFR 1010.230, Appendix A, *Certification Regarding Beneficial Owners of Legal Entity Customers* (2016).

¹¹ FinCEN, FIN-2018-G001, *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions*, Question #10, April 2018.

¹² FFIEC, *Core Examination Overview and Procedures, Customer Due Diligence Overview*, May 2018.

A bank need not establish the accuracy of every element of identifying information obtained, but must verify enough information to form a reasonable belief that it knows the true identity of the beneficial owner(s) of the legal entity customer. The bank's procedures for verifying the identity of the beneficial owners must describe when it uses documents, non-documentary methods, or a combination of methods.

Lack of Identification and Verification of Beneficial Ownership Information

Also consistent with 31 CFR 1020.220, the bank should establish policies, procedures, and processes for circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the beneficial owner(s) of a legal entity customer. These policies, procedures, and processes should describe:

- Circumstances in which the bank should not open an account.
- The terms under which a customer may use an account while the bank attempts to verify the identity of the beneficial owner(s) of a legal entity customer.
- When the bank should close an account, after attempts to verify the identity of the beneficial owner(s) of a legal entity customer have failed.
- When the bank should file a SAR in accordance with applicable law and regulation.

Recordkeeping and Retention Requirements

A bank must establish recordkeeping procedures for beneficial ownership identification and verification information. At a minimum, the bank must maintain any identifying information obtained, including without limitation the certification (if obtained), for a period of five years after the date the account is closed.

The bank must also keep a description of any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration), of any non-documentary methods and the results of any measures undertaken, and of the resolution of each substantive discrepancy for five years after the record is made.

Reliance on Another Financial Institution

A bank is permitted to rely on the performance by another financial institution (including an affiliate) of the requirements of the Beneficial Ownership Rule with respect to any legal entity customer of the covered financial institution that is opening, or has opened, an account or has established a similar business relationship with the other financial institution to engage in services, dealings, or other financial transactions, provided that:

- Reliance is reasonable, under the circumstances.
- The relied-upon financial institution is subject to a rule implementing 31 USC 5318(h) and is regulated by a federal functional regulator.¹³

¹³ Federal functional regulator means: Federal Reserve, FDIC, NCUA, OCC, U.S. Securities and Exchange Commission (SEC), or U.S. Commodity Futures Trading Commission (CFTC).

- The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the bank's procedures to comply with the requirements of the Beneficial Ownership Rule.

Examination Procedures

Beneficial Ownership

Objective: *Assess the bank's written procedures and overall compliance with regulatory requirements for identifying and verifying beneficial owner(s) of legal entity customers.*

1. Determine whether the bank has adequate written procedures for gathering and verifying information required to be obtained, and retained (including name, address, taxpayer identification number (TIN), and date of birth) for beneficial owner(s) of legal entity customers who open an account after May 11, 2018.
2. Determine whether the bank has adequate risk-based procedures for updating customer information, including beneficial owner information, and maintaining current customer information.

Transaction Testing

3. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of new accounts opened for legal entity customers since May 11, 2018 to review for compliance with the Beneficial Ownership Rule. The sample should include a cross-section of account types. From this sample, determine whether the bank has performed the following procedures:
 - Opened the account in accordance with the requirements of the Beneficial Ownership Rule (31 CFR 1010.230).
 - Obtained the identifying information for each beneficial owner of a legal entity customer as required (e.g. name, date of birth, address, and identification number).
 - Within a reasonable time after account opening, verified enough of the beneficial owner's identity information to form a reasonable belief as to the beneficial owner's true identity.
 - Appropriately resolved situations in which beneficial owner's identity could not be reasonably established.
 - Maintained a record of the identity information required by the Beneficial Ownership Rule, the method used to verify identity, and verification results (31 CFR 1010.230(i)).
 - Filed SARs as appropriate.
4. On the basis of the examination procedures completed, including transaction testing, form a conclusion about the adequacy of procedures for complying with the Beneficial Ownership Rule

Appendix 1 – Beneficial Ownership

Exclusions from the definition of Legal Entity Customer

Under 31 CFR 1010.230(e)(2) a legal entity customer does not include:

- A financial institution regulated by a federal functional regulator¹⁴ or a bank regulated by a state bank regulator;
- A person described in 31 CFR 1020.315(b)(2) through (5):
 - A department or agency of the United States, of any state, or of any political subdivision of any State;
 - Any entity established under the laws of the United States, of any state, or of any political subdivision of any state, or under an interstate compact between two or more states, that exercises governmental authority on behalf of the United States or any such state or political subdivision;
 - Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange (currently known as the NYSE American) or have been designated as a NASDAQ National Market Security listed on the NASDAQ stock exchange (with some exceptions);
 - Any subsidiary (other than a bank) of any “listed entity” that is organized under the laws of the United States or of any state and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity, provided that a person that is a financial institution, other than a bank, is an exempt person only to the extent of its domestic operations;
- An issuer of a class of securities registered under section 12 of the Securities Exchange Act of 1934 or that is required to file reports under section 15(d) of that Act;
- An investment company, investment adviser, an exchange or clearing agency, or any other entity that is registered with the SEC;
- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant that is registered with the CFTC;
- A public accounting firm registered under section 102 of the Sarbanes-Oxley Act;
- A bank holding company or savings and loan holding company;
- A pooled investment vehicle that is operated or advised by a financial institution that is excluded under paragraph (e)(2);
- An insurance company that is regulated by a state;

¹⁴ Federal functional regulator means: Federal Reserve, FDIC, NCUA, OCC, U.S. Securities and Exchange Commission (SEC), or U.S. Commodity Futures Trading Commission (CFTC).

- A financial market utility designated by the Financial Stability Oversight Council;
- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
- A non-U.S. governmental department, agency, or political subdivision that engages only in governmental rather than commercial activities;
- Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620.

Trusts

Trusts are not included in the definition of legal entity customer, other than statutory trusts created by a filing with a Secretary of State or similar office.¹⁵

Exemptions from the Ownership Prong

Certain legal entity customers are subject only to the control prong of the beneficial ownership requirement, including:

- A pooled investment vehicle operated or advised by a financial institution not excluded under paragraph 31 CFR 1010.230(e)(2); and
- Any legal entity that is established as a nonprofit corporation or similar entity and has filed its organizational documents with the appropriate state authority as necessary.

Exemptions and Limitations on Exemptions

Subject to certain limitations, banks are not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens any of the following categories of accounts:

- Accounts established at the point-of-sale to provide credit products, including commercial private label credit cards, solely for the purchase of retail goods and/or services at these retailers, up to a limit of \$50,000;
- Accounts established to finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of the postage products;
- Accounts established to finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker;
- Accounts established to finance the purchase or leasing of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

These exemptions will not apply:

- If the accounts are transaction accounts through which a legal entity customer can

¹⁵ FinCEN, [FIN-2016-G003](#), *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions*, Question #22, July 19, 2016.

make payments to, or receive payments from, third parties.

- If there is the possibility of a cash refund on the account activity opened to finance the purchase of postage, to finance insurance premiums, or to finance the purchase or leasing of equipment, then beneficial ownership of the legal entity customer must be identified and verified by the bank as required either at the initial remittance, or at the time such refund occurs.

Customer Due Diligence — Overview

Objective. *Assess the bank's compliance with the regulatory requirements for customer due diligence (CDD).*

The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of risk-based CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD is to enable the bank to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious.

Effective CDD policies, procedures, and processes provide the critical framework that enables the bank to comply with regulatory requirements including monitoring for and reporting of suspicious activity. An illustration of this concept is provided in Appendix K (“Customer Risk versus Due Diligence and Suspicious Activity Monitoring”). CDD policies, procedures, and processes are critical to the bank because they can aid in:

- Detecting and reporting unusual or suspicious activity that potentially exposes the bank to financial loss, increased expenses, or other risks.
- Avoiding criminal exposure from persons who use or attempt to use the bank's products and services for illicit purposes.
- Adhering to safe and sound banking practices.

Customer Due Diligence

FinCEN's final rule on CDD became effective July 11, 2016, with a compliance date of May 11, 2018. The rule codifies existing supervisory expectations and practices related to regulatory requirements and therefore, nothing in this final rule is intended to lower, reduce, or limit the due diligence expectations of the federal functional regulators or in any way limit their existing regulatory discretion.¹

In accordance with regulatory requirements, all banks must develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence,² including, but not limited to:

- Obtaining and analyzing sufficient customer information to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information

¹ Department of the Treasury, Financial Crimes Enforcement Network (2016), “Customer Due Diligence Requirements for Financial Institutions,” final rules (RIN 1506-AB25), *Federal Register*, vol. 81 (May 11), p. 29403.

² See 31 CFR 1020.210(b)(5)

regarding the beneficial owner(s) of legal entity customers. Additional guidance can be found in the examination procedures “Beneficial Ownership Requirements for Legal Entity Customers.”

At a minimum, the bank must establish risk-based CDD procedures that:

- Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
- Enable the bank to conduct ongoing monitoring
 - for the purpose of identifying and reporting suspicious transactions and,
 - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.

In addition, the bank’s risk-based CDD policies, procedures, and processes should:

- Be commensurate with the bank’s BSA/AML risk profile, with increased focus on higher risk customers.
- Contain a clear statement of management’s and staff’s responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer’s risk profile, as applicable.
- Provide standards for conducting and documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

Customer Risk Profile

The bank should have an understanding of the money laundering and terrorist financing risks of its customers, referred to in the rule as the customer risk profile.³ This concept is also commonly referred to as the customer risk rating. Any customer account may be used for illicit purposes, including money laundering or terrorist financing. Further, a spectrum of risks may be identifiable even within the same category of customers. The bank’s program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the money laundering and terrorist financing risks of its customers. Improper identification and assessment of a customer’s risk can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened BSA compliance program.

The assessment of customer risk factors is bank-specific, and a conclusion regarding the customer risk profile should be based on a consideration of all pertinent customer information, including ownership information generally. Similar to the bank’s overall risk assessment, there are no required risk profile categories and the number and detail of these categorizations will vary based on the bank’s size and complexity. Any one single indicator is not necessarily determinative of the existence of a lower or higher customer risk.

³ See 31 CFR 1020.210(b)(5)(i)

Examiners should primarily focus on whether the bank has effective processes to develop customer risk profiles as part of the overall CDD program. Examiners may review individual customer risk decisions as a means to test the effectiveness of the process and CDD program. In those instances where the bank has an established and effective customer risk decision-making process, and has followed existing policies, procedures, and processes, the bank should not be criticized for individual customer risk decisions unless it impacts the effectiveness of the overall CDD program, or is accompanied by evidence of bad faith or other aggravating factors.

The bank should gather sufficient information about the customer to form an understanding of the nature and purpose of customer relationships at the time of account opening. This understanding may be based on assessments of individual customers or on categories of customers. An understanding based on “categories of customers” means that for certain lower-risk customers, the bank’s understanding of the nature and purpose of a customer relationship can be developed by inherent or self-evident information such as the type of customer, the type of account opened, or the service or product offered.

The factors the bank should consider when assessing a customer risk profile are substantially similar to the risk categories considered when determining the bank’s overall risk profile. The bank should identify the specific risks of the customer or category of customers, and then conduct an analysis of all pertinent information in order to develop the customer’s risk profile. In determining a customer’s risk profile, the bank should consider risk categories, such as the following, as they relate to the customer relationship:

- Products and Services.
- Customers and Entities.
- Geographic Locations.

As with the risk assessment, the bank may determine that some factors should be weighted more heavily than others. For example, certain products and services used by the customer, the type of customer’s business, or the geographic location where the customer does business, may pose a higher risk of money laundering or terrorist financing. Also, actual or anticipated activity in a customer’s account can be a key factor in determining the customer risk profile. Refer to the further description of identification and analysis of specific risk categories in the “BSA/AML Risk Assessment - Overview” section of the FFIEC BSA/AML Examination Manual.

Customer Information – Risk-Based Procedures

As described above, the bank is required to form an understanding of the nature and purpose of the customer relationship. The bank may demonstrate its understanding of the customer relationship through gathering and analyzing information that substantiates the nature and purpose of the account. Customer information collected under CDD requirements for the purpose of developing a customer risk profile and ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, includes beneficial ownership information for legal entity customers. However, the collection of customer information regarding beneficial ownership is governed by the

requirements specified in the beneficial ownership rule. The beneficial ownership rule requires the bank to collect beneficial ownership information at the 25 percent ownership threshold regardless of the customer's risk profile. In addition, the beneficial ownership rule does not require the bank to collect information regarding ownership or control for certain customers that are exempted or not included in the definition of legal entity customer, such as certain trusts, or certain other legal entity customers.⁴

Other than required beneficial ownership information, the level and type of customer information should be commensurate with the customer's risk profile, therefore the bank should obtain more customer information for those customers that have a higher customer risk profile and may find that less information for customers with a lower customer risk profile is sufficient. Additionally, the type of appropriate customer information will generally vary depending on the customer risk profile and other factors, for example, whether the customer is a legal entity or an individual. For lower risk customers, the bank may have an inherent understanding of the nature and purpose of the customer relationship (*i.e.*, the customer risk profile) based upon information collected at account opening. As a result, the bank may not need to collect any additional customer information for these customers in order to comply with this part of the CDD requirements.

Customer information collected under the CDD rule may be relevant to other regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties. The bank should define in its policies, procedures and processes how customer information will be used to meet other regulatory requirements. For example, the bank is expected to use the customer information and customer risk profile in its suspicious activity monitoring process to understand the types of transactions a particular customer would normally be expected to engage in as a baseline against which suspicious transactions are identified and to satisfy other regulatory requirements.⁵

The bank may choose to implement CDD policies, procedures, and processes on an enterprise-wide basis. To the extent permitted by law, this implementation may include sharing or obtaining customer information across business lines, separate legal entities within an enterprise, and affiliated support units. To encourage cost effectiveness, enhance efficiency, and increase availability of potentially relevant information, the bank may find it useful to cross-check for customer information in data systems maintained within the financial institution for other purposes, such as credit underwriting, marketing, or fraud detection.

Higher Risk Profile Customers

Customers that pose higher money laundering or terrorist financing risks, (*i.e.*, higher risk profile customers), present increased risk exposure to banks. As a result, due diligence policies, procedures, and processes should define both when and what additional customer information will be collected based on the customer risk profile and the specific risks posed. Collecting additional information about customers that pose heightened risk, referred to as enhanced due diligence (EDD), for example, in the private and foreign correspondent banking context, is part

⁴ See 31 CFR 1010.230(e)(2) and 31 CFR 1010.230(h)

⁵ See 31 CFR 1020.210(b)(5)(ii)

of an effective due diligence program. Even within categories of customers with a higher risk profile, there can be a spectrum of risks and the extent to which additional ongoing due diligence measures are necessary may vary on a case-by-case basis. Based on the customer risk profile, the bank may consider obtaining, at account opening (and throughout the relationship), more customer information in order to understand the nature and purpose of the customer relationship, such as:

- Source of funds and wealth.
- Occupation or type of business (of customer or other individuals with ownership or control over the account).
- Financial statements for business customers.
- Location where the business customer is organized and where they maintain their principal place of business.
- Proximity of the customer's residence, place of employment, or place of business to the bank.
- Description of the business customer's primary trade area, whether transactions are expected to be domestic or international, and the expected volumes of such transactions.
- Description of the business operations, such as total sales, the volume of currency transactions, and information about major customers and suppliers.

Performing an appropriate level of ongoing due diligence that is commensurate with the customer's risk profile is especially critical in understanding the customer's transactions in order to assist the bank in determining when transactions are potentially suspicious. This determination is necessary for a suspicious activity monitoring system that helps to mitigate the bank's compliance and money laundering risks.

Consistent with the risk-based approach, the bank should do more in circumstances of heightened risk, as well as to mitigate risks generally. Information provided by higher risk profile customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank. The bank should establish policies and procedures for determining whether and/or when, on the basis of risk, obtaining and reviewing additional customer information, for example through negative media search programs, would be appropriate.

While not inclusive, certain customer types, such as those found in the "Persons and Entities" section of the FFIEC BSA/AML Examination Manual, may pose heightened risk. In addition, existing laws and regulations may impose, and supervisory guidance may explain expectations for, specific customer due diligence and, in some cases, enhanced due diligence requirements for certain accounts or customers, including foreign correspondent accounts,⁶ payable-through

⁶ See 31 CFR 1010.610.

accounts,⁷ private banking accounts,⁸ politically exposed persons,⁹ and money services businesses.¹⁰ The bank's risk-based customer due diligence and enhanced due diligence procedures must ensure compliance with these existing requirements and should meet these supervisory expectations.

Ongoing Monitoring of the Customer Relationship

The requirement for ongoing monitoring of the customer relationship reflects existing practices established to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

Therefore, in addition to policies, procedures, and processes for monitoring to identify and report suspicious transactions, the bank's CDD program must include risk-based procedures for performing ongoing monitoring of the customer relationship, on a risk basis, to maintain and update customer information, including beneficial ownership information of legal entity customers.¹¹ For more information on beneficial ownership of legal entity customers, refer to the "Beneficial Ownership Requirements for Legal Entity Customers" section of the FFIEC BSA/AML Examination Manual.

The requirement to update customer information is event-driven and occurs as a result of normal monitoring.¹² Should the bank become aware as a result of its ongoing monitoring that customer information, including beneficial ownership information, has materially changed, it should update the customer information accordingly. Additionally, if this customer information is material and relevant to assessing the risk of a customer relationship, then the bank should reassess the customer risk profile/rating and follow established bank policies, procedures, and processes for maintaining or changing the customer risk profile/rating. One common indication of a material change in the customer risk profile is transactions or other activity that are inconsistent with the bank's understanding of the nature and purpose of the customer relationship or with the customer risk profile.

The bank's procedures should establish criteria for when and by whom customer relationships will be reviewed, including updating customer information and reassessing the customer's risk profile. The procedures should indicate who in the organization is authorized to change a customer's risk profile. A number of factors may be relevant in determining when it is appropriate to review a customer relationship including, but not limited to:

- Significant and unexplained changes in account activity
- Changes in employment or business operation

⁷ See 31 CFR 1010.610(b)(1)(iii).

⁸ See 31 CFR 1010.620

⁹ Department of State, Department of the Treasury, Federal Reserve, FDIC, OCC, OTS, *Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds of Official Corruption*, January 1, 2001.

¹⁰ FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States*, April 26, 2005.

¹¹ See 31 CFR 1020.210(b)(5)(ii)

¹² Department of the Treasury, Financial Crimes Enforcement Network (2016), "Customer Due Diligence Requirements for Financial Institutions," final rules (RIN 1506-AB25), *Federal Register*, vol. 81 (May 11), p. 29399.

- Changes in ownership of a business entity
- Red flags identified through suspicious activity monitoring
- Receipt of law enforcement inquiries and requests such as criminal subpoenas, National Security Letters (NSL), and section 314(a) requests
- Results of negative media search programs
- Length of time since customer information was gathered and the customer risk profile assessed

The ongoing monitoring element does not impose a categorical requirement that the bank must update customer information on a continuous or periodic basis.¹³ However, the bank may establish policies, procedures, and processes for determining whether and when, on the basis of risk, periodic reviews to update customer information should be conducted to ensure that customer information is current and accurate.

¹³ Ibid.

Examination Procedures

Customer Due Diligence

Objective. *Assess the bank's compliance with the regulatory requirements for customer due diligence (CDD).*

1. Determine whether the bank has developed and implemented appropriate written risk-based procedures for conducting ongoing CDD and that they:
 - Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
 - Enable the bank to conduct ongoing monitoring
 - for the purpose of identifying and reporting suspicious transactions and,
 - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.
 - Enable the bank to use customer information and the customer risk profile to understand the types of transactions a particular customer would be expected to engage in and as a baseline against which suspicious transactions are identified.
2. Determine whether the bank, as part of the overall CDD program, has effective processes to develop customer risk profiles that identify the specific risks of individual customers or categories of customers.
3. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the bank's BSA/AML risk profile with increased focus on higher risk customers.
4. Determine whether policies, procedures, and processes contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable.
5. Determine that the bank has policies, procedures, and processes to identify customers that may pose higher risk for money laundering or terrorist financing that include whether and/or when, on the basis of risk, it is appropriate to obtain and review additional customer information.
6. Determine whether the bank provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.
7. Determine whether the bank has defined in its policies, procedures, and processes how customer information, including beneficial ownership information for legal entity customers, is used to meet other relevant regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties.

Transaction Testing

8. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of customer information. Determine whether the bank collects appropriate information sufficient to understand the nature and purpose of the customer relationship and effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. This sample can be performed when testing the bank's compliance with its policies, procedures, and processes as well as when reviewing transactions or accounts for possible suspicious activity.
9. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with CDD.



FinCEN GUIDANCE

FIN-2020-G002

Issued: August 3, 2020

Subject: Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions.

The Financial Crimes Enforcement Network (FinCEN), in consultation with the federal functional regulators, is issuing responses to three frequently asked questions (FAQs) regarding customer due diligence requirements for covered financial institutions. These FAQs clarify the regulatory requirements related to obtaining customer information, establishing a customer risk profile, and performing ongoing monitoring of the customer relationship in order to assist covered financial institutions with their compliance obligations in these areas. These FAQs are in addition to those that were published on [July 19, 2016](#) and [April 3, 2018](#). For further information regarding customer due diligence requirements, including the Customer Due Diligence Requirements for Financial Institutions¹ (the “CDD Rule”), please see FinCEN’s [CDD webpage](#).

I. Customer Information – Risk-Based Procedures

Q1: Is it a requirement under the CDD Rule that covered financial institutions:

- collect information about expected activity on all customers at account opening, or on an ongoing or periodic basis;
- conduct media searches or screening for news articles on all customers or other related parties, such as beneficial owners, either at account opening, or on an ongoing or periodic basis; or
- collect information that identifies underlying transacting parties when a financial institution offers correspondent banking or omnibus accounts to other financial institutions (i.e., a customer’s customer)?

1. See 31 U.S.C § 5318(h) and 31 CFR § 1010.210 for anti-money laundering program requirements, and, as applied to specific financial institutions, in 31 CFR §§ 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, and 1030.210.

- A. The CDD Rule does not categorically require (1) the collection of any particular customer due diligence information (other than that required to develop a customer risk profile, conduct monitoring, and collect beneficial ownership information); (2) the performance of media searches or particular screenings; or (3) the collection of customer information from a financial institution's clients when the financial institution is a customer of a covered financial institution.

A covered financial institution may assess, on the basis of risk, that a customer's risk profile is low, and that, accordingly, additional information is not necessary for the covered financial institution to develop its understanding of the nature and purpose of the customer relationship. In other circumstances, the covered financial institution might assess, on the basis of risk, that a customer presents a higher risk profile and, accordingly, collect more information to better understand the customer relationship.

Covered financial institutions must establish policies, procedures, and processes for determining whether and when, on the basis of risk, to update customer information to ensure that customer information is current and accurate. Information collected throughout the relationship is critical in understanding the customer's transactions in order to assist the financial institution in determining when transactions are potentially suspicious.

II. Customer Risk Profile

Q2: Is it a requirement under the CDD Rule that covered financial institutions:

- use a specific method or categorization to risk rate customers; or
 - automatically categorize as "high risk" products and customer types that are identified in government publications as having characteristics that could potentially expose the institution to risks?
- A. It is not a requirement that covered financial institutions use a specific method or categorization to establish a customer risk profile. Further, covered financial institutions are not required or expected to automatically categorize as "high risk" products or customer types listed in government publications.

Various government publications provide information and discussions on certain products, services, customers, and geographic locations that present unique challenges and exposures regarding illicit financial activity risks. However, even within the same risk category, a spectrum of risks may be identifiable and due diligence measures may vary on a case-by-case basis.

A covered financial institution should have an understanding of the money laundering, terrorist financing, and other financial crime risks of its customers to develop the customer risk profile. Furthermore, the financial institution's program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the risks of its customers. There are no prescribed risk profile categories, and the number and detail of these categories can vary.

III. Ongoing Monitoring of the Customer Relationship

Q3: *Is it a requirement under the CDD Rule that financial institutions update customer information on a specific schedule?*

- A. There is no categorical requirement that financial institutions update customer information on a continuous or periodic schedule. The requirement to update customer information is risk based and occurs as a result of normal monitoring. Should the financial institution become aware as a result of its ongoing monitoring of a change in customer information (including beneficial ownership information) that is relevant to assessing the risk posed by the customer, the financial institution must update the customer information accordingly. Additionally, if this customer information is relevant to assessing the risk of a customer relationship, then the financial institution should reassess the customer risk profile/rating and follow established financial institutions policies, procedures, and processes for maintaining or changing the customer risk profile/rating. However, financial institutions, on the basis of risk, may choose to review customer information on a regular or periodic basis.

For Further Information

Questions or comments regarding the contents of this guidance should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons

August 21, 2020

Introduction

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the Financial Crimes Enforcement Network (FinCEN), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) (collectively, the Agencies) are issuing this joint statement to address due diligence questions raised by banks¹ related to Bank Secrecy Act/Anti-Money Laundering (BSA/AML) regulatory requirements for customers whom banks may consider to be politically exposed persons (PEPs).² Banks have requested clarification on how to apply a risk-based approach to PEPs consistent with the customer due diligence (CDD) requirements contained in FinCEN's 2016 CDD Final Rule.³

The Agencies do not interpret the term "politically exposed persons" to include U.S. public officials. BSA/AML regulations do not define PEPs, but the term is commonly used in the financial industry to refer to foreign individuals who are or have been entrusted with a prominent public function, as well as their immediate family members and close associates. By virtue of this public position or relationship, these individuals may present a higher risk that their funds may be the proceeds of corruption or other illicit activity. The level of risk associated with PEPs, however, varies and not all PEPs are automatically higher risk. PEPs should not be confused with the term "senior foreign political figure" (SFPF) as defined under the BSA private banking regulation, a subset of PEPs.⁴

-
- 1 Under the Bank Secrecy Act, the term "bank" is defined in 31 CFR 1010.100(d) and includes each agent, agency, branch, or office within the United States of banks, savings associations, credit unions, and foreign banks.
 - 2 The Agencies that issued the *Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Corruption* (January 2001) are contemporaneously rescinding it.
 - 3 *Customer Due Diligence Requirements for Financial Institutions*, 81 FR 29398 (May 2016); see also 31 CFR Parts 1010, 1020, 1023, 1024, and 1026.
 - 4 31 CFR 1010.605(p) and 31 CFR 1010.620; see also "[FinCEN Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators](#)" (June 2018).

The Agencies recognize that, consistent with a risk-based approach, the level and type of CDD should be commensurate with the risks presented by the PEP relationship. The CDD rule does not create a regulatory requirement, and there is no supervisory expectation, for banks to have unique, additional due diligence steps for customers who are considered PEPs.⁵ Instead, the level and type of CDD should be appropriate for the customer risk.

This joint statement does not alter existing BSA/AML legal or regulatory requirements, nor does it establish new supervisory expectations. In addition, it does not require banks to cease existing risk management practices if the bank considers them necessary to effectively manage risk. Further, this statement does not, and should not be construed in any way to, diminish the serious national security or criminal threats posed by PEPs, including SFPFs, who engage in illicit acts and crimes, including terrorism, human rights abuses, extortion, corruption, human trafficking, narcotics trafficking, bribery, money laundering, and related crimes.

Customer Due Diligence Requirements and Considerations⁶

Like all bank accounts, those held by PEPs are subject to BSA/AML regulatory requirements. These include requirements related to suspicious activity reporting,⁷ customer identification,⁸ CDD, and beneficial ownership,⁹ as applicable.

Banks must apply a risk-based approach to CDD in developing the risk profiles of their customers, including PEPs, and are required to establish and maintain written procedures reasonably designed to identify and verify beneficial owners of legal entity customers. More specifically, banks must adopt appropriate risk-based procedures for conducting CDD that, among other things, enable banks to: (i) understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (ii) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

There is no regulatory requirement in the CDD rule, nor is there a supervisory expectation, for banks to have unique, additional due diligence steps for PEPs. The CDD rule also does not require a bank to screen for or otherwise determine whether a customer or beneficial owner of a legal entity customer may be considered a PEP. A bank may choose to determine whether a customer is a PEP at account opening, if the bank determines the information is necessary for

5 Likewise, the CDD rule does not create such a regulatory requirement or supervisory expectation for U.S. federal, state, or local public officials.

6 The requirements described in this section are limited to those of the Customer Due Diligence rule, which are found at 31 CFR 1010.210, 1020.210(b)(5) (CDD), and 1010.230 (beneficial ownership of legal entity customers). This section does not address the requirements of Section 312 of the USA PATRIOT Act, codified at 31 CFR 1010.600-630.

7 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).

8 12 CFR 208.63(b)(2), 211.5(m)(2), and 211.24(j)(2) (Federal Reserve); 12 CFR 326.8(b)(2) (FDIC); 12 CFR 748.2(b)(2) (NCUA); 12 CFR 21.21(c)(2) (OCC); and 31 CFR 1020.220 (FinCEN).

9 31 CFR 1010.210 and 1020.210(b)(5) (CDD), and 1010.230 (beneficial ownership of legal entity customers).

the development of a customer risk profile. Further, the bank may conduct periodic reviews with respect to PEPs, as part of or in addition to the required ongoing risk-based monitoring to maintain and update customer information.¹⁰

Not all PEPs are high risk solely by virtue of their status. Rather, the risk depends on facts and circumstances specific to the customer relationship. For example, PEPs with a limited transaction volume, a low-dollar deposit account with the bank, known legitimate source(s) of funds, or access only to products or services that are subject to specific terms and payment schedules could reasonably be characterized as having lower customer risk profiles.

Banks may leverage existing processes for assessing geographic-specific money laundering, corruption, and terrorist financing risks when developing the customer risk profile, which may also take into account the jurisdiction's legal and enforcement frameworks, including ethics reporting and oversight requirements. For a PEP who is no longer in active government service, banks may also consider the time that the customer has been out of office, and the level of influence he or she may still hold.

When developing the customer risk profile, and determining when and what additional customer information to collect, banks may take into account such factors as a customer's public office or position of public trust (or that of the customer's family member or close associate), as well as any indication that the PEP may misuse his or her authority or influence for personal gain. A bank may also consider other factors in assessing the risk of these customer relationships, including the type of products and services used,¹¹ the volume and nature of transactions, geographies associated with the customer's activity and domicile, the customer's official government responsibilities, the level and nature of the customer's authority or influence over government activities or officials, the customer's access to significant government assets or funds, and the overall nature of the customer relationship.¹² The customer information and customer risk profile may impact how the bank complies with other regulatory requirements, such as suspicious activity monitoring, since the bank structures its BSA/AML compliance program to address its risk profile, based on the bank's assessment of risks.

¹⁰ 31 CFR 1020.210(b)(5).

¹¹ For example, some banks have wealth management accounts that fall outside of the definition of "private banking account" but may still pose a higher risk of illicit financial activity. These accounts are often held by individuals with a high net worth and may also include high dollar accounts or large transactions. As with all customers, banks are required to apply BSA/AML regulatory requirements including, but not limited to, CDD and suspicious activity monitoring and reporting. Adherence to the existing BSA/AML framework will assist banks in identifying and managing the potentially higher risks associated with these customers and accounts.

¹² Available resources for use in assessing risks of PEPs include: [Guidance on Politically Exposed Persons](#) (2013); [Concealment of Beneficial Ownership](#) (2018); [Wolfsberg Guidance on Politically Exposed Persons \(PEPs\)](#) (2017); [International Narcotics Control Strategy Report](#) (2020); and [National Drug Control Strategy](#) (2020).

Conclusion

Addressing the money laundering threat posed by public corruption of foreign officials continues to be a national security priority for the United States. In high-profile cases over the years, foreign individuals who may be considered PEPs have used banks as conduits for their illegal activities, including corruption, bribery, money laundering, and related crimes. Banks are reminded of their obligation to identify and report suspicious activity, including transactions that may involve the proceeds of corruption. The Agencies recognize that PEP relationships present varying levels of money laundering risk, and those risks depend on the presence or absence of numerous factors. As described above, banks must adopt appropriate risk-based procedures for conducting CDD; however, under the CDD rule, there is no regulatory requirement or supervisory expectation for banks to have unique, additional due diligence steps for customers whom the banks consider to be PEPs.

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Financial Crimes Enforcement Network
National Credit Union Administration
Office of the Comptroller of the Currency**

**Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for
Charities and Non-Profit Organizations**

November 19, 2020

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the Financial Crimes Enforcement Network (FinCEN), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) (collectively, the Agencies) are issuing this joint fact sheet to provide clarity to banks¹ on how to apply a risk-based approach to charities and other non-profit organizations (NPOs), consistent with the customer due diligence (CDD) requirements contained in FinCEN's 2016 CDD Final Rule.² Some charities have reported difficulty in obtaining and maintaining access to financial services, jeopardizing the important contributions charities make to the most vulnerable. The Agencies remind banks that the U.S. government does not view the charitable sector as a whole as presenting a uniform or unacceptably high risk of being used or exploited for money laundering, terrorist financing (ML/TF), or sanctions violations.³ The Agencies remind banks that charities vary in their risk profiles and should be treated according to such profiles. Banks should apply the risk-based approach and evaluate charities according to their particular characteristics to determine whether they can effectively mitigate the potential risk some charities may pose. This approach helps to minimize illicit finance risks. This joint fact sheet does not alter existing Bank Secrecy Act/Anti-Money Laundering (BSA/AML) legal or regulatory requirements, nor does it establish new supervisory expectations.

Helping those in need is a core American value, particularly in the difficult conditions caused by the COVID-19 pandemic. The United States is committed to ensuring that humanitarian assistance continues to reach at-risk populations through legitimate and transparent channels, including during the COVID-19 pandemic.⁴ The Agencies recognize that it is vital for legitimate charities and other

1. Under the Bank Secrecy Act, the term "bank" is defined in 31 CFR 1010.100(d) and includes each agent, agency, branch, or office within the United States of banks, savings associations, credit unions, and foreign banks.
2. *Customer Due Diligence Requirements for Financial Institutions*, 81 FR 29398 (May 2016); see also 31 CFR Parts 1010, 1020, 1023, 1024, and 1026.
3. [National Terrorist Financing Risk Assessment](#) (2018), p. 23.
4. See U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) [Fact Sheet: Provision of Humanitarian Assistance and Trade to Combat COVID-19](#) (April 16, 2020). See also [OFAC Encourages Persons to Communicate OFAC Compliance Concerns Related to the Coronavirus Disease 2019 \(COVID-19\)](#) (April 20, 2020) and U.S. Department of the Treasury's [Press Release: Treasury Underscores Commitment to Global Flow of Humanitarian Aid in Face of Covid-19 Pandemic](#) (April 9, 2020).

NPOs to have access to financial services, including the ability to transmit funds. Charities and other NPOs rely on banks to facilitate the flow of funds transfers in a timely fashion. Although some charities and other NPOs have been misused to facilitate ML/TF⁵ or evade sanctions, the Agencies recognize that the vast majority of charities and other NPOs comply with the law and properly support charitable and humanitarian causes.

CDD Requirements

Like all bank accounts, those held by charity and NPO customers are subject to BSA/AML regulatory requirements. These include requirements related to suspicious activity reporting,⁶ customer identification,⁷ CDD, and beneficial ownership,⁸ as applicable.

Banks must apply a risk-based approach to CDD in developing the risk profiles of their customers, including charities and NPOs, and are required to establish and maintain written procedures reasonably designed to identify and verify beneficial owners of legal entity customers, as applicable.⁹ More specifically, banks must adopt appropriate risk-based procedures for conducting CDD that, among other things, enable banks to: (i) understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (ii) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.¹⁰ Consistent with a risk-based approach, the level and type of CDD should be appropriate for the risks presented by each customer. There is no regulatory requirement in the CDD rule, nor is there a supervisory expectation, for banks to have unique, additional due diligence steps for charities or other NPO customers.

Considerations for a Risk-Based Approach

As previously stated, charities and other NPOs do not present a uniform or unacceptably high ML/TF risk; rather, the risk to banks depends on facts and circumstances specific to the customer relationship. The ML/TF risk for charitable organizations can vary dramatically depending on the operations, activities, leadership, and affiliations of the organization. U.S. charities that operate and provide funds solely to domestic recipients generally present low TF risk. However, U.S. charities that operate abroad, provide funding to, or have affiliated organizations in conflict regions, can present potentially higher TF risks.¹¹

5. See FinCEN [Advisory to Financial Institutions Regarding Disaster-Related Fraud](#) (October 31, 2017).
6. 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).
7. 12 CFR 208.63(b)(2), 211.5(m)(2), and 211.24(j)(2) (Federal Reserve); 12 CFR 326.8(b)(2) (FDIC); 12 CFR 748.2(b)(2) (NCUA); 12 CFR 21.21(c)(2) (OCC); and 31 CFR 1020.220 (FinCEN).
8. 31 CFR 1010.230.
9. See 31 CFR 1010.230(e)(3)(ii) (requiring that nonprofit entities only identify a single individual with significant responsibility to control, manage, or direct the entity).
10. 31 CFR 1020.210(b)(5).
11. [National Terrorist Financing Risk Assessment](#) (2018), p. 23.

Charities and other NPOs are subject to federal and state reporting requirements and regulatory oversight. For example, charities report specific information annually on IRS Form 990 regarding their stated mission, programs, finances (including non-cash contributions), donors, activities, and funds sent and used abroad.¹² Many NPOs also adhere to voluntary self-regulatory standards¹³ and controls to improve individual governance, management, and operational practice, in addition to internal controls required by donors and others. Although the CDD rule does not require the collection of this specific information, the following customer information may be useful for banks in determining the ML/TF risk profile of charities and other NPO customers:

- Purpose and nature of the NPO, including mission(s), stated objectives, programs, activities, and services.
- Geographic locations served, including headquarters and operational areas, particularly in higher-risk areas where terrorist groups are most active.
- Organizational structure, including key principals, management, and internal controls of the NPO.
- State incorporation, registration, and tax-exempt status by the IRS and required reports with regulatory authorities.
- Voluntary participation in self-regulatory programs to enhance governance, management, and operational practice.
- Financial statements, audits, and any self-assessment evaluations.
- General information about the donor base, funding sources, and fundraising methods, and for public charities, level of support from the general public.
- General information about beneficiaries and criteria for disbursement of funds, including guidelines/standards for qualifying beneficiaries and any intermediaries that may be involved.
- Affiliation with other NPOs, governments, or groups.

Additional information that may be useful to banks in determining the customer risk profile of a charity or other NPO is available at the U.S. Department of the Treasury's Resource Center, *Protecting Charitable Organizations*.¹⁴

Conclusion

Charitable organizations and other NPOs build communities, relieve suffering, provide life-saving assistance, and help developing nations. During this COVID-19 pandemic, charities and other NPOs are on the front lines, both

12. The extensive Schedule F of Form 990 includes many categories of reporting requirements for charities with overseas activities.

13. [National Terrorist Financing Risk Assessment](#) (2018), p. 24.

14. <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/protecting-index.aspx>.

domestically and internationally, delivering medical supplies and vital assistance to areas most impacted by COVID-19. Banks that operate in compliance with applicable laws, properly manage customer relationships, and effectively mitigate risks by implementing controls commensurate with those risks are neither prohibited nor discouraged from providing banking services to charities and other NPOs. The Agencies are issuing this joint fact sheet to reaffirm that the level of ML/TF risk associated with charities and other NPOs varies; these bank customers do not present a uniform or unacceptably high ML/TF risk. The application of a risk-based approach for charities and other NPOs is consistent with existing CDD and other BSA/AML requirements.

Appendix F: Money Laundering and Terrorist Financing “Red Flags”

The following are examples of potentially suspicious activities, or “red flags” for both money laundering and terrorist financing. Although these lists are not all-inclusive, they may help banks and examiners recognize possible money laundering and terrorist financing schemes. FinCEN issues advisories containing examples of “red flags” to inform and assist banks in reporting instances of suspected money laundering, terrorist financing, and fraud. In order to assist law enforcement in its efforts to target these activities, FinCEN requests that banks check the appropriate box(es) in the Suspicious Activity Information section and include certain key terms in the narrative section of the SAR. The advisories and guidance can be found on FinCEN Web site.³⁰² Management’s primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime.

The following examples are red flags that, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Potentially Suspicious Activity That May Indicate Money Laundering

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual or suspicious identification documents that cannot be readily verified.
- A customer provides an individual taxpayer identification number after having previously used a Social Security number.
- A customer uses different taxpayer identification numbers with variations of his or her name.
- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- A customer’s home or business telephone is disconnected.
- The customer’s background differs from that which would be expected on the basis of his or her business activities.
- A customer makes frequent or large transactions and has no record of past or present employment experience.
- A customer is a trust, shell company, or Private Investment Company that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial

³⁰² Refer to [SAR Advisory Key Terms](#).

owners may hire nominee incorporation services to establish shell companies and open bank accounts for those shell companies while shielding the owner’s identity.

Efforts to Avoid Reporting or Recordkeeping Requirement

- A customer or group tries to persuade a bank employee not to file required reports or maintain required records.
- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.
- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.
- A customer deposits funds into several accounts, usually in amounts of less than \$3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as noncooperative countries and territories).
- A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits structured at or just under \$10,000, to evade CTR filing requirements.

Funds Transfers

- Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer’s business or history.
- Funds transfer activity occurs to or from a financial institution located in a higher risk jurisdiction distant from the customer’s operations.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer’s business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds transfer activity is unexplained, repetitive, or shows unusual patterns.

- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- Funds transfers are sent or received from the same person to or from different accounts.
- Funds transfers contain limited content and lack related party information.

Automated Clearing House Transactions

- Large-value, automated clearing house (ACH) transactions are frequently initiated through third-party service providers (TPSP) by originators that are not bank customers and for which the bank has no or insufficient due diligence.
- TPSPs have a history of violating ACH network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.
- Multiple layers of TPSPs that appear to be unnecessarily involved in transactions.
- Unusually high level of transactions initiated over the Internet or by telephone.
- NACHA — The Electronic Payments Association (NACHA) information requests indicate potential concerns with the bank’s usage of the ACH system.

Activity Inconsistent with the Customer’s Business

- The currency transaction patterns of a business show a sudden change inconsistent with normal activities.
- A large volume of cashier’s checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder’s business would not appear to justify such activity.
- A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.
- Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
- The owner of both a retail business and a check-cashing service does not ask for currency when depositing checks, possibly indicating the availability of another source of currency.
- Goods or services purchased by the business do not match the customer’s stated line of business.
- Payments for goods or services are made by checks, money orders, or bank drafts not drawn from the account of the entity that made the purchase.

Lending Activity

- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.

- Borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.
- Loans that lack a legitimate business purpose, provide the bank with significant fees for assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower).

Changes in Bank-to-Bank Transactions

- The size and frequency of currency deposits increases rapidly with no corresponding increase in noncurrency deposits.
- A bank is unable to track the true accountholder of correspondent or concentration account transactions.
- The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank’s location.
- Changes in currency-shipment patterns between correspondent banks are significant.

Cross-Border Financial Institution Transactions

- U.S. bank increases sales or exchanges of large denomination U.S. bank notes to Mexican financial institution(s).
- Large volumes of small denomination U.S. banknotes being sent from Mexican casas de cambio to their U.S. accounts via armored transport or sold directly to U.S. banks. These sales or exchanges may involve jurisdictions outside of Mexico.
- Casas de cambio direct the remittance of funds via multiple funds transfers to jurisdictions outside of Mexico that bear no apparent business relationship with the casas de cambio. Funds transfer recipients may include individuals, businesses, and other entities in free trade zones.
- Casas de cambio deposit numerous third-party items, including sequentially numbered monetary instruments, to their accounts at U.S. banks.
- Casas de cambio direct the remittance of funds transfers from their accounts at Mexican financial institutions to accounts at U.S. banks. These funds transfers follow the deposit of currency and third-party items by the casas de cambio into their Mexican financial institution.

Bulk Currency Shipments

- An increase in the sale of large denomination U.S. bank notes to foreign financial institutions by U.S. banks.

- Large volumes of small denomination U.S. bank notes being sent from foreign nonbank financial institutions to their accounts in the United States via armored transport, or sold directly to U.S. banks.
- Multiple wire transfers initiated by foreign nonbank financial institutions that direct U.S. banks to remit funds to other jurisdictions that bear no apparent business relationship with that foreign nonbank financial institution. Recipients may include individuals, businesses, and other entities in free trade zones and other locations.
- The exchange of small denomination U.S. bank notes for large denomination U.S. bank notes that may be sent to foreign countries.
- Deposits by foreign nonbank financial institutions to their accounts at U.S. banks that include third-party items, including sequentially numbered monetary instruments.
- Deposits of currency and third-party items by foreign nonbank financial institutions to their accounts at foreign financial institutions and thereafter direct wire transfers to the foreign nonbank financial institution’s accounts at U.S. banks.

Trade Finance

- Items shipped that are inconsistent with the nature of the customer’s business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).
- Customers conducting business in higher-risk jurisdictions.
- Customers shipping items through higher-risk jurisdictions, including transit through noncooperative countries.
- Customers involved in potentially higher-risk activities, including activities that may be subject to export/import restrictions (e.g., equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore, and crude oil).
- Obvious over- or under-pricing of goods and services.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties should prompt additional OFAC review.

Privately Owned Automated Teller Machines

- Automated teller machine (ATM) activity levels are high in comparison with other privately owned or bank-owned ATMs in comparable geographic and demographic locations.
- Sources of currency for the ATM cannot be identified or confirmed through withdrawals from account, armored car contracts, lending arrangements, or other appropriate documentation.

Insurance

- A customer purchases products with termination features without concern for the product’s investment performance.
- A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.
- A customer purchases a product that appears outside the customer’s normal range of financial wealth or estate planning needs.
- A customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.
- Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include secondhand endowment and bearer insurance policies.
- A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.
- A customer uses multiple currency equivalents (e.g., cashier’s checks and money orders) from different banks and money services businesses to make insurance policy or annuity payments.

Shell Company Activity

- A bank is unable to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of accounts or other banking activity (using Internet, commercial database searches, or direct inquiries to a respondent bank).
- Payments to or from the company have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
- Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
- Transacting businesses share the same address, provide only a registered agent’s address, or have other address inconsistencies.

- Unusually large number and variety of beneficiaries are receiving funds transfers from one company.
- Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk offshore financial centers.
- A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern of funds transfers that is inconsistent with its normal business activity.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- Purpose of the shell company is unknown or unclear.

Embassy and Foreign Consulate Accounts

- Official embassy business is conducted through personal accounts.
- Account activity is not consistent with the purpose of the account, such as pouch activity or payable upon proper identification transactions.
- Accounts are funded through substantial currency transactions.
- Accounts directly fund personal expenses of foreign nationals without appropriate controls, including, but not limited to, expenses for college students.

Employees

- Employee exhibits a lavish lifestyle that cannot be supported by his or her salary.
- Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
- Employee is reluctant to take a vacation
- Employee overrides a hold placed on an account identified as suspicious so that transactions can occur in the account.

Other Unusual or Suspicious Customer Activity

- Customer frequently exchanges small-dollar denominations for large-dollar denominations.
- Customer frequently deposits currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- Customer purchases a number of cashier’s checks, money orders, or traveler’s checks for large amounts under a specified threshold.
- Customer purchases a number of open-end prepaid cards for large amounts. Purchases of prepaid cards are not commensurate with normal business activities.
- Customer receives large and frequent deposits from online payments systems yet has no apparent online or auction business.

- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.
- Suspicious movements of funds occur from one bank to another, and then funds are moved back to the first bank.
- Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.
- Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.
- Customer visits a safe deposit box or uses a safe custody account on an unusually frequent basis.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution’s service area, despite the availability of such services at an institution closer to them.
- Customer repeatedly uses a bank or branch location that is geographically distant from the customer’s home or office without sufficient business purpose.
- Customer exhibits unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, several individuals arrive together, enter frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.
- Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system. Similarly, a customer establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system.
- Unusual use of trust funds in business transactions or other financial activity.
- Customer uses a personal account for business purposes.
- Customer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities or appear to be an effort to hide the beneficial ownership from the bank.
- Customer makes multiple and frequent currency deposits to various accounts that are purportedly unrelated.
- Customer conducts large deposits and withdrawals during a short time period after opening and then subsequently closes the account or the account becomes dormant. Conversely, an account with little activity may suddenly experience large deposit and withdrawal activity.
- Customer makes high-value transactions not commensurate with the customer’s known incomes.

Potentially Suspicious Activity That May Indicate Terrorist Financing

The following examples of potentially suspicious activity that may indicate terrorist financing are primarily based on guidance “Guidance for Financial Institutions in Detecting Terrorist Financing” provided by the FATF.³⁰³ FATF is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

Activity Inconsistent With the Customer’s Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as noncooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

³⁰³ Refer to [Guidance for Financial Institutions in Detecting Terrorist Financing](#), April 24, 2002.

Other Transactions That Appear Unusual or Suspicious

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from higher-risk locations open accounts.
- Funds are sent or received via international transfers from or to higher-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

SUSPICIOUS ACTIVITY REPORTING

I. INTRODUCTION

A. Overview – Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States’ ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Financial institutions should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system. While the federal examiners recognize that for a practical matter, it is not possible for a financial institution to detect and report all potentially illicit transactions that flow through the institution, the examiners will focus on evaluating the institution’s policies, procedures, and processes to identify, evaluate, and report suspicious activity. The sophistication of the monitoring systems utilized should be dictated by the institution’s risk-profile, with particular emphasis on the composition of higher-risk products, services, clients, entities, and geographic markets. The institution should ensure that adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking into account the institution’s overall risk profile and the volume of transactions processed.

B. Key Suspicious Activity Monitoring Components – Effective suspicious activity monitoring and reporting systems include five interdependent components including:

1. Identification or “Alert” of unusual activity – includes employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output;
2. Managing the “Alerts” – the processes used to investigate and evaluate identified unusual activity. Institutions should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.
3. SAR Decision Making – File, or Not File? – After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker, be it individual or committee, with that person or group having the authority to make the final SAR filing decision. (When an institution uses a committee, there should be a clearly defined process to resolve differences of opinion on filing decisions.) Institutions should document ALL SAR decisions, including the specific reasons for either “filing” or “not filing”. “The decision to file a SAR is an inherently subjective judgment and the examiners should focus on whether the institution has an effective SAR decisions-making process, not individual SAR decisions”
4. SAR Completion and Filing – filed SARs must be complete, thorough, and timely. SAR narratives are subjective, and should thoroughly describe the extent and nature of the suspicious activity.
5. Monitoring and SAR Filing on Continuing Activity – If the suspicious activity continues, a “Continuing SAR” is filed after each 90-Day review. This practice notifies law enforcement of the continuing nature of the

activity in aggregate. In addition, this ongoing filing reminds the institution that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as management making the determination to terminate the relationship. Institutions should develop policies, procedures, and processes indicating when to escalate issues or problems identified as a result of repeated SAR filings including:

- Review by senior management and legal staff (e.g. BSA Officer or SAR committee);
- Criteria for when analysis of the overall customer relationship is necessary;
- Criteria for whether and, if so, when to close the account;
- Criteria for when to notify law enforcement, if appropriate.

C. SAR Activity Review – The *SAR Activity Review* is an online publication available at FinCEN’s web site: www.fincen.gov, under the “News Room”, then “Reports & Publications” link. The *SAR Activity Review* is a product of continuing dialogue and close collaboration among the nation’s financial institutions, law enforcement officials, and regulatory agencies to provide meaningful information about the preparation, use, and value of SARs filed by financial institutions.

D. SAR STATS – Annually, FinCEN provides Data and Technical updates to institutions regarding SAR filings through the publication of the report titled “SAR STATS”, the successor publication to the previous *SAR Activity Review: By the Numbers*. The inaugural publication was July 2014. Newly added features to the statistical recap include: Enhanced Data; Trending “Now” in “Other” Sections; SAR Narrative Spotlight – perceived key emerging trends; Sector Highlights; and Data Insider, which discusses the structure, framework, and methodology behind the data.

II. REPORTABLE TRANSACTIONS – Numerous activities and transactions may be suspicious; however, not all are of interest to law enforcement, and therefore not all suspicious transactions are reportable.

A. Definitions – Treasury regulation 31 CFR 1020.320 defines reportable suspicious transactions. When a bank knows, or should have known, that a reportable suspicious transaction has taken place, the obligation to file a SAR is created.

1. A suspiciously reportable transaction is:

- a. Any transaction that involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (i.e., money laundering); or
- b. Any transaction designed to evade any regulations promulgated under the Bank Secrecy Act (this includes structuring as well as other attempts to avoid required reporting or recordkeeping); or

NOTE: Structuring is the breaking down of currency transactions into amounts under \$10,000 for the purpose of evading currency transaction reporting requirements. Failing to observe the

reporting requirements, or intentionally splitting a transaction into parts in order to fall below reporting thresholds can be a crime and can result in civil enforcement actions, including fines. These consequences can apply even when the funds involved were derived from legitimate, not criminal, activity.

- c. Any transaction having no business or apparent lawful purpose, or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.
- 2. For BSA purposes, “transaction” means any deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock/bond/certificate of deposit/other monetary instrument/investment security, or any other payment, transfer, or delivery by, through, or to a bank.

B. Reporting Thresholds – Since law enforcement cannot pursue all suspicious activity, suspicious are required to be reported only when the amount involved meets certain thresholds. Banks are required to file SARs at these dollar levels; however, they may file SARs on transactions involving lesser amounts.

- 1. If a bank insider is involved, there is zero tolerance, and any suspicious transaction is reportable. An insider is generally a director, officer, employee, or controlling stockholder, and can also include a shareholder, joint venture partner, accountant, appraiser, attorney or other agent or independent contractor of the bank.
- 2. If a potential suspect has been identified, transactions involving \$5,000 or more are reportable.
- 3. If no potential suspect has been identified, transactions involving \$25,000 or more are reportable.
- 4. If BSA violations, e.g., money laundering or structuring, are involved, transactions involving \$5,000 or more are reportable.

C. Relationship to Currency Transaction Report – BSA mandates that the bank file a CTR whenever a single transaction or series of transactions in currency exceeds \$10,000 on any one business day. If a transaction exceeds \$10,000 in currency and is suspicious, both a SAR and a CTR must be filed. If a currency transaction involves \$10,000 or less and is suspicious, the bank should only file a SAR.

D. Exceptions

- 1. A SAR is not required to be filed for those robberies and burglaries that are reported to local authorities.

III. THE SUSPICIOUS ACTIVITY REPORT (SAR) – Reportable suspicious activities are reported by banks on the FinCEN SAR, Form 111.

A. Time Frames

1. A SAR must be filed no later than 30 calendar days after the date of initial “detection” of facts that may constitute a basis for filing a SAR.
2. If no suspect was identified on the date of “detection” of the incident requiring the filing, the filing of the SAR may be delayed for an additional 30 calendar days to identify a suspect.
 - a. Unlike the CTR, the SAR addresses overall suspicious activity, not just transactions occurring on a single business day. A pattern of suspicious activity based on a group or series of transactions on different days may create the obligation to file a SAR.
3. If, after an initial SAR has been filed, related activity continues to occur, the institution should report the continuing suspicious activity on a “continuing” SAR. Continuing SAR reports should be filed at least every 90 days until the suspicious activity ceases. Continuing SARs must be completed in their entirety, including the information about all the subjects involved in the suspicious activity and all financial institutions where the activity occurred. The continuing report Part V narrative should include all details of the suspicious activity for the 90-day period encompassed by the report, and only such data from prior reports as necessary to understand the activity. Do not reproduce the narratives from prior reports in the continuing report. (Provide the dollar amount of the current 90-day period in Item 26, and the cumulative dollar amount for the current and all prior reports in Item 28. If continuing losses are involved, record the 90-day loss in Item 63, and the cumulative loss in Part V).
4. In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the financial institution shall immediately notify by telephone an appropriate law enforcement authority in addition to filing a timely SAR. Financial institution wishing to voluntarily report suspicious transactions that may relate to terrorist activity may call FinCEN’s “Hotline” at 866-556-3974 in addition to filing a timely SAR.
5. First stated in *SAR Activity Review # 10* (May 2006) and further clarified in *SAR Activity Review # 14* (October 2008), the phrase “initial detection” should not be interpreted as meaning the moment a transaction is highlighted for review. The institution’s automated account monitoring system or initial discovery of potentially suspicious information such as system-generated reports, may flag a transaction, however, that should not be considered initial detection of suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a “determination” is made that the transaction under review is “suspicious” with the meaning of the SAR regulations. A review must be initiated promptly upon identification of unusual activity that warrants investigation, and the timeframe required for completing the review of the identified activity may vary given the situation. In any event, the review

should be completed “in a reasonable period of time”. (“Date of Determination” should be explicitly stated in the narrative).

6. In *SAR Activity Review # 21* (May 2012), FinCEN’s original intent regarding the timing of the filing of the 90 day update was clarified and now states “Financial institutions with SAR requirements may file SARs for continuing activity after a 90 day review, with the filing deadline being 120 days after the date of the previously related SAR filing. Financial institutions may also file SARs on continuing activity earlier than the 120 day deadline if the institution believes the activity warrants earlier review by law enforcement”. (Variations in the wording on this topic in *SAR Activity Reviews # 1* and *# 8* had created some uncertainty as to when the 90-day update had to be submitted).

B. Completing the SAR

1. FinCEN continues to reiterate that institutions are not responsible for investigating the underlying suspected (or alleged) crime; investigations remain the responsibility of law enforcement. Institutions are responsible for reporting the information they know at the time they conclude that suspicious activity is present.
2. When evaluating suspicious activity and completing a SAR, institutions should report the characteristics of the suspicious activity and types of financial services that best apply, based on information that readily comes available during the course of their case reviews. The new SAR (Form 111) does contain additional and more specific data elements as a more efficient way to bring information about suspicious activity to FinCEN’s and law enforcement’s attention, but as before, financial institutions should report the information that they know, or that otherwise arises as part of their case reviews.
3. The SAR contains both “Critical Fields” (*) and fields not marked as critical. For “Critical Fields”, the filing institution must either provide the requested information or affirmatively check the “unknown” box that is provided with each “Critical Field”, or the BSA E-Filing System will NOT accept the filing of the report. For the fields not marked as critical, the BSA E-Filing System will accept reports in which those fields are left blank, however, FinCEN expects that financial institutions will provide the most complete filing information available within each report consistent with existing regulatory expectations, regardless of whether or not the individual fields are deemed critical for technical filing purposes. (NOTE: Other than the “Critical Fields”, filers should not consider the presence of the new and expanded lists of data elements as requiring them to determine as part of their reviews whether any and/or all apply to the matter being reported. Moreover, the addition of the new and expanded data elements does not create an expectation that financial institutions will revise internal programs, or develop new programs to capture information that reflects the expanded lists.

4. Attachment - Filers can include a single Microsoft Excel compatible comma separated values (CSV) file with no more than one megabyte of data as an attachment to the SAR report. This capability allows an institution to include data (such as specific financial transactions and funds transfers or other analytics), which is more readable and usable in this format, and at times is too large to record in the narrative itself. (The contents of this file however, must be described in the narrative (Part V). This attachment is considered a part of the narrative and is not considered to be a substitute for the narrative. As with other information that may be prepared in connection with the filing of a SAR, it can also be considered supporting documentation when not attached to the SAR, and should be accorded confidentiality to the extent that it indicates the existence of a SAR. Filers must retain all supporting documentation or a business record equivalent for five (5) years from the date of the report (31CFR1010.430). All supporting documentation must be made available to appropriate authorities upon request. (See "Attachment D – Batch Attachments" in the document *Electronic Filing Requirements for the FinCEN Suspicious Activity Report (FinCEN SAR)* for instructions on how to submit attachments for one or more FinCEN SARs within their batch file.)
5. Prohibited Words and Phrases -- Filers may not use the following words or variations of these words in text fields of Form 111, EXCEPT in the Narrative Section (Part V):
 - a. AKA
 - b. COMPUTER GENERATED
 - c. CUSTOMER
 - d. DBA
 - e. NON CUSTOMER
 - f. NONE
 - g. NOT APPLICABLE
 - h. OTHER
 - i. SAME
 - j. SAME AS ABOVE
 - k. SEE ABOVE
 - l. SEE NARRATIVE
 - m. SIGNATURE CARD
 - n. T/A
 - o. UNKNOWN
 - p. VARIOUS
 - q. XX
6. The narrative section of the SAR is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators. Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion. This description should encompass the data provided in Parts I through IV, but should include any other information necessary to explain the nature and circumstances of the suspicious activity. Filers should provide any information the filers believe necessary to better enable investigators to understand the reported suspicious activity. (Narratives must be completed in English).

- a. The narrative should identify the six essential elements of information (the “5 Ws” and “How”):
- (1) Who is conducting the criminal or suspicious activity? Provide any additional details about the suspect that may be relevant, e.g., employer and occupation information, the relationship between the suspect and the bank, and the length of the financial relationship.
 - (2) What instruments or mechanisms facilitated the suspect activity/transactions? Describe the transactions that raised suspicions, e.g., cash deposits and/or withdrawals, checks, foreign currency, ATM or ACH transfers, etc.
 - (3) When did the criminal or suspect activity occur? Identify the date of a one-time occurrence, when a pattern of activity was initiated together with a description of its duration, and when the suspect activity was detected.
 - (4) Where did the suspicious activity take place? Identify the branch/department locations where the activity occurred and all account numbers and account types affected.
 - (5) Why does the bank think the activity is suspicious? Describe your institution, e.g., “commercial bank with 400 branches in five states,” “state-chartered credit union with one rural location,” etc., and why the activity is considered suspicious including any relevant information about suspicious customer activity in the bank’s files at the time the SAR is filed.
 - (6) Finally, describe how the suspicious activity occurred, e.g., how the suspect transaction or pattern of transactions were completed. For account activity, provide as completely as possible an explanation of the cycle of funds including the source of the funds and their application.
- b. Organize the narrative into three parts:
- (1) Introduction: the purpose of the report, a general description of the activity, description and dates of any previously filed SARs on the subject, and any internal investigative numbers used by the bank to make records of the SAR.
 - (2) Body: all relevant facts and specifics about the activity, identifying the “5 Ws” of essential information, and how the activity occurred.
 - (3) Conclusion: summary of the report as well as any planned or completed follow-up actions.

- c. Do not include supporting documentation or any evidence that has been collected with the SAR. Any such documentation is instead retained for five years and made available to appropriate authorities upon request.
 - d. With the expanded Suspicious Activity Section of the Form 111, and with the ability to add an “attachment” with tabular details too voluminous for inclusion in previous narrative sections, Part V of the SAR is now limited to only 17,000 characters (versus the 39,000 character limit found in the legacy SAR form).
 - e. Suggestions as to additional information which can be included in the narrative section of the FinCEN SAR are available in the document titled “*FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Requirements*” available at www.fincen.gov. (Guidance on General Filing Instructions, Error Correction Instructions, and the proper handling of “Batch Attachments” are also included in the same document). In Part IV of *SAR Activity Review #22* discussions and examples of writing an effective SAR narrative were presented.
7. Correcting or Amending – A corrected report on a previously filed FinCEN SAR must be filed whenever errors are discovered in the data reported in that FinCEN SAR. An amended report must be filed on a previously filed FinCEN SAR whenever new data about a reported suspicious activity is discovered and circumstances will not justify filing a continuing report. Both corrected and amended reports must be completed in their entirety, with the necessary corrections or amendments made to the data. In both cases Box 1b “Correct or Amend prior report” must be checked, and if known, the prior report’s BSA Identifier (BSAID) must be entered in field 1e. (If the prior DCN or BSAID is unknown, zero-fill box 1e). All corrections or amendments must be described completely at the beginning of the Narrative section (Part V)
- If a FinCEN SAR is filed to correct or amend a prior FinCEN SAR version, the current FinCEN SAR must be completed in its entirety. This includes current items not that apply to the suspicious activity but were not present on the prior FinCEN SAR version. FinCEN SAR items not on the prior FinCEN SAR version need not be described in the narrative. BSA IDs are provided in acknowledgement records sent to financial institutions by the *BSA E-Filing System*.
8. “Thoughts and Musings” – Form 111 – When entering data into SAR Form 111, filers should take into consideration the following:
- a. Line 30 – If the reported event occurs on a single day, enter that date in the “From” field, and leave the “To” field blank (Note, unlike the legacy SAR, Line 30 is the date or date range of the activity FOR THIS REPORT);
 - b. Line 29 – The dollar amount for this report;
 - c. Line 31 – The cumulative amount on the “Continuing Activity” SAR;

- d. Lines 45 & 46 – If any items are checked, address items 56, 68 & 28 as well. Items 56, 68 & 28 are non-critical fields, however, and only need to be completed if they are applicable to the activity being reported. (As an example, if the activity reported involved only the structuring of cash deposits, then the reporting institution would not complete items 56, 68 & 28 as the DFI was neither a “paying” nor “selling” location in the activity being reported. If the activity involved the suspicious purchase of a cashier’s check by a client of the institution, then the reporting institution would check Item 46i, and use item 56 & 68 to indicated that it was the “Selling Location”);
- e. Line 56 & 81 – “RSSD” numbers may be obtained from your CFO, or from www.ffiec.gov/nicpubweb/content/help/HelpBranchLocatorSearch.htm ;
- f. Line 88 – This optional block provides the opportunity for the filing institution to assign a “unique-to-this-SAR-never-to-used-again” number to each report, to which law enforcement will refer to without disclosing the existence or the content of a particular SAR report;
- g. Line 93 – Contact Office – filers will now provide the office internally through which law enforcement can follow-up on the filed SAR. (This protects the confidentiality of the individuals involved in the SAR process);
- h. Filers should “SAVE” the SAR to their own system, as the *BSA E-Filing System* is a records storage and retrieval system, but not for the filing institution. **NOTE: “A filer should NOT save a copy of the SAR on a public computer or a computer that is not regularly accessed by the filer.** This will ensure that the file remains appropriately secured”;
- i. Addresses and Identifying numbers are keyed as single “strings” of data without formatting or special characters, except for the e-mail address and web address fields;
- j. Monetary amounts are keyed in U.S. Dollars, rounded up to the next whole dollar;
- k. Part 3 contains the information on where the suspicious activity occurred;
- l. Part IV records information about the lead institution, holding company, agency, or other entity that is filing the SAR. A single institution with multiple branches that also files their SARs out of the home office location, should complete Part IV with information on the home office of the institution, and then complete Part III page with information on the branch location where the activity occurred. If the activity occurs at multiple branches, items 64-70 are completed on the additional branch offices involved in the

suspicious activity being reported. In Part IV, the filing institution should enter the name of the contact office that should be contacted to obtain additional information about the report;

- m. To report “Check Kiting”, check boxes 34-D, and 34-Z, and in the box following “Z”, insert the words “Check Kiting”.
- n. Reporting Cyber Events – Cyber events directly affecting financial institutions and/or their clients are occurring on an ever-increasing basis. Prompt retrieval of cyber event information is a critical step in combating malicious cyber activity. To facilitate and support prompt identification and retrieval of malicious cyber event information, specific fields (42, 43, and 44) have been added to the Part II section of the FinCEN SAR. These fields are not meant to be exhaustive or to replace attachments. Use of these fields to highlight selected information (that may also be in attachments) can assist law enforcement in identifying key indicators. Completion of cyber event fields 42 to 44 is not mandatory, but is encouraged where financial institutions have sufficient capacity to do so. A principal source of cyber related information will be the financial institution’s internal technology department or external technology contractor. Reporting cyber event information is not a new requirement and financial institutions are expected to report this information when available.

Item 42, Cyber Event: Complete item 42 to indicate if the cyber event was directed against the financial institution or its customer/account holder. Events against the institution may include, but not be limited to, a digital denial of service (DDoS), an attempt to break (hack) into the financial institution’s computer system or attempt to take over the financial institution’s wire transfer system, the institution’s website, a Business E-Mail Attack (BEA), etc. Examples of cyber events against the institution’s clients may include the takeover (or attempted takeover) of the client’s account, the sending of bogus e-mails (BEC fraud or EAC fraud) that appear to come from the client directing various financial transactions that do not follow the client’s normal account activity, etc.

Item 43, IP Addresses: If known, enter the IP address of the subject’s electronic internet based contact with the financial institution. (If reporting an IP address in connection with a cyber-event, complete item 44).

Item 44, Cyber-event indicator: Enter the cyber-event indicator by selecting the appropriate indicator from the dropdown list provided and enter the supporting information in the associated text field. Cyber-event indicator information must be explained in the FinCEN SAR Part V – Narrative.

- o. Item 2 - Filing Institution Note to FinCEN – This 50 character field is provided for the filer to alert FinCEN that this SAR is being filed in response to a current specific geographic targeting order (GTO), or Advisory, or Guidance, or other activity. If completing the SAR

in response to a GTO or Advisory, enter the GTO/Advisory title/reference and provide a brief description of the activity. (Leave Item 2 blank if the FinCEN SAR does not relate to a specific GTO or Advisory).

C. Filing the SAR – SARs are filed electronically using FinCEN’s *BSA E-Filing System*. Financial institutions that file reports individually will use FinCEN’s discrete SAR report to file their reports. Financial institutions that use batch filing, or system-to-system to transmit multiple reports must transmit files that conform to the requirements of FinCEN’s Electronic Filing Requirements which are found at www.fincen.gov.

1. The board of directors must be informed that a SAR has been filed at the next meeting following the filing.
2. A copy of the SAR and all supporting documentation must be retained for a period of five years from the date of filing.

IV. SAFE HARBOR

A. Protection – Significant personally identifiable information is acquired and reported when a SAR is filed. Federal law (31 U.S.C. 5318(g)(3)) provides financial institutions complete protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to a regulatory requirement or on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees, and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure.

1. To fall within the “safe harbor” protection, the bank must make a good faith effort to investigate suspicious activities, document the investigation, and maintain the underlying reports and evidence that led to the SAR filing. The bank should also respond to appropriate law enforcement information requests following FinCEN Guidance 2007-G003 (June 13, 2007).
2. A bank, and any director, officer, employee, or agent of any bank that makes a voluntary disclosure of any possible violation of law or regulation to a government agency, including a disclosure made jointly with another institution, shall be protected for any such disclosure.

Suspicious Activity Report

Home

Step 1. Filing Institution
Contact Information

Step 2. Financial Institution
Where Activity Occurred

Step 3. Subject
Information

Step 4. Suspicious
Activity Information

Step 5. Narrative



Suspicious Activity Report

Version Number: 1.2

OMB No. 1506-0065 (Report)

OMB No. 1506-0001, 1506-0006, 1506-0015, 1506-0019, 1506-0029, and 1506-0061 (Regulations)

Filing Instructions:

1. Complete the report in its entirety with all requested or required data known to the filer.
2. Click "Validate" to ensure proper formatting and that all required fields are completed.
3. Click "Sign with PIN" and enter your 8-digit PIN to electronically sign the report.
4. Click "Save" to save a local copy of the report.
5. Click "Print" (*optional*) to print a paper copy of the report for record keeping purposes.
6. Click "Submit" and go to your "Track Status" to confirm acceptance.

Filing name

*1 Type of filing

(Check all that apply)

☐ Initial report

☐ Correct/Amend prior report

☐ Continuing activity report

☐ Joint report

Prior report BSA Identification
Number (BSA ID)

2 Filing Institution Note to FinCEN

Attachment

Add Attachment

Delete Attachment

View/Save Attachment

Save

Validate

Submit

Print

By providing my PIN, I acknowledge that I am electronically signing the BSA report submitted.

Sign with PIN

Release Date: 06/22/2018

Suspicious Activity Report

Home

Step 1. Filing Institution
Contact Information

Step 2. Financial Institution
Where Activity Occurred

Step 3. Subject
Information

Step 4. Suspicious
Activity Information

Step 5. Narrative

Part IV Filing Institution Contact Information

*79 Type of financial institution

*75 Primary federal regulator

*76 Filer name (Holding company, lead financial institution, or agency, if applicable)

*77 TIN *78 TIN type

80 Type of Securities and Futures institution or individual filing this report - check box(es) for functions that apply to this report

<input type="checkbox"/> Clearing broker-securities	<input type="checkbox"/> Introducing broker-securities	<input type="checkbox"/> SRO Securities
<input type="checkbox"/> CPO/CTA	<input type="checkbox"/> Investment Adviser	<input type="checkbox"/> Subsidiary of financial/bank holding company
<input type="checkbox"/> Execution-only broker securities	<input type="checkbox"/> Investment company	<input type="checkbox"/> Other <input type="text"/>
<input type="checkbox"/> Futures Commission Merchant	<input type="checkbox"/> Retail foreign exchange dealer	
<input type="checkbox"/> Holding company	<input type="checkbox"/> Self-clearing broker securities	
<input type="checkbox"/> Introducing broker-commodities	<input type="checkbox"/> SRO Futures	

81 Financial institution identification Type Number

*82 Address

*83 City

*84 State *85 ZIP/Postal Code *86 Country

87 Alternate name, e.g., AKA - individual or trade name, DBA - entity

88 Internal control/file number

89 LE contact agency

90 LE contact name

91 LE contact phone number (Include Area Code) Ext.

92 LE contact date

*93 Filing institution contact office

*94 Filing institution contact phone number (Include Area Code) Ext.

95 Date filed (Date filed will be auto-populated when the form is signed.)

Suspicious Activity Report

Home

Step 1. Filing Institution
Contact Information

Step 2. Financial Institution
Where Activity Occurred

Step 3. Subject
Information

Step 4. Suspicious
Activity Information

Step 5. Narrative

Part III Information about Financial Institution Where Activity Occurred 1 of 1

Would you like to insert all applicable filing institution information into Part III?

Yes

*51 Type of financial institution

*52 Primary federal regulator

53 Type of gaming institution

☐ State licensed casino ☐ Tribal authorized casino ☐ Card club ☐ Other (specify)

54 Type of Securities and Futures institution or individual where activity occurred - check box(es) that apply to this report

☐ Clearing broker-securities ☐ Introducing broker-securities ☐ Subsidiary of financial/bank holding company

☐ Execution-only broker securities ☐ Investment Adviser ☐ Other

☐ Futures Commission Merchant ☐ Investment company

☐ Holding company ☐ Retail foreign exchange dealer

☐ Introducing broker-commodities ☐ Self-clearing broker securities

55 Financial institution identification

Type

Number

56 Financial institution's role in transaction ☐ Selling location ☐ Paying location ☐ Both

*57 Legal name of financial institution ☐ Unknown

58 Alternate Name, e.g., AKA - individual or trade name, DBA - entity

*59 TIN ☐ Unknown 60 TIN type

*61 Address ☐ Unknown

*62 City ☐ Unknown

63 State

*64 ZIP/Postal Code ☐ Unknown

*65 Country ☐ Unknown

66 Internal control/file number

67 Loss to financial institution \$.00

Branch where activity occurred information

If no branch activity involved, check this box ☐

Branch Information

68 Branch's role in transaction ☐ Selling location ☐ Paying location ☐ Both

69 Address of branch or office where activity occurred

71 City 70 RSSD Number

72 State 73 ZIP/Postal Code *74 Country

Home	Step 1. Filing Institution Contact Information	Step 2. Financial Institution Where Activity Occurred	Step 3. Subject Information	Step 4. Suspicious Activity Information	Step 5. Narrative
Part I Subject Information 1 of 1 <div style="float: right;"> + - </div>					
3 Check: <input type="checkbox"/> if entity, <input type="checkbox"/> if all critical* subject information is unavailable (Does not include item 24)					
*4 Individual's last name or entity's legal name <input type="checkbox"/> Unknown <div style="border: 1px solid black; height: 20px; width: 100%;"></div>					
*5 First name <input type="checkbox"/> Unknown <div style="border: 1px solid black; height: 20px; width: 60%;"></div>					
6 Middle name/initial <div style="border: 1px solid black; height: 20px; width: 60%;"></div>					
7 Suffix <div style="border: 1px solid black; height: 20px; width: 60%;"></div> 8 Gender <div style="border: 1px solid black; padding: 2px;"> Male </div>					
*19 Date of birth <input type="checkbox"/> Unknown <div style="border: 1px solid black; height: 20px; width: 20%;"></div>					
9 Alternate name, e.g., AKA - individual or trade name, DBA - entity <div style="display: flex; align-items: center;"> + - <div style="border: 1px solid black; height: 20px; width: 90%;"></div> </div>					
10 Occupation or type of business <div style="border: 1px solid black; height: 20px; width: 50%;"></div>					
10a NAICS Code <div style="border: 1px solid black; height: 20px; width: 95%;"></div>					
*16 TIN <input type="checkbox"/> Unknown <div style="border: 1px solid black; height: 20px; width: 30%;"></div> 17 TIN type <div style="border: 1px solid black; padding: 2px;"> Individual </div>					
21 Phone number <div style="display: flex; align-items: center;"> + - <div style="border: 1px solid black; height: 20px; width: 20%;"></div> <div style="margin: 0 5px;">Ext.</div> <div style="border: 1px solid black; height: 20px; width: 10%;"></div> <div style="margin: 0 5px;">20 Type</div> <div style="border: 1px solid black; height: 20px; width: 10%;"></div> </div>					
22 E-mail address <div style="display: flex; align-items: center;"> + - <div style="border: 1px solid black; height: 20px; width: 95%;"></div> </div>					
22a Website (URL) address <div style="display: flex; align-items: center;"> + - <div style="border: 1px solid black; height: 20px; width: 95%;"></div> </div>					
23 Corroborative statement to filer? <div style="border: 1px solid black; padding: 2px;"> None </div> 28 Subject's role in suspicious activity <div style="border: 1px solid black; padding: 2px;"> Customer </div>					
Subject Address Information <div style="float: right;"> + - </div>					
*11 Address <input type="checkbox"/> Unknown <div style="border: 1px solid black; height: 20px; width: 70%;"></div>					
*12 City <input type="checkbox"/> Unknown <div style="border: 1px solid black; height: 20px; width: 60%;"></div>					
*13 State <input type="checkbox"/> Unknown <div style="border: 1px solid black; padding: 2px;"> CA </div> *14 ZIP/Postal Code <input type="checkbox"/> Unknown <div style="border: 1px solid black; height: 20px; width: 15%;"></div>					
*15 Country <input type="checkbox"/> Unknown <div style="border: 1px solid black; height: 20px; width: 60%;"></div>					
*18 Form of identification for subject <div style="display: flex; align-items: center;"> <input type="checkbox"/> Unknown <div style="margin-left: 20px;"> <div style="display: flex; align-items: center;"> + - </div> <div style="border: 1px solid black; height: 20px; width: 70%;"></div> </div> </div>					
Type <div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px;"> ID </div> <div style="border: 1px solid black; height: 20px; width: 70%;"></div> </div>					
Number <div style="border: 1px solid black; height: 20px; width: 30%;"></div> Country <div style="border: 1px solid black; padding: 2px;"> US </div> Issuing State <div style="border: 1px solid black; padding: 2px;"> CA </div>					
24 Relationship of the subject to an institution listed in Part III or IV (check all that apply)					
a Institution TIN <div style="border: 1px solid black; padding: 2px;"> 1234567890 </div>					
<div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;"> b <input type="checkbox"/> Accountant c <input type="checkbox"/> Agent d <input type="checkbox"/> Appraiser </div> <div style="width: 50%;"> e <input type="checkbox"/> Attorney f <input type="checkbox"/> Borrower g <input type="checkbox"/> Customer </div> <div style="width: 50%;"> h <input type="checkbox"/> Director i <input type="checkbox"/> Employee j <input type="checkbox"/> No relationship to institution </div> <div style="width: 50%;"> k <input type="checkbox"/> Officer l <input type="checkbox"/> Owner or Controlling Shareholder z <input type="checkbox"/> Other </div> </div>					
25 Status of relationship <div style="border: 1px solid black; padding: 2px;"> Customer </div> 26 Action date <div style="border: 1px solid black; padding: 2px;"> 12/31/2023 </div>					
*27 Financial institution TIN and account number(s) affected that are related to subject <input type="checkbox"/> No known accounts involved					
Institution TIN <div style="border: 1px solid black; height: 20px; width: 40%;"></div> <input type="checkbox"/> Non-US Financial Institution <div style="float: right;"> + - </div>					
<div style="display: flex; align-items: center;"> + - <div style="margin-left: 10px;"> account number <div style="border: 1px solid black; height: 20px; width: 30%;"></div> </div> <div style="margin-left: 20px;"> Closed? Yes <input type="checkbox"/> </div> </div>					

Suspicious Activity Report

Home

Step 1. Filing Institution
Contact Information

Step 2. Financial Institution
Where Activity Occurred

Step 3. Subject
Information

Step 4. Suspicious
Activity Information

Step 5. Narrative

Part II Suspicious Activity Information

*29 Amount involved in this report ☐ Amount Unknown ☐ No amount involved \$.00

*30 Date or date range of suspicious activity for this report From To

31 Cumulative amount (only applicable when "Continuing activity report" is checked in Item 1) \$.00

When completing item 32 through 42, check all that apply

32 Structuring

- | | |
|---|---|
| a <input type="checkbox"/> Alters or cancels transaction to avoid BSA recordkeeping requirement | d <input type="checkbox"/> Transaction(s) below BSA recordkeeping threshold |
| b <input type="checkbox"/> Alters or cancels transaction to avoid CTR requirement | e <input type="checkbox"/> Transaction(s) below CTR threshold |
| c <input type="checkbox"/> Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements | z <input type="checkbox"/> Other <input type="text"/> |

33 Terrorist Financing

- | | |
|--|---|
| a <input type="checkbox"/> Known or suspected terrorist/terrorist organization | z <input type="checkbox"/> Other <input type="text"/> |
|--|---|

34 Fraud

- | | | | |
|--|--|---|---|
| a <input type="checkbox"/> ACH | e <input type="checkbox"/> Consumer loan | i <input type="checkbox"/> Mass-marketing | m <input type="checkbox"/> Wire |
| b <input type="checkbox"/> Advance fee | f <input type="checkbox"/> Credit/Debit card | j <input type="checkbox"/> Ponzi scheme | z <input type="checkbox"/> Other <input type="text"/> |
| c <input type="checkbox"/> Business loan | g <input type="checkbox"/> Healthcare/Public or private health insurance | k <input type="checkbox"/> Pyramid scheme | |
| d <input type="checkbox"/> Check | h <input type="checkbox"/> Mail | l <input type="checkbox"/> Securities fraud | |

35 Gaming activities

- | | |
|--|---|
| a <input type="checkbox"/> Chip walking | d <input type="checkbox"/> Unknown source of chips |
| b <input type="checkbox"/> Minimal gaming with large transactions | z <input type="checkbox"/> Other <input type="text"/> |
| c <input type="checkbox"/> Suspicious use of counter checks or markers | |

36 Money Laundering

- | | |
|---|--|
| a <input type="checkbox"/> Exchange small bills for large bills or vice versa | h <input type="checkbox"/> Suspicious receipt of government payments/benefits |
| b <input type="checkbox"/> Funnel account | i <input type="checkbox"/> Suspicious use of multiple accounts |
| c <input type="checkbox"/> Suspicion concerning the physical condition of funds | j <input type="checkbox"/> Suspicious use of noncash monetary instruments |
| d <input type="checkbox"/> Suspicion concerning the source of funds | k <input type="checkbox"/> Suspicious use of third-party transactors (straw-man) |
| e <input type="checkbox"/> Suspicious designation of beneficiaries, assignees or joint owners | l <input type="checkbox"/> Trade Based Money Laundering/Black Market Peso Exchange |
| f <input type="checkbox"/> Suspicious EFT/wire transfers | m <input type="checkbox"/> Transaction out of pattern for customer(s) |
| g <input type="checkbox"/> Suspicious exchange of currencies | z <input type="checkbox"/> Other <input type="text"/> |

37 Identification/Documentation

- | | |
|---|---|
| a <input type="checkbox"/> Changes spelling or arrangement of name | e <input type="checkbox"/> Refused or avoided request for documentation |
| b <input type="checkbox"/> Multiple individuals with same or similar identities | f <input type="checkbox"/> Single individual with multiple identities |
| c <input type="checkbox"/> Provided questionable or false documentation | z <input type="checkbox"/> Other <input type="text"/> |
| d <input type="checkbox"/> Provided questionable or false identification | |

38 Other Suspicious Activities

- | | | |
|--|--|---|
| a <input type="checkbox"/> Account takeover | h <input type="checkbox"/> Human trafficking | o <input type="checkbox"/> Suspicious use of multiple transaction locations |
| b <input type="checkbox"/> Bribery or gratuity | i <input type="checkbox"/> Identity theft | p <input type="checkbox"/> Transaction with no apparent economic, business, or lawful purpose |
| c <input type="checkbox"/> Counterfeit instruments | j <input type="checkbox"/> Little or no concern for product performance penalties, fees, or tax consequences | q <input type="checkbox"/> Transaction(s) involving foreign high risk jurisdiction |
| d <input type="checkbox"/> Elder financial exploitation | k <input type="checkbox"/> Misuse of position or self-dealing | r <input type="checkbox"/> Two or more individuals working together |
| e <input type="checkbox"/> Embezzlement/theft/disappearance of funds | l <input type="checkbox"/> Suspected public/private corruption (domestic) | s <input type="checkbox"/> Unlicensed or unregistered MSB |
| f <input type="checkbox"/> Forgeries | m <input type="checkbox"/> Suspected public/private corruption (foreign) | z <input type="checkbox"/> Other <input type="text"/> |
| g <input type="checkbox"/> Human smuggling | n <input type="checkbox"/> Suspicious use of informal value transfer system | |

Suspicious Activity Report

Home	Step 1. Filing Institution Contact Information	Step 2. Financial Institution Where Activity Occurred	Step 3. Subject Information	Step 4. Suspicious Activity Information	Step 5. Narrative																								
<p>39 Insurance Enable this block</p> <table> <tr> <td>a <input type="checkbox"/> Excessive insurance</td> <td>e <input type="checkbox"/> Suspicious termination of policy or contract</td> </tr> <tr> <td>b <input type="checkbox"/> Excessive or unusual cash borrowing against policy/annuity</td> <td>f <input type="checkbox"/> Unclear or no insurable interest</td> </tr> <tr> <td>c <input type="checkbox"/> Proceeds sent to or received from unrelated third party</td> <td>z <input type="checkbox"/> Other <input type="text"/></td> </tr> <tr> <td>d <input type="checkbox"/> Suspicious life settlement sales insurance (e.g., STOLI's, Viaticals)</td> <td></td> </tr> </table>						a <input type="checkbox"/> Excessive insurance	e <input type="checkbox"/> Suspicious termination of policy or contract	b <input type="checkbox"/> Excessive or unusual cash borrowing against policy/annuity	f <input type="checkbox"/> Unclear or no insurable interest	c <input type="checkbox"/> Proceeds sent to or received from unrelated third party	z <input type="checkbox"/> Other <input type="text"/>	d <input type="checkbox"/> Suspicious life settlement sales insurance (e.g., STOLI's, Viaticals)																	
a <input type="checkbox"/> Excessive insurance	e <input type="checkbox"/> Suspicious termination of policy or contract																												
b <input type="checkbox"/> Excessive or unusual cash borrowing against policy/annuity	f <input type="checkbox"/> Unclear or no insurable interest																												
c <input type="checkbox"/> Proceeds sent to or received from unrelated third party	z <input type="checkbox"/> Other <input type="text"/>																												
d <input type="checkbox"/> Suspicious life settlement sales insurance (e.g., STOLI's, Viaticals)																													
<p>40 Securities / Futures / Options Enable this block</p> <table> <tr> <td>a <input type="checkbox"/> Insider trading</td> <td>d <input type="checkbox"/> Unauthorized pooling</td> </tr> <tr> <td>b <input type="checkbox"/> Market manipulation</td> <td>e <input type="checkbox"/> Wash trading</td> </tr> <tr> <td>c <input type="checkbox"/> Misappropriation</td> <td>z <input type="checkbox"/> Other <input type="text"/></td> </tr> </table>						a <input type="checkbox"/> Insider trading	d <input type="checkbox"/> Unauthorized pooling	b <input type="checkbox"/> Market manipulation	e <input type="checkbox"/> Wash trading	c <input type="checkbox"/> Misappropriation	z <input type="checkbox"/> Other <input type="text"/>																		
a <input type="checkbox"/> Insider trading	d <input type="checkbox"/> Unauthorized pooling																												
b <input type="checkbox"/> Market manipulation	e <input type="checkbox"/> Wash trading																												
c <input type="checkbox"/> Misappropriation	z <input type="checkbox"/> Other <input type="text"/>																												
<p>41 Mortgage Fraud</p> <table> <tr> <td>a <input type="checkbox"/> Application fraud</td> <td>d <input type="checkbox"/> Loan Modification fraud</td> </tr> <tr> <td>b <input type="checkbox"/> Appraisal fraud</td> <td>e <input type="checkbox"/> Origination fraud</td> </tr> <tr> <td>c <input type="checkbox"/> Foreclosure/Short sale fraud</td> <td>z <input type="checkbox"/> Other <input type="text"/></td> </tr> </table>						a <input type="checkbox"/> Application fraud	d <input type="checkbox"/> Loan Modification fraud	b <input type="checkbox"/> Appraisal fraud	e <input type="checkbox"/> Origination fraud	c <input type="checkbox"/> Foreclosure/Short sale fraud	z <input type="checkbox"/> Other <input type="text"/>																		
a <input type="checkbox"/> Application fraud	d <input type="checkbox"/> Loan Modification fraud																												
b <input type="checkbox"/> Appraisal fraud	e <input type="checkbox"/> Origination fraud																												
c <input type="checkbox"/> Foreclosure/Short sale fraud	z <input type="checkbox"/> Other <input type="text"/>																												
<p>42 Cyber event</p> <table> <tr> <td>a <input type="checkbox"/> Against Financial Institution(s)</td> <td>z <input type="checkbox"/> Other <input type="text"/></td> </tr> <tr> <td>b <input type="checkbox"/> Against Financial Institution Customer(s)</td> <td></td> </tr> </table>						a <input type="checkbox"/> Against Financial Institution(s)	z <input type="checkbox"/> Other <input type="text"/>	b <input type="checkbox"/> Against Financial Institution Customer(s)																					
a <input type="checkbox"/> Against Financial Institution(s)	z <input type="checkbox"/> Other <input type="text"/>																												
b <input type="checkbox"/> Against Financial Institution Customer(s)																													
<p>45 Were any of the following product type(s) involved in the suspicious activity? (Check all that apply)</p> <table> <tr> <td>a <input type="checkbox"/> Bonds/Notes</td> <td>g <input type="checkbox"/> Forex transactions</td> <td>m <input type="checkbox"/> Microcap securities</td> <td>s <input type="checkbox"/> Stocks</td> </tr> <tr> <td>b <input type="checkbox"/> Commercial mortgage</td> <td>h <input type="checkbox"/> Futures/Options on futures</td> <td>n <input type="checkbox"/> Mutual fund</td> <td>t <input type="checkbox"/> Swap, hybrid, or other derivatives</td> </tr> <tr> <td>c <input type="checkbox"/> Commercial paper</td> <td>i <input type="checkbox"/> Hedge fund</td> <td>o <input type="checkbox"/> Options on securities</td> <td>z <input type="checkbox"/> Other (List below)</td> </tr> <tr> <td>d <input type="checkbox"/> Credit card</td> <td>j <input type="checkbox"/> Home equity line of credit</td> <td>p <input type="checkbox"/> Prepaid access</td> <td><input type="text"/></td> </tr> <tr> <td>e <input type="checkbox"/> Debit card</td> <td>k <input type="checkbox"/> Home equity loan</td> <td>q <input type="checkbox"/> Residential mortgage</td> <td></td> </tr> <tr> <td>f <input type="checkbox"/> Deposit account</td> <td>l <input type="checkbox"/> Insurance/Annuity products</td> <td>r <input type="checkbox"/> Security futures products</td> <td></td> </tr> </table>						a <input type="checkbox"/> Bonds/Notes	g <input type="checkbox"/> Forex transactions	m <input type="checkbox"/> Microcap securities	s <input type="checkbox"/> Stocks	b <input type="checkbox"/> Commercial mortgage	h <input type="checkbox"/> Futures/Options on futures	n <input type="checkbox"/> Mutual fund	t <input type="checkbox"/> Swap, hybrid, or other derivatives	c <input type="checkbox"/> Commercial paper	i <input type="checkbox"/> Hedge fund	o <input type="checkbox"/> Options on securities	z <input type="checkbox"/> Other (List below)	d <input type="checkbox"/> Credit card	j <input type="checkbox"/> Home equity line of credit	p <input type="checkbox"/> Prepaid access	<input type="text"/>	e <input type="checkbox"/> Debit card	k <input type="checkbox"/> Home equity loan	q <input type="checkbox"/> Residential mortgage		f <input type="checkbox"/> Deposit account	l <input type="checkbox"/> Insurance/Annuity products	r <input type="checkbox"/> Security futures products	
a <input type="checkbox"/> Bonds/Notes	g <input type="checkbox"/> Forex transactions	m <input type="checkbox"/> Microcap securities	s <input type="checkbox"/> Stocks																										
b <input type="checkbox"/> Commercial mortgage	h <input type="checkbox"/> Futures/Options on futures	n <input type="checkbox"/> Mutual fund	t <input type="checkbox"/> Swap, hybrid, or other derivatives																										
c <input type="checkbox"/> Commercial paper	i <input type="checkbox"/> Hedge fund	o <input type="checkbox"/> Options on securities	z <input type="checkbox"/> Other (List below)																										
d <input type="checkbox"/> Credit card	j <input type="checkbox"/> Home equity line of credit	p <input type="checkbox"/> Prepaid access	<input type="text"/>																										
e <input type="checkbox"/> Debit card	k <input type="checkbox"/> Home equity loan	q <input type="checkbox"/> Residential mortgage																											
f <input type="checkbox"/> Deposit account	l <input type="checkbox"/> Insurance/Annuity products	r <input type="checkbox"/> Security futures products																											
<p>46 Were any of the following instrument type(s)/payment mechanism(s) involved in the suspicious activity? (Check all that apply)</p> <table> <tr> <td>a <input type="checkbox"/> Bank/Cashier's check</td> <td>d <input type="checkbox"/> Gaming instruments</td> <td>g <input type="checkbox"/> Personal/Business check</td> <td>z <input type="checkbox"/> Other (List below)</td> </tr> <tr> <td>b <input type="checkbox"/> Foreign currency</td> <td>e <input type="checkbox"/> Government payment</td> <td>h <input type="checkbox"/> Travelers checks</td> <td><input type="text"/></td> </tr> <tr> <td>c <input type="checkbox"/> Funds transfer</td> <td>f <input type="checkbox"/> Money orders</td> <td>i <input type="checkbox"/> U.S. Currency</td> <td></td> </tr> </table>						a <input type="checkbox"/> Bank/Cashier's check	d <input type="checkbox"/> Gaming instruments	g <input type="checkbox"/> Personal/Business check	z <input type="checkbox"/> Other (List below)	b <input type="checkbox"/> Foreign currency	e <input type="checkbox"/> Government payment	h <input type="checkbox"/> Travelers checks	<input type="text"/>	c <input type="checkbox"/> Funds transfer	f <input type="checkbox"/> Money orders	i <input type="checkbox"/> U.S. Currency													
a <input type="checkbox"/> Bank/Cashier's check	d <input type="checkbox"/> Gaming instruments	g <input type="checkbox"/> Personal/Business check	z <input type="checkbox"/> Other (List below)																										
b <input type="checkbox"/> Foreign currency	e <input type="checkbox"/> Government payment	h <input type="checkbox"/> Travelers checks	<input type="text"/>																										
c <input type="checkbox"/> Funds transfer	f <input type="checkbox"/> Money orders	i <input type="checkbox"/> U.S. Currency																											
<p>43 IP Address (enter the IP address/date/timestamp of the subject's electronic internet based contact with the financial institution, if known)</p> <p> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> </p>																													
<p>44 Cyber Event Indicators (select the appropriate indicator(s) from the drop-down list and provide the associated supporting information)</p> <p> Event type <input type="text"/> <input type="text"/> <input type="text"/> </p> <p> Event value <input type="text"/> <input type="text"/> <input type="text"/> </p>																													
<p>47 Commodity type (if applicable) <input type="text"/></p>																													
<p>48 Product/Instrument description (if needed) <input type="text"/></p>																													
<p>49 Market where traded <input type="text"/></p>																													
<p>50 CUSIP® number <input type="text"/></p>																													

Suspicious Activity Report

Home

Step 1. Filing Institution
Contact Information

Step 2. Financial Institution
Where Activity Occurred

Step 3. Subject
Information

Step 4. Suspicious
Activity Information

Step 5. Narrative

Part V Suspicious Activity Information - Narrative* [See Instructions](#)

V. LIMITS ON DISCLOSING SAR INFORMATION

- A. Confidentiality of SARS** – A SAR, and any information that would reveal the existence of a SAR are confidential and shall not be disclosed except as authorized in the regulation.
- B. Prohibition on Disclosures by Banks** – No bank, and no director, officer, employee, or agent of any bank, shall disclose a SAR or any information that would reveal the existence of a SAR. Any bank, and any director, officer, employee, or agent of any bank that is subpoenaed or otherwise requested to disclose a SAR or any information that would reveal the existence of a SAR shall decline to produce the SAR or such information citing, 31 CFR 1020.320 (e)(1), and 31 U.S.C. 5318(g)(2)(A)(i), and shall notify FinCEN's Office of Chief Counsel (703-905-3590), and the financial institution's primary federal regulator of any such request and the response thereto.
- C. Unauthorized Disclosure Penalties** - The unauthorized disclosure of SARs is a violation of federal law. Both civil and criminal penalties may be imposed for SAR disclosure violations. Violations may be enforced through civil penalties of up to \$100,000 for each violation, and criminal penalties of up to \$250,000 and/or imprisonment not to exceed five years. In addition, financial institutions could be liable for civil money penalties resulting from anti-money laundering program deficiencies that led to the improper SAR disclosure. Such penalties could be up to \$25,000 per day for each day the violation continues. (See FinCEN Advisory 2010-A014, 11/23/10).
- D. Exceptions** – Provided that no person involved in any reported suspicious transaction is notified that the transaction has been reported, the prohibition on disclosure does not prohibit:
1. The disclosure by a bank, or any director, officer, employee or agent of a bank of a SAR, or any information that would reveal the existence of a SAR to FinCEN, or any Federal, State, or local law enforcement agency, or to any Federal regulatory authority that examines the bank for compliance with the Bank Secrecy Act, or to any State regulatory authority administering a State law that requires the bank to comply with the Bank Secrecy Act or otherwise authorizes the State authority to ensure that the bank complies with the Bank Secrecy Act.

NOTE: In the instances where State agencies request that copies of SARs filed with FinCEN be provided to the State authority ("dual-filings"), financial institutions should provide SAR information only to those State entities that administer a State law that requires financial institutions to comply with the BSA, or State entities that otherwise are authorized to ensure that the financial institution complies with the BSA. State entities that do not meet the regulatory test should seek access directly from FinCEN for SAR information. (75FR75598).

2. The disclosure of the underlying facts, transactions, or documents upon which a SAR is based, including but not limited to, disclosures:
 - a. To another financial institution, or any director, officer, employee or agent of a financial institution, for the preparation of a joint SAR; or

- b. In connection with certain written employment referral requests or termination notices. (Provided the disclosure is not made with malicious intent, there is complete protection from civil liability under this exception. Even though the bank can disclose information contained in a SAR under the written employment referral exception, the bank is prohibited from disclosing the fact that a SAR was filed).

NOTE: Clearly, any document or other information that affirmatively states that a SAR has been filed, and by extension, any document that states that a SAR has not been filed, should be afforded confidentiality. “Underlying documents” (e.g., a document memorializing a customer transaction such as an account statement indicating a cash deposit, or a record of funds transfer) may identify suspicious activity, but if they do not reveal that a SAR exists that document should not be afforded this SAR confidentiality.

NOTE: Additional commenters requested guidance from FinCEN regarding the appropriate use of SARs by agents of the financial institution, including independent auditors or other contracted service providers (e.g. information technology, legal counsel, etc). FinCEN is considering additional guidance on these matters, but until such guidance is issued, FinCEN reminds financial institutions of their ultimate responsibility to protect through reasonable controls or agreements with such agents, the confidentiality of a SAR, or any information that would reveal the existence of a SAR.

NOTE: In the BSA/AML Compliance Program – Overview section contained within the interagency *Bank Secrecy Act/Anti-Money Laundering Examination Manual (2014)*, it states that the independent testing (for BSA/AML compliance) should at a minimum include “an assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the bank’s policy”.

(See 75 FR 75593 – 75607, 12/03/2010).

- E. SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions** – On March 02, 2012, FinCEN issued Advisory FIN-2012-A002, to remind financial institutions, and in particular, the lawyers that advise them, of the requirement to maintain the confidentiality of the Suspicious Activity Reports (SARs). FinCEN remains concerned that an increasing number of private parties who are not authorized to know of the existence of filed SARs, are seeking SARs from financial institutions for use in civil litigation and other matters. Financial institutions, and their current or former directors, officers, employees, agents, and contractors, are prohibited from disclosing SARs, or any information that would reveal the existence of a SAR. (FinCEN recognizes that an escalation in the number of requests for the use of SARs in private litigation may increase the likelihood of an unauthorized disclosure of a SAR). Additional risk-based measures to enhance the confidentiality of SARs could include limiting access to SARs on a “need-to-know” basis, restricting areas for reviewing SARs, logging access to SARs, and

using cover sheets for SARs or information that reveals the existence of a SAR. FinCEN's Office of Chief Counsel can be reached at: 703-905-3590.

- F. Sharing SARs by Depository Institutions with Certain U.S. Affiliates** - The sharing of a SAR, or any information that would reveal the existence of a SAR with "certain" affiliates within the bank's corporate organizational structure, provided that the affiliate is subject to a SAR regulation is allowed under the regulations. (This expands on the FinCEN Guidance from January 20, 2006 that stated that a U.S. bank or savings association may share a SAR with its controlling company (whether domestic or foreign), and a U.S. branch or agency of a foreign bank may share a SAR with its head office). An affiliate of an authorized institution that receives shared SAR information may not then share the SAR information with its own affiliates.

NOTE: There may be circumstances under which a depository institution, its affiliate, or both entities would be liable for direct or indirect disclosure by the affiliate of a SAR or any information that would reveal the existence of a SAR. Therefore, the depository institution, as part of its internal controls, should have policies and procedures in place to ensure that its affiliates protect the confidentiality of the SAR. (These policies and procedures do not replace the confidentiality agreements required under the January 2006 guidance).

NOTE: An "Affiliate" of a depository financial institution means any company under common control with, or controlled by, that depository institution. "Under common control" means that another company (1) directly or indirectly or acting through one or more persons owns, controls, or has the power to vote 25% or more of any class of the voting securities of the company and the depository institution; or (2) controls in any manner the election of a majority of the directors or trustees of the company of the depository institution. "Controlled by" means that the depository institution (1) directly or indirectly has the power to vote 25% or more of any class of the voting securities of the company; or (2) controls in any manner the election of a majority of the directors or trustees of the company.

(See FinCEN Guidance 2010-G006, 11/23/2010, and 75FR 75607- 75610).

VI. OTHER FINCEN SAR GUIDANCE

- A. Mortgage "Scams"** - FinCEN has issued an advisory (FIN – 2009 – A001) requesting the industry's assistance in identifying and reporting any business involved in Loan Modification/Foreclosure Rescue Scams. Persons or entities perpetrating these loan modification/foreclosure rescue scams may seek the services of DFIs for the purpose of receiving, depositing, or moving the funds associated with these scams. DFIs may also become aware of such scams through their interactions with clients who have become the victim of such a scam. (The advisory provides a list of "red-flags" that could be indicators of the presence of a foreclosure rescue scam). If a DFI suspects that a loan modification/foreclosure rescue scam has taken place, a SAR should be filed containing all relevant information (remembering that the homeowner is not the suspect, they are the victim), and the words "Foreclosure Rescue Scam" should go on the first line of the SAR narrative. On November 17, 2009, DOJ, DOT, HUD and the SEC announced the establishment of an interagency financial fraud enforcement task force to strengthen efforts to combat financial crime.

- B. L/E Requests to Maintain Accounts** - FinCEN Guidance (2007-G002, June 13, 2007 – Requests by Law Enforcement for Financial Institutions to Maintain Accounts) states that if a law enforcement agency requests that a financial institution maintain a particular account to facilitate an ongoing investigation, the financial institution should ask for a written request to support the request. The request should be issued by a supervisory agent or by an attorney in the United States Attorney’s Office, or another office in the Department of Justice. If a state or local law enforcement agency requests that an account be maintained, the written request should come from a supervisor of the state or local law enforcement agency or from an attorney within a state or local prosecutor’s office. The written request should indicate that the agency has requested that the financial institution maintain the account, and the purpose of the request. The request should also indicate the duration for the request, not to exceed six months. (Law enforcement may issue subsequent requests for account maintenance after the expiration of the initial request). FinCEN recommends that financial institutions maintain documentation of such requests for five years after the request has expired.

ULTIMATELY, the decision to maintain or close an account should be made by a FINANCIAL INSTITUTION in accordance with its own standards and guidelines. Although there is no requirement that a financial institution maintain a particular account relationship, financial institutions should be mindful that complying with such a request may further law enforcement efforts to combat money laundering, terrorist financing, and other crimes. If a financial institution chooses to maintain an account in response to a request from law enforcement, it is required to comply with all applicable BSA Rules, including the filing of SARs.

- C. Requests for SAR Supporting Documentation** - FinCEN Guidance (2007-G003, June 13, 2007 – Suspicious Activity Reporting Supporting Documentation) states that when a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. Financial institutions must provide all documentation supporting the filing of the SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency. (Financial institutions should take care to verify that a requestor of information is in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. Independent employment verification of the requestor with the requestor’s filed office, or face-to-face review of the requestor’s credentials are examples of such verification.)

“Supporting documentation” refers to all documents or records that assisted a financial institution in making the determination that certain activity required a SAR filing, and a financial institution must identify supporting documentation at the time the SAR is filed, in the narrative section of the SAR. Examples of supporting documentation include transaction records, new account information, tape recordings, e-mail messages, and correspondence.

Although the Right to Financial Privacy Act generally prohibits financial institutions from disclosing a customer’s financial records to a Government agency without service of legal process, no such requirement applies when FinCEN or an appropriate law enforcement agency or supervisory agency requests either a copy of the SAR or supporting documentation underlying the SAR.

- D. Regulation GG Impact - Prohibition on Funding of Unlawful Internet Gambling** - On November 18, 2008, the Treasury Department and the Federal Reserve Bank published the Final Rule implementing the applicable provisions of the Unlawful Internet Gambling Enforcement Act. All non-exempt participants in designated payment systems shall establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions.

Under the final Rule, the term “restricted transaction” would not include funds going to a gambler, and would only include funds going to an internet gambling business. However, under the final Rule, nothing in such Rule modifies any requirement imposed on any participant by other applicable law or regulation to file a SAR to the appropriate authorities. The effective date of this regulation was January 19, 2009, with compliance by non-exempt participants in designated payment systems not required until June 1, 2010. (73 FR 69382 – 69411 and 74 FR 62687).

- E. Elder Financial Exploitation – FinCEN Advisory 2011-A-003 (February 22, 2011)** – Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation provides assistance to the industry in reporting instances of financial exploitation of the elderly, which is a form of elder abuse. Often financial institutions are quick to suspect elder financial exploitation based on personnel familiarity to their elderly clients. While anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable.

Advisory 2011-A003 contains examples of “Red-Flags” that COULD indicate the existence of elder financial exploitation. Institutions should evaluate indicators of potential financial exploitation in combination with other “red-flags” and expected transaction activity being conducted by or on behalf of the elder. Institutions may become aware of persons or entities perpetrating illicit activity against the elderly through monitoring transaction not consistent with expected behavior, and through their direct interactions with the elderly clients who are being financially exploited. When completing the BSA-SAR, check box 38-D and use the description “Elder Financial Exploitation”, and check any other block in sections 45 and 46 that apply to the specific situation being reported. In addition, in the first part of the narrative, display the words “Elder Financial Exploitation” prominently to assist law enforcement in identifying these situations.

NOTE: On December 4, 2019, FinCEN released a strategic analysis of BSA reporting, indicating that elders face an increased threat to their financial security by both domestic and foreign actors. Elder financial exploitation SARs increased dramatically over the six-year study period. Several major scam categories were identified including: Romance; Emergency/Person-in-Need; and Prize/Lottery. The study also found that when the elder is the victim of theft from a bank or brokerage account, family members and non-family member caregivers are most often implicated. The entire analysis is available at: <https://www.fincen.gov/news/news-releases/fincen-analysis-bank-secrecy-act-reports-filed-financial-institutions-help>.

NOTE: The elderly victim of the possible abuse is not the suspect, and should not be reported as the subject of the SAR. All available information on the elderly victim should be included in the narrative portion of the SAR.

NOTE: Elder abuse, including financial exploitation, is generally reported and investigated at the local level. SAR filers should continue to report all forms of elder abuse according to institutional policies and procedures and the requirements of state and local laws and regulations where applicable.

- F. Account Takeover Activity – FinCEN Advisory 2011 – A016 (December 19, 2011)** - Advisory to assist financial institution with identifying account takeover activity and reporting the activity through the filing of SARs. Cybercriminals are increasingly using sophisticated methods to obtain access to accounts, including the use of malware, SQL injection attacks, spyware, Trojans, and worms. These attacks aim to deliberately exploit a client's account and in many instances, to gain seemingly legitimate access to another client's accounts. Through ongoing monitoring, financial institutions may identify inconsistencies with a client's normal account activity which could include unusual ATM activity, clustered ACH transactions in different geographic areas, sudden wire transfers, or changes to customer and account profiles. Account takeover activity differs from other forms of computer intrusion as the client, rather than the financial institution, is the primary target.

When completing a BSA-SAR for suspected account takeover activity, institutions should check Box 38-A "account takeover." The reference to "account takeover" should also appear in the narrative section of the SAR, along with a detailed description of the activity. Additional boxes in Blocks 45 and 46 should also be checked to enhance the usefulness of the SAR filing.

- G. Update on Tax Refund Fraud and Related Identity Theft – FinCEN Advisory 2013-A001 – (February 26, 2013)** – Advisory to remind financial institutions of previously-published information concerning tax refund fraud and the subsequent reporting of such activity through the filing of Suspicious Activity Reports (SARs). Identity theft can be a precursor to tax fraud because individual income tax returns filed in the United States are tracked and processed by TINs and the individual taxpayer names associated with these numbers. Criminals can obtain TINs through various methods of identity theft, including phishing schemes and the establishment of fraudulent tax preparation businesses. In response to this problem, the IRS has developed a comprehensive strategy focused on preventing, detecting, and resolving instances of tax-related identity theft crimes. Financial institutions are critical in identifying tax refund fraud because the methods for tax refund distribution – issuance of paper checks and direct deposit into demand deposit or prepaid access card accounts – often involve various financial service providers, and the number of tax refunds being distributed via direct deposit has increased significantly over the past several years and continues to increase annually.

Advisory 2013-A001 (and its precursor, 2012-A005) has identified a number of "red-flags" to assist in the identification and reporting of tax refund fraud including but not limited to:

1. Multiple direct deposit tax refund payments, directed to different individuals, from the U.S. Department of Treasury or from state or local revenue offices, made to a demand deposit or prepaid access account held in the name of a single accountholder;
2. Suspicious or authorized account opening at a depository institution, on behalf of individuals who are not present, with the absent individuals being accorded signatory authority over the account. The subsequent

deposits are comprised solely of tax refunds payments. (This activity often occurs with fraudulent returns for the elderly, minors, prisoners, the disabled, or the recently deceased);

3. A single individual opening multiple prepaid card accounts in different names, using valid TINs for each of the supplied names and having the cards mailed to the same address. Shortly after card activation, ACH credits from Treasury, state or local offices representing tax refunds occur, followed quickly by ATM withdrawals and/or POS purchases;
4. Business accountholders processing third-party tax refund checks in a manner inconsistent with their stated business model or at a volume inconsistent with expected activity. Similarly, individuals processing third-party tax refund checks through a personal account with no business or apparent lawful purpose;
5. Business accountholders processing third-party tax refund checks that are of a significant volume when compared to other checks cashed, or a large volume of checks bear the addresses of customers out of state, or the checks are sequentially numbered or within a few numbers of each other;
6. The opening of a business account for a check cashing business, which subsequently processes a high volume of tax refund checks for individuals from other states;
7. Individuals attempting to negotiate double endorsed Treasury tax refund checks with questionable identification; and
8. Employees of financial institutions may also facilitate tax refund fraud, including tellers who regularly process large quantities of tax refund checks, including one or more tellers during a specific time frame.

When completing a SAR on suspected tax-refund fraud, financial institutions should check box 34-Z, insert the words “Tax-Refund Fraud” in the accompanying box, and in the narrative, use the same term and provide a detailed description of the activity. Due to the time sensitive nature of these transactions, a financial institution may also wish to contact their local IRS-CID field office to alert them to the fact that a SAR has been filed related to tax refund fraud. (Contact information for IRS-CID can be obtained from FinCEN’s Regulatory Helpline).

- H. BSA Expectations Regarding Marijuana-Related Businesses – FinCEN Guidance FIN-2014 - G001 – February 14, 2014** - Guidance to clarify “how” financial institutions can provide services to marijuana-related businesses consistent with their BSA related obligations, and aligns the information provided by financial institutions in BSA reports with federal and state law enforcement priorities. In general, “the decisions to open, close, or refuse any particular account or relationship should be made by each financial institution based on a number of factors specific to that institution”. These factors may include its particular business objectives, an evaluation of the risks associated with offering a particular product or service, and its capacity to manage those risks effectively. The obligation to file a SAR is unaffected by any state law that legalizes marijuana-related activity, and a financial institution that provides banking services to a marijuana-related business is required to file SARs as follows:

- “*Marijuana-Limited*” – identifying businesses engaged in marijuana-related activity;
- “*Marijuana-Priority*” – the marijuana-related business implicates one of the “Cole memo” priorities or violates state law; and
- “*Marijuana-Termination*” – if the institution decides to terminate the relationship with a marijuana-related business, a “marijuana-termination” SAR should be filed. If the financial institution suspects the marijuana-related business is moving to another DFI, the 314(b) process can be utilized to alert the second DFI as to potential illegal activity.

The Guidance from FinCEN includes red flags that might indicate that a marijuana-related business may be engaged in activity that implicates one of the “Cole memo” priorities or violates state law, and the presence of such could indicate the need to file a SAR (Marijuana-Priority). This Guidance is available at www.fincen.gov.

I. Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity – FinCEN Advisory FIN – 2020 – A008 – October 15, 2020 –

FinCEN issued this Advisory, which supplements the *2014 Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags*, to help save lives, and to protect the most vulnerable in our society from predators and cowards who prey on the innocent and defenseless for money and greed. Human traffickers and their facilitators exploit adults and children in the United States, and around the world, for financial gain, among other reasons. Victims are placed into forced labor, slavery, involuntary servitude, and peonage, and/or forced to engage in commercial sex acts. Anyone can be a victim regardless of origin, sex, age, or legal status. And anyone can be a trafficker, from a single individual, such as a family member, to a criminal network, terrorist organization, or corrupt government regime. The global COVID-19 pandemic can exacerbate the conditions that contribute to human trafficking, as the support structures for potential victims collapse and traffickers target those most impacted and vulnerable. In the United States, human trafficking now occurs in a broad range of licit and illicit industries (e.g., hospitality, agricultural, janitorial services, construction, restaurants, care for persons with disabilities, salon services, massage parlors, retail, fairs and carnivals, peddling and begging, child care, domestic work, and drug smuggling and distribution).

Since the 2014 Advisory, FinCEN (working with law enforcement) has identified 20 new financial and behavioral indicators of labor and sex trafficking, and four additional typologies. (The 2014 Advisory remains relevant, and provides information related to human smuggling in addition to human trafficking). The four new identified typologies include: Front Companies – where illicit proceeds are mixed with proceeds from legitimate business operations; Exploitive Employment Practices – such as visa fraud and wage retention; Funnel Accounts – where the traffickers use interstate funnel accounts to transfer funds between geographic areas, move proceeds rapidly, and maintain anonymity; and Alternative Payment Methods, such as credit cards, prepaid cards, mobile payment applications, and convertible currency. The 2020 Advisory provides both updated behavioral and financial red-flag indicators that could indicate the presence of human trafficking.

When filing a SAR in response to this Advisory, the financial institution should provide all pertinent available information in the SAR form and narrative. A potential victim of human trafficking should not be reported as the subject of the SAR, but all available information about the victim should be included in the narrative section of the report. Financial institutions should include the key term “Human Trafficking FIN-2020-A008 in Field 2 of the SAR and in the narrative. Financial institutions should also check box 38(h) on the SAR form, and include behavioral indicators, email addresses, phone numbers, and IP addresses to aid law enforcement investigations.

- J. Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes – FinCEN Advisory FIN-2019-A005 – July 16, 2019** (Updates FinCEN Advisory FIN-2016-A003 – 09/06/16) – Updated Advisory to alert financial institutions to predominant trends in reported business email compromise (BEC) fraud, including key sectors, entities, and vulnerable business processes targeted in many BEC schemes. This updated advisory offers updated operational definitions of email compromise fraud; provides information on the targeting of non-business entities and data by BEC schemes; highlights general trends in BEC schemes targeting sectors and jurisdictions; and alerts financial institutions to risks associated with the targeting of vulnerable business processes by BEC criminals. (The red flags from the 2016 BEC Advisory remain relevant and can be useful to financial institutions in better identifying and reporting instances of BEC Fraud.) This Advisory will assist financial institutions in recognizing and guarding against increased email compromise fraud schemes and in considering their own or their customers’ potential vulnerability to compromise of payment authorization and communications from email compromise fraud.

FinCEN broadens its definitions of email compromise fraud activities to clarify that such fraud targets a variety of types of entities and may be used to misdirect any kind of payment or transmittal of other things of value. While many email compromise fraud scheme payments are carried out via wire transfer, FinCEN has observed BEC schemes fraudulently inducing funds or value transfers through other methods of payment to include convertible virtual currency (CVC) payments, ACH transfers, and purchases of gift cards. The updated and expanded definitions of email compromise fraud now read:

- Email Compromise Fraud: Schemes in which 1) criminals compromise the email accounts of victims to send fraudulent payment instructions to financial institutions or other business associates in order to misappropriate funds or value; or in which 2) criminal compromise the email accounts of victims to effect fraudulent transmission of data that can be used to conduct financial fraud. The main types of email compromise include:
 - Business Email Compromise (BEC): Targets accounts of financial institutions or customers of financial institutions that are operational entities, including commercial, non-profit, not-governmental, or government entities.
 - Email Account Compromise (EAC): Targets personal email accounts belonging to an individual.

FinCEN analysis has indicated criminal groups use a variety of techniques to conduct BEC fraud against individuals, particularly and increasingly those with high net worth, and entities that routinely use email to make or arrange payments between partners, customers, or suppliers. The targets of these schemes fall

outside of the definition of traditional business customers, such as government entities and non-profit organizations or even the financial institutions themselves. FinCEN analysis also reveals that the top three business sectors commonly targeted in BEC Schemes are manufacturing and construction, commercial services, and real estate. FinCEN analysis also indicates the majority of BEC incidents affecting U.S. financial institutions and their customers increasingly involve initial domestic funds transfers, likely taking advantage of money mule networks across the United States to move the stolen funds. Once the funds are moved internationally, the top destinations reported by the FBI are China, Hong Kong, the United Kingdom, Mexico, and Turkey.

Due to the nature of BEC and EAC schemes, FinCEN encourages communication among financial institutions under the auspices of Section 314(b) to share valuable information about BEC beneficiaries and perpetrators for the purposes of identifying and where appropriate, reporting activities that they suspect may involve possible terrorist activity or money laundering. In filing SARs, institutions should reference this Advisory in Field 2, list either BEC or EAC fraud in the SAR Narrative, and highlight cyber-event (field 42), and cyber-event indicators (field 44 (a)-(j), (z)). In instances of reporting BEC schemes that result in the communication of *information* that may be used to facilitate future fraudulent transactions, which may be voluntary, FinCEN requests that the term “*BEC Data Theft*” be included in the SAR narrative.

K. Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime – FinCEN Advisory 2016-A005 – Frequently Asked Questions (FAQs) -- October 25, 2016 – FinCEN has issued this advisory and accompanying FAQs document to assist financial institutions in understanding their BSA obligations regarding cyber-events and cyber-enabled crime. The advisory advises institutions on:

1. Reporting cyber-enabled crime and cyber-events through SARs;
2. Including relevant and available cyber-related information (e.g. Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SAR reports;
3. Collaborating between BSA/Anti-Money Laundering (AML) units and in-house cyber-security units to identify (and then report) suspicious activity; and
4. Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime.

For purposes of this advisory:

- Cyber-Event is defined as an attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information;
- Cyber-Enabled Crime is defined to include illegal activities (e.g. fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.
- Cyber- Related Information is defined to include information that describes technical details of electronic activity and behavior, such as IP addresses,

timestamps, and “Indicators of Compromise” (IOCs). Cyber-related information also includes but is not limited to, data regarding the digital footprint of individuals and their behavior.

Cyber-events targeting financial institutions often constitute criminal activity and can serve as means to commit a wide range of further criminal activity. Cyber-Events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities. (To determine the monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event). As everyday financial transactions increasingly rely on electronic systems and resources, illicit financial activity often has a digital footprint, which may correspond to illicit actors and their associates, their activity, and related suspicious transactions. Financial institutions SHOULD include available cyber-related information when reporting any suspicious activity, including those related to cyber-events as well as those related to other activity such as fraudulent wire transfers. To the extent available, SARs involving cyber-events should include:

- Description and magnitude of the event;
- Known or suspected time, location, and characteristics or signatures of the event;
- Indicators of compromise;
- Relevant IP addresses and their timestamps;
- Device Identifiers;
- Methodologies Used; and
- Other information the institution believes is relevant.

Collaboration and ongoing communication among BSA/AML, cybersecurity, and other units will help financial institutions conduct a more comprehensive threat assessment and develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime. Financial institutions can work together to identify threats, vulnerabilities, and criminals. Under Section 314(b) financial institutions may share information, including cyber-related information, regarding individuals, entities, and organizations, and countries for the purposes of identifying and reporting money laundering and terrorist activities.

- L. Advisory Regarding Disaster-Related Fraud – FinCEN Advisory 2017-A007 – October 31, 2017** – FinCEN has issued this Advisory to warn financial institutions about the potential for fraudulent transactions in the wake of disasters, including recent hurricanes and wild fires. This advisory is not intended to deter legitimate donations and relief assistance efforts. Rather the purpose is to help financial institutions identify and prevent fraudulent activity that may interfere with legitimate relief efforts. Three potential fraud areas were covered in this Advisory:
1. Benefits Fraud – where individuals apply for emergency assistance benefits to which they are not entitled.
 2. Charities Fraud – where criminals seek to exploit the charities established to accept donations to assist hurricane victims.

3. Cyber-Related Fraud – where cyber actors take advantage of public interest during natural disasters in order to conduct financial fraud and disseminate malware. Financial institutions may want to be aware of public reporting on hurricane-related or wild fire phishing campaigns, malicious websites, and associated malware.
 - a. When filing a SAR to report disaster-related fraud, FinCEN requests, but does not require, that financial institutions reference this advisory, and include the term “Disaster-Related Fraud” in the narrative, and in SAR field 31(z) (Fraud-Other) to indicate a connection between the suspicious activity being reported and possible misuse of relief funds.

M. Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators – FinCEN Advisory 2018-A003 – June 12, 2018 – FinCEN issued this Advisory to U.S. financial institutions to highlight the connection between corrupt senior foreign political figures and their enabling of human rights abuses. The Advisory describes a number of typologies used by them to access the U.S. financial system, obscure, and further their illicit activity. The Advisory also provides red flags that may assist financial institutions in identifying the methods used by corrupt senior foreign political figures, including the use of facilitators, to move and hide the proceeds of their corruption, which contribute directly or indirectly to human rights abuses or other illicit activity, through the U. S. financial system.

N. Advisory to Financial Institutions on the Risk of Proceeds of Corruption from Nicaragua – FinCEN Advisory 2018-A005 – October 04, 2018 – FinCEN issued this advisory to alert financial institutions of the increasing risk that proceeds of political corruption from Nicaragua may enter or traverse the U.S. financial system. In particular, FinCEN expects that senior foreign political figures connected with the regime of Nicaraguan President Daniel Ortega could react to the perceived threat of further unrest, potential sanctions, or other factors by moving assets that are the proceeds of corruption out of their accounts in Nicaragua or elsewhere.

O. Advisory on the Iranian Regime’s Illicit and Malign Activities and Attempts to Exploit the Financial System – FinCEN Advisory 2018-A006 – October 11, 2018 – FinCEN issued this Advisory to help U.S. financial institutions better detect potentially illicit transactions related to the Islamic Republic of Iran. The Iranian regime has long used front and shell companies to exploit financial systems around the world to generate revenues and transfer funds in support of malign conduct, which includes support to terrorist groups, ballistic missile development, human rights abuses, support to the Syrian regime, and other destabilizing actions targeted by U.S. sanctions.

This Advisory highlights the Iranian regime’s exploitation of financial institutions worldwide, and describes a number of typologies used by the regime to illicitly access the international financial system and obscure and further its malign activity. It also provides red flags that may assist financial institutions in identifying these methods. Additionally, the Advisory is intended to assist financial institutions in light of the United States’ withdrawal from the Joint Comprehensive Plan of Action (JCPOA) and the re-imposition of U.S. sanctions previously lifted under the JCPOA.

P. Updated Advisory on Widespread Public Corruption in Venezuela – FinCEN Advisory FIN-2019-A002 – May 03, 2019 – FinCEN issued this update to the 09/20/2017 Advisory covering widespread public corruption in Venezuela to alert financial institutions of continuing widespread public corruption in Venezuela under the regime of Nicolas Maduro, which the U.S. Government considers illegitimate. It also alerts financial institutions to additional methods utilized by corrupt Venezuelan senior political figures to move and hid corruption proceeds – money stolen from the Venezuelan people – and contribute to the dire humanitarian situation in Venezuela, which includes among other things, starvation, human rights violations, lack of medicine or medical care, and children and the elderly being separated from their families because they cannot care for them.

Q. Advisory on Illicit Activity Involving Convertible Virtual Currency – FinCEN Advisory FIN-2019-A003 – May 09, 2019 – FinCEN issued this advisory to assist financial institutions in identifying and reporting suspicious activity concerning how criminals and other bad actors exploit convertible virtual currencies (CVCs) for money laundering, sanctions evasion, and other illicit financing purposes, particularly involving darknet marketplaces, peer-to-peer (P2P) exchangers, foreign-located Money Services Businesses (MSBs), and CVC kiosks. Virtual currencies, particularly CVCs, are increasingly used as alternatives to traditional payment and money transmission systems. This Advisory highlights prominent typologies and red flags associated with such activity and identifies information that would be most valuable to law enforcement, regulators, and other national security agencies in the filing of SARs. In filing SARs in response to the information contained within this Advisory, financial institutions should list “**CVC FIN-2019-A003**” in Field 2, and in the SAR Narrative (Part V), to indicate a connection between the suspicious activity being reported and possible illicit activity involving CVC.

On the same date, FinCEN issued **FinCEN Guidance FIN-2019-G001**, interpretive guidance to remind persons subject to BSA how FinCEN regulations relating to money services businesses (MSBs) apply to certain business models involving money transmission denominated in value that substitutes for currency, specifically, convertible virtual currencies (CVCs). This guidance did not establish any new regulatory expectations or requirements. Rather it consolidated current FinCEN regulations and related administrative rulings and guidance issued since 2011, and then applies them to other common business models involving CVC engaging in the same underlying patterns of activity.

R. Advisory on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids – FinCEN Advisory FIN-2019-A006 – August 21, 2019 – FinCEN issued this Advisory to alert financial institutions to illicit financial schemes and mechanisms related to the trafficking of fentanyl, fentanyl analogues, and other synthetic opioids, and to assist them in detecting and reporting related activity. The Advisory highlights the primary typologies and red flags derived from sensitive financial reporting which are associated with (i) the sale of these drugs by Chinese, Mexican, or other foreign suppliers; (ii) methods used by Mexican and other TCOs to launder the proceeds of fentanyl trafficking; and (iii) financial methodologies associated with the sale and procurement of fentanyl over the Internet by purchasers located in the United States. Fentanyl can be purchased alone; mixed with heroin, cocaine, or methamphetamine; or pressed into pill form and falsely sold as prescription opioids, many times being ingested by unsuspecting victims. Fentanyl trafficking in the United States generally follows one of two pathways: direct purchase of

fentanyl from China by U.S. individuals for personal consumption or domestic distribution; or cross-border trafficking of fentanyl from Mexico by TCOs and smaller criminal networks. In filing SARs in response to the information contained within this Advisory, financial institutions should list **“FENTANYL FIN-2019-A006”** in Field 2, and in the SAR Narrative (Part V), to indicate a possible connection between the suspicious activities being reported and activities highlighted in this Advisory.

- S. Joint Statement on Providing Financial Services to Customers Engaged in Hemp-Related Businesses – December 03, 2019** – FinCEN, along with the Conference of State Bank Supervisors (CSBS) the FRB, the OCC, and the FDIC issued this joint statement to provide clarity regarding the legal status of commercial growth and production of hemp and relevant requirements for banks under the BSA. Because hemp is no longer a Schedule I controlled substance under the Controlled Substances Act, banks are not required to file a SAR on customers solely because they are engaged in the growth or cultivation of hemp in accordance with applicable laws and regulations. Bank customers engaged in hemp-related business activities are responsible for complying with the requirements set forth in the 2018 Farm Bill and applicable regulations. When deciding to serve hemp-related businesses, banks must comply with applicable regulatory requirements for CIP, SAR reporting, CTR reporting, and risk-based CDD, including the collection of beneficial ownership information for legal entity customers. For hemp-related customers, banks are expected to follow standard SAR procedures, and file a SAR if indicia of suspicious activity warrants.

On June 29, 2020, FinCEN released Guidance FIN-2020-G001 explaining how financial institutions can conduct due diligence for hemp-related businesses and identifies the type of information and documentation financial institutions can collect from hemp-related businesses to comply with BSA requirements. The guidance provides risk considerations only for businesses or individuals that grow hemp, and processors and manufacturers who purchase hemp directly from such growers. (This guidance does not replace or supersede FinCEN’s 2014 Marijuana Guidance).

- T. Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)** – FinCEN Advisory 2020-A002 – May 18, 2020 – FinCEN issued this Advisory to alert financial institutions to rising medical scams related to the Covid-19 pandemic. The Advisory contains descriptions of Covid-19 related medical scams, red flags, and information on reporting suspicious activity. Possible illicit activities related to the Covid-19 pandemic include (1) fraudulent cures, tests, vaccines, and services; (2) non-delivery scams; and (3) price gouging and hoarding of medical-related items, such as face masks and hand sanitizer. In filing a SAR in response to this Advisory, institutions should select 34(z) Fraud – Other and then indicate the type of fraud or scam (E.g. Product Fraud – non-delivery scam). Institutions should also reference this Advisory in field 2 on the cover sheet, and in the narrative as well.

On the same date, FinCEN also published a Notice Related to the Coronavirus Disease 2019 (COVID-19) which contains pertinent information regarding reporting Covid-19 related criminal and suspicious activity while reminding financial institutions of certain BSA advisories.

- U. Advisory on Imposter Scams and Money Mule Schemes Related to COVID-19 – FinCEN Advisory FIN – 2020 – A003 – July 07, 2020** – FinCEN issued this advisory to alert financial institutions to potential indicators of

imposter scams and money mule schemes, which are two forms of consumer fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of imposter scams and money mule schemes, financial red flag indicators for both, and information on reporting suspicious activity. In imposter scams, criminals impersonate organizations such as government agencies, non-profit groups, universities, or charities to offer fraudulent services or otherwise defraud victims. A money mule is “a person who transfers illegally acquired money on behalf of or at the direction of another”. Money mule schemes span the spectrum of using unwitting, witting, or complicit money mules.

- V. Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the COVID-19 Pandemic – FinCEN Advisory FIN – 2020 – A005 – July 31, 2020** – FinCEN issued this advisory to alert financial institutions to potential indicators of cybercrime and cyber-enabled crime observed during the COVID-19 pandemic. This advisory contains descriptions of COVID-19 related malicious cyber activity and scams, associated financial red-flag indicators, and information on reporting suspicious activity. Cybercriminals and malicious state actors are targeting vulnerabilities in remote applications and virtual environments to steal sensitive information, compromise financial activity, and disrupt business operations. Remote identity processes also face significant risks, which may include: digital manipulation of identity documentation where criminals seek to undermine online identity verification through the use of fraudulent identity documents created by manipulating digital images of legitimate government issued identity documents; and leveraging compromised credentials across accounts where the cybercriminals commonly undermine weak authentication processes in attempted account takeovers via methods such as account stuffing attacks (using lists of stolen account credentials to conduct automated login attempts to gain unauthorized access to victim accounts).
- W. Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments – FinCEN Advisory FIN – 2020 – A006 – October 01, 2020** – FinCEN issued this Advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. The Advisory provides information on: (1) the role of financial intermediaries in the processing of ransomware payments; (2) trends and typologies of ransomware and associated payments; (3) ransomware-related financial red-flag indicators; and (4) reporting and sharing information related to ransomware attacks. Ransomware is a form of malicious software designed to block access to a computer system or data, often by encrypting data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims’ access to their systems or data. In some cases, in addition to the attack, the perpetrators threaten to publish sensitive files belonging to the victims.

- X. Advisory on Unemployment Insurance Fraud During the Coronavirus Disease (COVID-19) Pandemic – FinCEN Advisory FIN- 2020 – A – 007 – October 13, 2020** – FinCEN issued this Advisory to alert financial institutions to unemployment insurance (UI) fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. The Advisory contains descriptions of COVID-19-related UI fraud, associated red flag indicators, and information on reporting suspicious activity. The representative types of illicit UI activity referenced include: Fictitious employer-employee fraud; employer-employee collusion fraud; misrepresentation of income fraud; insider fraud; and identity-related fraud. The Advisory identified financial “red-flag” indicators to alert financial institutions to fraud schemes targeting UI programs, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such fraud.
- Y. Notice on Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks – FinCEN Notice FIN-2020-NTC4 – December 28, 2020** – FinCEN issued this Notice to alert financial institutions about the potential for fraud, ransomware attacks, or similar types of criminal activity related to COVID-19 vaccines and their distribution. COVID-19 vaccine fraud may include the sale of unapproved and illegally marketed vaccines, the sale of counterfeit versions of approved vaccines, and illegal diversion of legitimate vaccines. Already, fraudsters have offered, for a fee, to provide potential victims with the vaccine sooner than permitted under the applicable vaccine distribution plan. When filing the SAR, institutions should reference “FIN-2020-NTC4” in field 2, and then select field 34(z) (Fraud-Other) and insert vaccine scam or vaccine ransomware. Filers should also detail the reported activity in the narrative section of the SAR.
- Z. Advisory on COVID-19 Health Insurance-and Health Care-Related Fraud – FinCEN Advisory FIN – 2021 – A001 – February 2, 2021** – FinCEN issued this advisory to alert financial institutions to health insurance and health care frauds related to the COVID-19 pandemic. These frauds target Medicare, Medicaid/Children’s Health Insurance Program (CHIP), and TRICARE, as well as health care programs provided through Department of Labor and Veterans Affairs and private health insurance companies. In addition, the United States government has observed frauds in connection with COVID-19 relief funds for health care providers, such as those provided under the Paycheck Protection Program and Health Care Enhancement Act (PPP-HCEA). This Advisory contains descriptions of COVID-19 related fraud involving health care benefit programs and health insurance, associated financial red flag indicators, select case studies, and information on reporting suspicious activity.
- AA. Advisory on Financial Crimes Targeting COVID-19 Economic Impact Payments – FinCEN Advisory FIN – 2021 – A002 – February 24, 2021** – FinCEN issued this Advisory to alert financial institutions to fraud and other financial crimes related to the Economic Impact Payments (EIPs) authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act, and the Coronavirus Response and Relief Supplemental Appropriations Act of 2021. U. S. Authorities have detected a wide range of EIP-related fraud and theft involving a variety of criminal actors. The advisory contains descriptions of EIP fraud, associated red flag indicators, and information on reporting suspicious activity.

When filing a SAR, FinCEN requests that financial institutions reference this advisory by including the key term “FIN-2021-A002” in SAR field 2 and in the narrative portion of the SAR, mentioning the term economic impact payment in the narrative as well. Financial institutions should also select SAR field 34(z)

(Fraud-other) and include the type of fraud and/or name of the scam or product (e.g. economic impact payment) in SAR field 34(z). Filers should not report the potential victim of an EIP fraud scheme as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

BB. Consolidated COVID-19 Suspicious Activity Report Key Terms and Filing Instructions – FinCEN Notice – FIN – 2021 – NTC1 – February 24, 2021 –

FinCEN issued this Notice to consolidate filing instructions and key terms for fraudulent activities, crimes, and cyber and ransomware attacks related to COVID-19 , and to remind institutions of recent updates to FinCEN guidance concerning Section 314(b). FinCEN has published a series of advisories and notices on COVID-19 related threats to assist financial institutions with the filing of SARs involving such threats. Three tables are included in the Notice: Table 1 contains key terms and instructions related to government programs; Table 2 contains a summary of the key terms and instructions for COVID-19-related activities that are not tied to a specific government program; and Table 3 provides a list of additional FinCEN’s COVID-19-related publications. Financial institutions should consult previously published advisories and notices for additional SAR filing instructions related to the COVID-19 advisories and notices.

CC. FinCEN Informs Financial Institutions of Efforts Related to Trade in Antiquities and Art – FinCEN Notice – FIN – 2021 – NTC2 – March 09, 2021 –

FinCEN issued this Notice to inform financial institutions about the (1) the Anti Money Laundering Act efforts related to trade in antiquities and art; (2) select sources of information about existing illicit activity related to antiquities and art, and (3) provide specific instructions for filing SARs related to trade in antiquities and art. Section 6110(a) of the AML Act amends the definition of “financial institution” under the BSA to include persons “engaged in the trade of antiquities”. The BSA obligations imposed by Section 6110(a) will take effect on the effective date of the final regulations. Financial institutions should be aware that illicit activity associated with the trade in antiquities and art may involve their institutions. Crimes relating to antiquities and art may include looting or theft, the illicit excavation of archaeological items, smuggling, and the sale of stolen or counterfeit objects. Crimes relating to antiquities and art also may include money laundering and sanctions violations, and have been linked to transnational criminal networks, international terrorism, and the persecution of individuals or groups on cultural grounds. When filing a SAR, FinCEN requests that financial institutions reference “FIN-2021-NTC2” in SAR field 2 and in the narrative portion on the SAR. Institutions should also select field 36z (Money Laundering – Other) and in insert “Antiquities”, “Art”, or both (as in some instances, an object could be considered both an antiquity and a work of art).

VII. INTERNAL PROCEDURES – Taking organizational action is critical since SARs must be filed within specific time frames. Internal procedures should be established for identifying, investigating, and determining whether to report suspicious activity.

A. Communication System – The bank should set up an internal system for communicating to the proper personnel that suspicious activity or transactions have been detected. Channels for reporting suspected activity or transactions can include phone calls, memos, or internally developed forms.

B. Central Office(r) – The bank should designate a centralized employee, officer, or department to serve as a clearinghouse for branch or line personnel to report suspicious transactions. This Central Office(r)'s duties should include:

1. Reviewing internal reports and determining if additional investigation is necessary.
2. Conducting any necessary investigation.
3. Informing senior management if a SAR filing is warranted.
4. Ensuring that the investigation documents and evidence supporting any SAR filing are obtained and maintained for five years.

NOTE: Proper documentation of the investigation is especially critical if the decision not to file a SAR is made. This establishes that the bank acted in good faith and is not guilty of “willful blindness” regarding the suspect activity.

5. Serving as the contact point when regulatory agencies or FinCEN requests additional information.

C. Auditing the Suspicious Activity Reporting Program - Tips for developing and administering an audit program to review and independently test compliance with SAR requirements can be found in the *SAR Activity Review* #6 November 2003, and in the *SAR Activity Review* #16 October 2009.

VIII. EXAM PROCEDURES - Contained within the current Interagency BSA/AML Examination Manual are the core examination procedures covering an institution's SAR program. Highly qualitative and subjective in nature, the Federal examiner will evaluate the program to determine whether it is appropriate for the institution. The examiner will also determine whether the suspicious activity monitoring systems and reporting processes are adequate and effectively implemented by considering a number of factors including, but not limited to:

Identification of Unusual Activity

1. Lines of communication for the referral of unusual activity to appropriate personnel;
2. Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities;
3. Monitoring systems used to identify unusual activity;
4. Procedures for reviewing and evaluating the transaction activity of subjects included in law enforcement requests for suspicious activity. The examiner is instructed to evaluate policies, procedures, and processes for:
 - a. Responding to National Security Letters (NSLs);
 - b. Evaluating the account of the target for suspicious activity;
 - c. Filing SARs, if necessary; and

- d. Handling account closures.

SAR Decision Making

5. Manual transaction monitoring reports – Do they capture all areas that pose money laundering and terrorist financing risks? Do the manual transaction monitoring systems use reasonable filtering criteria that has been independently verified, and that generate accurate reports at a reasonable frequency?
6. Automated Account monitoring surveillance – Identify the system methodology and filtering criteria utilized, ask the “reasonable” question, determine if independently validated, and ensure that access to the system is limited and there is sufficient oversight of assumption changes.

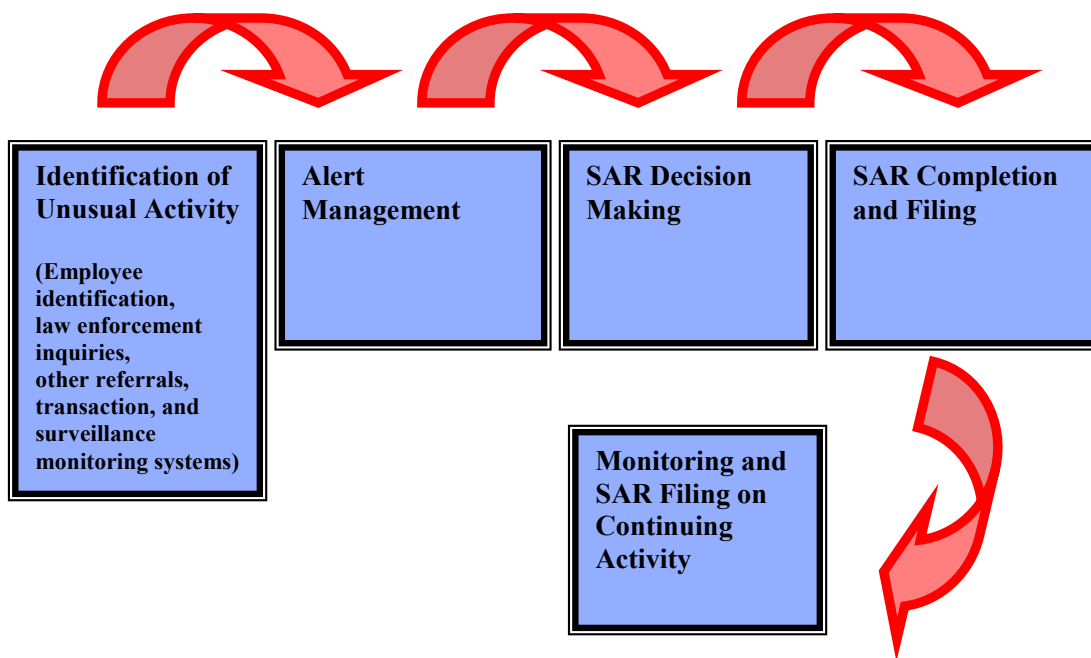
Managing Alerts

7. Policies, procedures, and processes to ensure timely generation of, and review of, and response to reports used to identify unusual activity. Determine if such procedures require appropriate research when suspicious activity is identified.
8. Policies, procedures, and processes for referring suspicious activity from all business lines to the personnel or department responsible for evaluating the unusual activity. (Criminal subpoenas, NSLs, 314(a) requests should be effectively evaluated).
9. Staffing levels are sufficient to review reports and alerts and investigate items, and the staff possess the requisite experience level and proper investigatory tools. (The volume of alerts and investigations should NOT be tailored solely to meet existing staffing levels).
10. SAR decision process should consider all available CDD and EDD information.
11. Procedures for documenting decision not to file a SAR - are such decisions supported and reasonable?
12. Procedures for escalating issues identified as the result of repeat SAR filings on accounts.
13. Procedures for considering closing accounts as a result of continuous suspicious activity;

SAR Completion and Filing

14. Procedures for completing, filing, and retaining SARs and their supporting documentation; Procedures for reporting SARs to the board of directors, or a committee thereof, and senior management; Procedures for sharing SARs with head offices and controlling companies;
15. Transactional testing of the SAR monitoring systems and reporting processes; Financial institutions may obtain copies of the exam procedures from www.ffiec.gov/bsa_aml_infobase/.

Appendix S: Key Suspicious Activity Monitoring Components



The narrative section of the report is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators. Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion. This description should encompass the data provided in Parts I through III, but should include any other information necessary to explain the nature and circumstances of the suspicious activity. Filers should provide any information the filers believe necessary to better enable investigators to understand the reported suspicious activity. Narratives must be completed in English. Filers should use the following checklist as a guide for preparing the narrative:

- If filers have additional information pertaining to items in Parts I through IV this information should be recorded in the narrative and referenced to the item number.
- If this report is a corrected or amended report, complete the report in its entirety with whatever corrections or amendments were required. Describe the corrections or amendments at the beginning of the narrative.
- If this report is a continuing report, describe the circumstances surrounding the suspicious activity for the 90-day period encompassing the report. Include information from prior FinCEN SAR narratives only when it is necessary for an understanding of the nature and circumstances of the suspicious activity. Never include the entire narratives of the prior FinCEN SARs.
- If any item in the report was insufficient for recording all item data held by the filer, or if an item's instructions require entry of additional data or explanation in the narrative, record the additional data referenced by item number in the narrative.
- Information provided in other sections of the FinCEN SAR need not be repeated in the narrative unless necessary to provide a clear and complete description of the suspicious activity.
- Describe the conduct or transaction(s) that caused suspicion. If appropriate, this description should be chronological when the activity involves multiple instances or encompasses more than one day.
- Explain whether any transaction(s) involved were completed or only attempted.
- Explain who benefited and how they benefited, financially or otherwise, from the activity.
- Describe all supporting documentation and retain the documentation for five years. DO NOT include supporting documentation with the FinCEN SAR. (See General Instruction 6.)
- If the FinCEN SAR is jointly-filed, name all joint filers and describe the nature of supporting document held by the joint filers. Provide the contact office name and telephone number for each joint filer.
- Describe and retain any evidence of cover-up or evidence of an attempt to deceive federal or state examiners or others
- Describe and retain any admission or explanation of the activity or transaction(s) provided by the subject(s), witness(s), or other person(s), including to whom and when it was given.
- Indicate where the suspicious activity took place, e.g. branch, cage, gaming pit, agent location, etc.
- Indicate whether the suspicious activity is an isolated incident or related to other activity.
- Indicate whether any U.S. or foreign currency or other negotiable instruments were involved. If foreign currency or other foreign instruments, provide the foreign amount, currency name, and country of origin.
- Indicate if there is any litigation related to the activity by specifying the name of the litigation and court where the action is pending.
- Describe the nature of losses and recoveries related to the suspicious activity, including aggregated losses and recoveries in continuing activity.
- Identify the names of financial institutions associated with account numbers when the financial institution TINs were unknown.
- If the subject is a foreign national provide all available information on the subject's passport(s), visa(s), and other identification. Include identifying data such as issuing date, country, document numbers, issuing authority, and nationality.
- If the suspicious activity involves transfers of funds to or from a foreign country or currency exchanges involving foreign currencies, identify the foreign currency, country of issue, and the source or destination of the funds.
- If a subject involved in the suspicious activity has an insider relationship with a financial institution, describe the subject's position with the financial institution and how that position related to the suspicious activity.
- Provide information on the victims of the suspicious activity only when it is necessary for a complete understanding of the activity. DO NOT record victim information in a Part I Subject Information record.
- Provide information about the financial institution's business policies and practices only if it is necessary for a complete understanding of the suspicious activity. DO NOT include legal disclaimers in the narrative.
- Do not include tabular data in a FinCEN SAR narrative. Such data should be reported in an appropriate comma separated values attachment.

If this SAR contains information provided by another financial institution under the 314(b) Voluntary Information Sharing Program, include in the narrative the statement "This SAR contains 314(b) data." Filers can include with a FinCEN SAR an attachment containing tabular data (such as transaction data) that provides additional suspicious activity information not suitable for inclusion in the narrative. This file must be an MS Excel-compatible comma separated value (CSV) file with a maximum size of 1 megabyte. Discrete FinCEN SAR filers can attach this file by clicking the "Add Attachment" button on the discrete FinCEN SAR header page and following the instructions provided. Batch filers must follow the instructions in Attachment D – Batch Attachments to add CSV files to a batch file.

- (continuing activity report) is checked
- * (32–42: *specific type of suspicious activity*) When completing items 32 through 42, check all that apply.
32. Structuring
- Alters or cancels transaction to avoid BSA recordkeeping requirement
 - Alters or cancels transaction to avoid CTR requirement
 - Transaction(s) below BSA recordkeeping threshold
 - Transaction(s) below CTR threshold
 - Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements
 - Other (*specify type of suspicious activity in space provided*)
33. Terrorist Financing
- Known or suspected terrorist/terrorist organization
 - Other (*specify type of suspicious activity in space provided*)
34. Fraud
- ACH
 - Advance Fee
 - Check
 - Consumer loan (see instructions)
 - Credit/Debit card
 - Healthcare
 - Mail
 - Ponzi Scheme
 - Pyramid scheme
 - Securities Fraud
 - Wire
 - Other (*specify type of suspicious activity in space provided*)
35. Gaming Activities
- Chip walking
 - Minimal gaming with large transactions
 - Suspicious use of counter checks or markers
 - Unknown source of chips
 - Other (*specify type of suspicious activity in space provided*)
36. Money laundering
- Exchanges small bills for large bills or vice versa
 - Funnel account
 - Suspicion concerning the physical condition of funds
 - Suspicion concerning the source of funds
 - Suspicious designation of beneficiaries, assignees or joint owners
 - Suspicious EFT/Wire transfers
 - Suspicious exchange of currencies
 - Suspicious receipt of government payments/benefits
 - Suspicious use of multiple accounts
 - Suspicious use of noncash monetary instruments
 - Suspicious use of third-party transactors (straw-man)
 - Trade Based Money Laundering/Black Market Peso Exchange
 - Transaction out of pattern for customer(s)
 - Other (*specify type of suspicious activity in space provided*)
37. Identification/Documentation
- Changes spelling or arrangement of name
 - Multiple individuals with same or similar identities
 - Provided questionable or false documentation
 - Provided questionable or false identification
 - Refused or avoided request for documentation
 - Single individual with multiple identities
 - Other (*specify type of suspicious activity in space provided*)
38. Other suspicious activities
- Account takeover
 - Bribery or gratuity
 - Counterfeit instruments
 - Elder financial exploitation
 - Embezzlement/theft/disappearance of funds
 - Forgeries
 - Human Trafficking/Smuggling
 - Identity theft
 - Little or no concern for product performance penalties, fees, or tax consequences
 - Misuse of position or self-dealing
 - Suspected public/private corruption (domestic)
 - Suspected public/private corruption (foreign)
 - Suspicious use of informal value transfer system
 - Suspicious use of multiple transaction locations
 - Transaction with no apparent economic, business, or lawful purpose
 - Transaction(s) involving Foreign high risk jurisdiction
 - Two or more individuals working together
 - Unlicensed or unregistered MSB
 - Other (*specify type of suspicious activity in space provided*)
39. Insurance
- Excessive insurance
 - Excessive or unusual cash borrowing against policy/annuity
 - Proceeds sent to or received from unrelated third party
 - Suspicious life settlement sales insurance (e.g. STOLI's, Viaticals)
 - Suspicious termination of policy or contract
 - Unclear or no insurable interest
 - Other (*specify type of suspicious activity in space provided*)
40. Securities/Futures/Options
- Insider trading
 - Market manipulation
 - Misappropriation
 - Unauthorized pooling
 - Wash Trading
 - Other (*specify type of suspicious activity in space provided*)
41. Mortgage fraud
- Application fraud
 - Appraisal fraud
 - Foreclosure/Shortsale fraud
 - Loan modification fraud
 - Origination fraud
 - Other (*specify type of suspicious activity in space provided*)
42. Cyber Event
- Against Financial Institution(s)
 - Against Financial Institution Customer(s)
 - Other (*specify type of suspicious activity in space provided*)
43. Were any of the following product type(s) involved in the suspicious activity? Check all that apply:
- Bonds/Notes
 - Commercial mortgage
 - Commercial paper
 - Credit card
 - Debit card
 - Forex transactions
 - Futures/Options on futures
 - Hedge fund
 - Home equity loan
 - Home equity line of credit
 - Insurance/Annuity products
 - Mutual fund
 - Options on securities
 - Microcap securities
 - Prepaid access
 - Residential mortgage
 - Security futures products
 - Stocks
 - Swap, hybrid or other derivative
 - Other (*specify type in space provided*)
44. Were any of the following instrument type(s)/payment mechanism(s) involved in the suspicious activity? Check all that apply:
- Bank/cashier's check
 - Foreign currency
 - Funds transfer
 - Gaming instruments
 - Government payment
 - Money orders
 - Personal/Business check
 - Travelers checks
 - U.S. Currency
 - Other (*specify type in space provided*)
45. Commodity type (if applicable) (*multiple entries allowed*)
46. Product/Instrument description (if needed) (*multiple entries allowed*)
47. Market where traded (*list of codes will be provided—dropdown menu for electronic filers*) (*multiple entries allowed*)
48. IP Address (if available) (*multiple entries allowed*)
- 48a. Date (YYYYMMDD)
- 48b. Time Stamp(UTC) HH:MM:SS
49. Cyber-Event Indicators (*multiple entries up to 99*)
- 49a. Command and Control IP address
- 49a1 Event value text field (each entry of 49a must have a corresponding event value text field).
- 49a2 Event value text field (Date associated with the value in 49a1).
- 49a3 Event value text field (Timestamp associated with the value in 49a1).
- 49b. Command & Control URL/Domain
- 49b1 Event value text field (each entry of 49b must have a corresponding event value text field).
- 49c. Malware MD5, Malware SHA–1, or Malware SHA–256.
- 49c1 Event value text field (each entry of 49c must have a corresponding event value text field).
- 49d. Media Access control (MAC) Address
- 49d1 Event value text field (each entry of 49d must have a corresponding event value text field).
- 49e. Port
- 49e1 Event value text field (each entry of 49e must have a corresponding event value text field).
- 49f. Suspicious Email Address
- 49f1 Event value text field (each entry of 49f must have a corresponding event value text field).

- 49g. Suspicious Filename
 49g1 Event value text field (each entry of 49g must have a corresponding event value text field).
 49h. Suspicious IP Address
 49h1 Event value text field (each entry of 49h must have a corresponding event value text field).
 49h2 Event value Date associated with the value in 49h1.
 49h3 Event value Timestamp associated with the value in 49h1.
 49i. Suspicious URL/Domain
 49i1 Event value text field (each entry of 49i must have a corresponding event value text field).
 49j. Targeted System
 49j1 Event value text field (each entry of 49j must have a corresponding event value text field).
 49z. Other
 49z Text description of Other value
 49z1 Event value text field (each entry of 49z must have a corresponding event value text field).
 50. CUSIP number (*multiple entries allowed*)

Part III Information About Financial Institution Where Activity Occurred

- * 51. Type of financial institution (check only one)
 a. Casino/Card club
 b. Depository institution
 c. Insurance company
 d. MSB
 e. Securities/Futures
 z. Other (*specify type of institution in space provided*)
 * 52. Primary Federal Regulator (*instructions specify banking agencies, SEC, CFTC, IRS*)
 CFTC
 Federal Reserve
 FDIC
 IRS
 NCUA
 OCC
 SEC
 Not Applicable
 53. If item 51a is checked, indicate type of gaming institution (check only one)
 a. State licensed casino
 b. Tribal authorized casino
 c. Card club
 z. Other (*specify type of gaming institution in space provided*)
 54. If item 51e is checked, indicate type of Securities and Futures institution or individual where activity occurred—check box(es) for functions that apply to this report
 a. Clearing broker—securities
 b. Futures commission merchant
 c. Holding company
 d. Introducing broker—commodities
 e. Introducing broker—securities
 f. Investment adviser
 g. Investment company
 h. Retail foreign exchange dealer
 i. Subsidiary of financial/bank holding company
 z. Other (*specify type of institution or individual in space provided*)
 55. Filing institution identification number (Check one box to indicate type)
 a. Central Registration Depository (CRD) number

- b. Investment Adviser Registration Depository (IARD) number
 c. National Futures Association (NFA) number
 d. Research, Statistics, Supervision, and Discount (RSSD) number
 e. Securities and Exchange Commission (SEC) number
 f. Identification number
 56. Financial institution's role in transaction (if applicable)
 a. (*check if*) Selling location
 b. (*check if*) Paying location
 c. (*check if*) Both a & b
 * 57. Legal name of financial institution
 a. (*check if*) unknown
 58. Alternate name, e.g., AKA—individual or trade name, DBA—entity
 * 59. TIN (*enter number in space provided and check appropriate type below*)
 a. (*check if*) unknown
 60. TIN type (* if 59 is known)
 a. EIN
 b. SSN-ITIN
 c. Foreign
 * 61. Address
 a. (*check if*) unknown
 * 62. City
 a. (*check if*) unknown
 63. State
Note: FinCEN will derive State through third party data as enhanced data if not provided and Country is US, Mexico or Canada and ZIP/Postal Code is provided.
 * 64. ZIP/Postal Code
 a. (*check if*) unknown
Note: FinCEN will derive ZIP + 4 through third party data as enhanced data if not provided or verified through third party data if provided.
 New Data Element of County—FinCEN will derive through third party data as enhanced data.
 * 65. Country (*2 letter code—list provided*)
 a. (*check if*) unknown
 66. Internal control/file number
 67. Loss to financial institution (*if applicable*)
 68. Branch's role in transaction (if applicable)
 a. (*check if*) Selling location
 b. (*check if*) Paying location
 c. (*check if*) Both a & b
 * 69. Address of branch or office where activity occurred
 a. (if no branch activity involved, check box a)
 70. Research, Statistics, Supervision, and Discount (RSSD) number (*of the Branch*)
 71. City
 72. State
Note: FinCEN will derive State through third party data as enhanced data if not provided and Country is US, Mexico or Canada and ZIP/Postal Code is provided.
 73. ZIP/Postal Code
Note: FinCEN will derive ZIP + 4 through third party data as enhanced data if not provided or verified through third party data if provided.
 New Data Element of County—FinCEN will derive through third party data as enhanced data.
 New Data Elements for GEO Coding—FinCEN will derive through third party data

as enhanced data will be identified for the financial institution and any branches provided.

New Data Element of HIFCA code—FinCEN will derive through third party data as enhanced data will be identified for the financial institution and any branches provided.

New Data Element of HIDTA code—FinCEN will derive through third party data as enhanced data will be identified for the financial institution and any branches provided.

74. Country (*2 letter code—list provided*) (*multiple entries allowed for items 68–74:*)

Part III Information about Financial Institution Where Activity Occurred can be repeated up to a total of 99 financial institutions.

Part IV Filing Institution Contact Information

- * 75. Primary Federal Regulator (*instructions specify banking agencies, SEC, CFTC, IRS*)
 CFTC
 Federal Reserve
 FDIC
 IRS
 NCUA
 OCC
 SEC
 Not Applicable
 * 76. Filer name (Holding company, lead financial institution, or agency, if applicable).
 * 77. TIN (*enter number in space provided and check appropriate type below*)
 * 78. TIN type
 a. EIN
 b. SSN/ITIN
 c. Foreign
 * 79. Type of financial institution (check only one)
 a. Casino/Card club
 b. Depository institution
 c. Insurance company
 d. MSB
 e. Securities/Futures
 z. Other (*specify type of institution in space provided*)
 80. Type of Securities and Futures institution or individual filing this report—check box(es) for functions that apply to this report
 a. Clearing broker—securities
 b. CPO/CTA
 c. Futures commission merchant
 d. Holding company
 e. Introducing broker—commodities
 f. Introducing broker—securities
 g. Investment adviser
 h. Investment company
 i. Retail foreign exchange dealer
 j. SRO Futures
 k. SRO Securities
 l. Subsidiary of financial/bank holding company
 z. Other (*specify type of institution or individual in space provided*)
 81. Filing institution identification number (Check one box to indicate type)
 a. Central Registration Depository (CRD) number
 b. Investment Adviser Registration Depository (IARD) number

is providing the examples below. Please note that these examples highlight instances where an institution may be limited in its ability to identify cyber-related information due to limits in cyber expertise or resource availability. Each example is an acceptable and appropriate use of these fields.

Example 1.

Bank A is told by its customer, ABC Corp, that a recent wire payment issued from its account was fraudulent. Bank A is told that fraudsters imitated the CEO of ABC Corp.'s e-mail to instruct ABC employees to wire funds from ABC's accounts at Bank A to an account at Bank B. ABC Corp tells Bank A that these fraudulent e-mails were made to look like the CEO used the e-mail address CEO@ABCcorp.co instead of the legitimate CEO@ABCcorp.com. These fraudulent e-mails appeared to be instructing employees to issue urgent payments to one of ABC's suppliers for \$300,000. Bank A recognizes this as a Business E-mail Compromise (BEC) scheme. In the FinCEN SAR narrative, Bank A describes the incident and mentions the term "BEC Fraud" and FinCEN advisory FIN-2016-A003.

Bank A places the following information in the new fixed fields on the FinCEN SAR form:

Item 42: Cyber Event

b. Against Financial Institution Customer(s) [check box]

Field 44f. Suspicious e-mail address

44f1. Event value: CEO@ABCcorp.com

Example 2.

Bank A is told by its customer, ABC Corp, that a recent wire payment issued from its account was fraudulent. Bank A is told by its customer that the CEO of ABC Corp.'s e-mail was hacked and used to instruct ABC employees to wire funds from ABC's accounts at Bank A to an account at Bank B. ABC Corp tells Bank A that these e-mails were made to look like the CEO was instructing employees to issue payments to ABC's suppliers for \$300,000. No additional technical information was provided to Bank A. Bank A recognizes this as a Business E-mail Compromise (BEC) scheme. In the FinCEN SAR narrative, Bank A describes the incident and mentions the term "BEC Fraud" and FinCEN advisory FIN-2016-A003.

Bank A places the following information in the new fixed fields on the FinCEN SAR form:

Item 42: Cyber Event

b. Against Financial Institution Customer(s) [check box]

Item 44: BLANK

Example 3.

Bank C identifies a cyber incident that targeted Bank C's own systems, resulting in access to Bank C's payment systems and an attempted transfer of \$1 million through Bank C's 123-wire system. Bank C's compliance team asks its IT department for additional technical information related to this incident, and whether there were any key indicators associated with the event. The IT department is still gathering information, but has identified one piece of relevant malware and the IP address that relayed instructions to attempt the \$1 million funds transfer. They also have a .csv file containing possibly related technical information that Bank C decides to include as an attachment.

Bank C files a FinCEN SAR with the following information in the new fixed fields:

Item 42: Cyber Event

a. Against Financial Institution [check box]

Field 44a. Command & Control IP Address

44a1. Event value: 127.0.0.1

44a2. Date (2017/01/01)

44a3. UTC Time (00:00:01)
 Field 44c. Malware MD5, Malware SHA-1, Malware SHA-256:
 44c1Event value: 9e107d9d372bb6826bd81d3542a419d6
 Field 44j. Targeted System:
 44j1. Event value: 123-wire

Example 4.

Bank D identifies an incident that targeted Bank D's own systems, resulting in access to Bank D's payment systems and an attempted transfer of \$50,000 through Bank D's 123-wire system. Bank D's compliance team asks its IT department for additional technical information related to this incident, and whether there were any key indicators associated with the event. Bank D's IT department confirms that the incident was a cyber event against Bank D, but is unable to spend resources locating additional information due to their necessary focus on continuity of business operations. Bank D files a FinCEN SAR based on the available information.

Bank D files a FinCEN SAR with the following information in the fixed fields:

Item 42: Cyber Event

a. Against Financial Institution [check box]

Field 44j. Targeted System:

44j1. Event Indicator value: 123-wire

Example 5.

Bank E is told by its customer that a fraudulent wire was sent from their online banking account. The customer does not know how fraudsters gained access to their account. Bank D is able to identify the record of the fraudulent wire and when it occurred. Bank D's compliance department asks its IT department for IP log information associated with the targeted customer's account at the time of the fraudulent wire transfer. The IT department is able to provide the information from their logs.

Bank E files a FinCEN SAR with the following information in the new fixed fields:

Item 43:

- a. IP address: 127.0.0.1
- b. Date: 2017-01-30
- c. UTC Time: 00:00:01

9.6.2. Item Instructions:

NOTE: Critical fields are identified with the * symbol in front of the data element number.

----- Type of Filing -----

*1. Type of filing (*check all that apply*)

- a. Initial report
- b. Correct/Amend prior report
- c. Continuing activity report
- d. Joint report
- e. Prior report BSA Identification Number if items 1b or 1c are checked

Item *1 Type of filing: Check box 1a "Initial report" if this is the first report filed on the suspicious activity. Check box 1b "Correct/Amend prior report" if the report corrects or amends a previously-filed FinCEN SAR. See General Instruction 3 for additional instructions on filing corrected or amended SARs. Check box 1c "Continuing activity report" if the FinCEN SAR continues reporting on previously-reported suspicious activity. If the FinCEN SAR corrects a previously-filed continuing activity report, both 1b and 1c must be checked. See General Instruction 4 for additional instructions on filing continuing activity reports. Check box 1d "Joint report" if a FinCEN SAR of any filing type is filed

Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations

January 19, 2021

The Financial Crimes Enforcement Network (FinCEN), jointly with the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) (collectively, the Federal banking agencies), and in consultation with the staff of certain other federal functional regulators, is issuing answers to frequently asked questions (FAQs) regarding suspicious activity reports (SARs) and other anti-money laundering (AML) considerations for financial institutions covered by SAR rules.¹ The answers to these FAQs clarify the regulatory requirements related to SARs to assist such financial institutions with their compliance obligations, while enabling financial institutions to focus resources on activities that produce the greatest value to law enforcement agencies and other government users of Bank Secrecy Act (BSA) reporting. The answers to these FAQs neither alter existing BSA/AML legal or regulatory requirements, nor establish new supervisory expectations; they were developed in response to recent Bank Secrecy Act Advisory Group (BSAAG) recommendations, as described in more detail in FinCEN's Advance Notice of Proposed Rulemaking (ANPRM) on Anti-Money Laundering Program Effectiveness, published in September 2020.²

Question 1: Requests by Law Enforcement for Financial Institutions to Maintain Accounts

Can a financial institution maintain an account or customer relationship for which it has received a written "keep open" request from law enforcement, even though the financial institution has identified suspicious or potentially illicit activity?³

-
1. Financial institutions subject to SAR requirements include: Banks (31 CFR § 1020.320), Casinos and Card Clubs (31 CFR § 1021.320), Money Services Businesses (31 CFR § 1022.320), Brokers or Dealers in Securities (31 CFR § 1023.320), Mutual Funds (31 CFR § 1024.320), Insurance Companies (31 CFR § 1025.320), Futures Commission Merchants and Introducing Brokers in Commodities (31 CFR § 1026.320), Loan or Finance Companies (31 CFR § 1029.320), and Housing Government Sponsored Enterprises (31 CFR § 1030.320).
 2. See <https://www.federalregister.gov/documents/2020/09/17/2020-20527/anti-money-laundering-program-effectiveness>.
 3. The response provided to this question clarifies current regulatory requirements. Under the recently-enacted Anti-Money Laundering Act of 2020, the Secretary of the Treasury is required to issue guidance on the required elements of a keep open request, which is forthcoming. See § 6306 of the Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, §§ 6001 – 6511 (enacted as Division F of the National Defense Authorization Act for Fiscal Year 2021).

Yes. Law enforcement may have an interest in ensuring that certain accounts and customer relationships remain open notwithstanding suspicious or potential criminal activity in connection with the account. A financial institution may decide to maintain an account based on a written “keep open” request from a law enforcement agency, however, it is not obligated to do so. The written request should be specific and indicate both that the law enforcement agency has requested that the financial institution maintain the account, as well as the purpose and duration of the request.⁴ Keeping such an account open as requested may be highly useful to law enforcement and may further efforts to identify and combat money laundering, terrorist financing, and other illicit financial activities.

A financial institution should not be criticized solely for its decision to maintain an account relationship at the request of law enforcement or for its decision to close the account. Ultimately, the decision to maintain or close an account should be made by a financial institution in accordance with its own policies, procedures, and processes. It may be useful for financial institutions to maintain documentation of “keep open” requests, including after a request has expired. If financial institutions keep such an account open as requested by law enforcement, they are still required to comply with all applicable BSA requirements, including requirements to conduct ongoing risk-based monitoring, and, as appropriate, file SARs,⁵ including continuing activity SARs consistent with FinCEN guidance.⁶

Question 2: Receipt of Grand Jury Subpoenas/Law Enforcement Inquiries and SAR Filing

Should a financial institution file a SAR solely on the basis of receiving a grand jury subpoena or other law enforcement inquiries?

No. The receipt of a law enforcement inquiry, such as a grand jury subpoena, does not by itself indicate that the criteria requiring the filing of a SAR have been met. However, receipt of a grand jury subpoena or other law enforcement inquiry is pertinent information relevant to a financial institution’s overall assessment of risk and the risk profile for the relevant customer(s) and account(s). Generally, a financial institution will assess and review all relevant information it has about a customer that is the subject of a grand jury subpoena or other law enforcement inquiries, in accordance with its risk-based AML program. For example, the receipt of a grand jury subpoena should cause a financial institution to review relevant account activity and transactions.⁷

-
4. A written request from a federal law enforcement agency should be issued by a supervisory agent or by an attorney within a United States Attorney’s Office or another office of the Department of Justice. If a state or local law enforcement agency requests that an account be maintained, then the financial institution should obtain a written request from a supervisor of the state or local law enforcement agency or from an attorney within a state or local prosecutor’s office. For additional guidance about the content of “keep open” requests, see “Requests by Law Enforcement for Financial Institutions to Maintain Accounts,” available at <https://www.fincen.gov/resources/statutes-regulations/guidance/requests-law-enforcement-financial-institutions-maintain>.
 5. See 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR Chapter X (FinCEN).
 6. See https://www.fincen.gov/sites/default/files/shared/sar_tti_21.pdf at p. 53.
 7. See https://www.fincen.gov/sites/default/files/shared/sar_tti_10.pdf at p. 43.

The financial institution should determine whether SAR filing is necessary based on its assessment of all information available and applicable regulatory requirements. If a financial institution files a SAR on a customer or transaction following the receipt of a grand jury subpoena or other law enforcement inquiry, the SAR should focus on the facts and circumstances that support a finding of suspicious activity rather than the subpoena or inquiry itself.⁸

Question 3: Maintaining a Customer Relationship Following the Filing of a SAR or Multiple SARs

Is a financial institution required to terminate a customer relationship following the filing of a SAR or multiple SARs?

No. There is no BSA regulatory requirement to terminate a customer relationship after the filing of a SAR or any number of SARs. The decision to maintain or close a customer relationship as a result of the identification of suspicious activity is a determination for a financial institution to make based on the information available to it, its assessment of money laundering or other illicit financial activity risks, and established policies, procedures, and processes.

Financial institutions have the flexibility to develop risk-based procedures and monitoring processes for the purpose of updating the customer risk profile and determining when to maintain or close accounts. Generally, financial institutions have policies, procedures, and processes in place that establish an escalation process for decisions to maintain or terminate customer relationships based on relevant factors, including SAR filing(s). These processes establish criteria, including when review by senior management and legal staff is warranted, for the decision to maintain or terminate the customer relationship in light of elevated risk factors. As indicated above, there is no specific number of SAR filings that a financial institution must consider to trigger any particular escalation step. Rather, the number of SAR filings and other factors that trigger escalation steps may vary based upon, among other things, the risk profile of the customer, including the geographical locations involved, the volume and type of transactions conducted by customers, the type of account, and the types of SARs filed by the financial institution in relation to the customer.⁹

Question 4: SAR Filing on Negative News Identified in Media Searches

Is a financial institution required to file a SAR based solely on negative news?

No. The existence of negative news related to a customer or other activity at a financial institution does not by itself indicate that the criteria requiring the filing of a SAR have been met, and does not automatically require the filing of a SAR by a financial institution. A financial institution may review media reports, news articles and/or other references to assist in its performance of customer due diligence, as well as its evaluation of any transactions or activity it

8. Financial institutions are reminded that grand jury proceedings and certain law enforcement inquiries may be subject to specific confidentiality provisions. For example, National Security Letters are subject to certain disclosure prohibitions. See, e.g., https://www.fincen.gov/sites/default/files/shared/sar_tti_08.pdf at p. 36.

9. As referenced in Question 1, there may be instances where law enforcement requests a financial institution to maintain an account relationship, notwithstanding potential suspicious activity, and the financial institution should continue filing SARs, or continuing activity SARs, as applicable.

considers unusual or potentially suspicious. For example, negative news may cause a financial institution to review customer activity as well as other related information, such as that of third parties with transactions involving the customer's account. As with other identified unusual or potentially suspicious activity, financial institutions should comply with applicable regulatory requirements and follow their established policies, procedures, and processes to determine the extent to which it investigates and evaluates negative news, in conjunction with its review of transactions occurring by, at, or through the institution, to determine if a SAR filing is required.

Question 5: SAR Monitoring on Multiple Negative Media Alerts

If there are multiple negative news alerts based on the same event, is a financial institution expected to independently investigate each of those alerts?

No. In circumstances where there are multiple negative news alerts (as identified through monitoring for unusual or suspicious activity) based on the same underlying events, a financial institution does not need to independently investigate each alert, but rather may consider whether the alert contains new or different information that warrants further investigation or whether the negative news otherwise assists or informs the evaluation of the activity at issue. Many financial institutions maintain a process for managing a high volume of alerts generated by news. This type of process will allow the financial institution to identify and evaluate new information and assess whether to update customer information and risk profile, investigate transactions which may result in the filing of a SAR, or escalate or terminate a customer relationship, as appropriate consistent with its policies, procedures, and processes. Financial institutions have flexibility in developing risk-based procedures and monitoring processes for the purpose of complying with customer due diligence requirements and, where appropriate, consideration of negative news.¹⁰

Question 6: Information in Data Fields and Narrative

Do financial institutions need to repeat information in the SAR narrative that has already been included in other SAR data fields?

No. As stated in the SAR instructions, information provided in other sections of a SAR does not need to be repeated in the narrative unless necessary to provide a clear and complete description of the suspicious activity.¹¹ Consistent with FinCEN's SAR instructions, financial institutions should focus the SAR narrative on the information necessary to enable the reader to understand the activity reported, including what was unusual or irregular about the activity

10. Customer Due Diligence (CDD) regulations (31 CFR §§ 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, and 1030.210) do not categorically require the performance of media searches or particular screenings. However, in certain circumstances, a financial institution might assess, on the basis of risk, that a customer presents a higher risk profile and, accordingly, collect more information (such as media searches) to better understand the customer relationship. Such information also assists a financial institution in determining when transactions are potentially suspicious. See, e.g., "Frequently Asked Questions Regarding Customer Due Diligence Requirements for Covered Financial Institutions," August 3, 2020, <https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-regarding-customer-due-1>.

11. See FinCEN Suspicious Activity Report Electronic Filing Requirements, last updated July 2020, available at: https://bsaefiling.fincen.treas.gov/docs/XMLUserGuide_FinCENSAR.pdf at p. 167.

that caused suspicion. For example, granular detail (such as subject identification data) that is reported in the appropriate SAR data fields does not need to be repeated in the SAR narrative, unless such information is necessary to clearly describe the activity reported. Additionally, the SAR narrative may benefit from information about the suspicious activity that may not be readily evident from SAR data fields alone, such as an explanation about why the filer selected different characterizations of suspicious activity in the SAR data fields. Note, however, that FinCEN Advisories may include requests for financial institutions to incorporate certain terms in SAR field 2 (Financial Institution Note to FinCEN) and in the narrative to indicate a connection between the suspicious activity being reported and the subject of an advisory.¹²

Question 7: SAR Character Limits

Should financial institutions file additional SARs on the same suspicious activity to accommodate narratives that are longer than the SAR narrative character limits?

No. Filers must provide a clear, complete, and concise description of the suspicious activity that led to the decision to file the SAR.¹³ A financial institution that reaches the SAR narrative character limit should not file an additional SAR to continue a narrative in order to avoid duplicate filings on the same activity in the database.¹⁴ Instead, filers should focus the relevant information in the narrative as much as possible, and may include additional, relevant information as an attachment to the SAR, or note that it is available as supporting documentation.

To keep narratives within the character limit and enable efficient review of information (such as transaction records) that is displayed most clearly in tabular format, filers can include a single comma-separated values (CSV) file with no more than one megabyte of data as an attachment to a SAR. If a filer wishes to include information in a tabular format in a SAR, the CSV attachment should be used; filers should not include tabular information within the SAR narrative.

Filers must retain all supporting documentation or a business record equivalent for five years from the date of the report.¹⁵ All supporting documentation (such as copies of instruments; receipts; sale, transaction or clearing records; photographs; and surveillance audio or video recordings) must be made available to appropriate authorities upon request.¹⁶

12. For additional information on FinCEN Advisories, see <https://www.fincen.gov/resources/advisoriesbulletinsfactsheets>.

13. See FinCEN Suspicious Activity Report Electronic Filing Requirements, last updated July 2020, available at: https://bsaefiling.fincen.treas.gov/docs/XMLUserGuide_FinCENSAR.pdf at p. 167.

14. A SAR narrative can have a maximum of 20,000 characters. For more information, see FinCEN Suspicious Activity Report Electronic Filing Requirements, last updated July 2020, available at: https://bsaefiling.fincen.treas.gov/docs/XMLUserGuide_FinCENSAR.pdf at p. 105.

15. 31 CFR § 1010.430; 31 CFR § 1010.320; subpart C of the relevant financial institution part of 31 CFR Chapter X.

16. 31 CFR § 1010.320; subpart C of the relevant financial institution part of 31 CFR Chapter X.



FinCEN NOTICE

FIN-2021-NTC1

February 24, 2021

Consolidated COVID-19 Suspicious Activity Report Key Terms and Filing Instructions

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to consolidate filing instructions and key terms for fraudulent activities, crimes, and cyber and ransomware attacks related to Coronavirus Disease 2019 (COVID-19), and to remind financial institutions of recent updates to FinCEN guidance concerning Section 314(b). FinCEN has published a series of advisories and notices on COVID-19-related threats to assist financial institutions with the filing of suspicious activity reports (SARs) involving such threats. In this Notice, FinCEN further requests that financial institutions consult the tables below when filing SARs for COVID-19-related activity.

Table 1 contains key terms and instructions related to government programs. Table 2 contains a summary of the key terms and instructions for COVID-19-related activities that are not tied to specific government programs. Table 3 provides a list of additional FinCEN's COVID-19-related publications. Financial institutions that follow the instructions set forth below will assist FinCEN, law enforcement, financial regulators, and other relevant government agencies in identifying and utilizing the information submitted in COVID-19-related SARs.

Financial institutions should consult previously published advisories and notices for additional SAR filing instructions related to the advisories and notices included below. If financial institutions wish to cite more than one advisory, then they should use only the FinCEN identification numbers (FINs) listed in the tables below in Field 2, and provide the full references in the SAR narrative. FinCEN requests that filers be as specific as possible in their SAR filings. For instance, if the SAR addresses a government program, FinCEN requests that filers use program-specific keywords, as detailed in the keyword columns in Table 1 below, and avoid relying on generalized key terms, such as "stimulus," "CARES Act," or "benefit." Doing so will expedite identification of relevant SARs for appropriate investigative, analytical, supervisory, and other authorized purposes.

FINCEN NOTICE

Table 1: COVID-19 Government Programs

Government Program	Keyword(s) for Suspicious Activity and narrative	Field 2 (Note to FinCEN)	Suspicious Activity Field(s) 32-42
Economic Injury Disaster Loan (EIDL) Program ¹	Economic injury disaster	COVID19 EIDL FUNDS FRAUD ²	34(z) (Fraud - other)
Economic Impact Payments (EIP) ³	Economic impact payment	FIN-2021-A002	34(z) (Fraud - other)
Paycheck Protection Program (PPP) ⁴	Paycheck protection	FIN-2021-NTC1	34(z) (Fraud - other)
State Unemployment Insurance ⁵	Unemployment	COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007 ⁶	34(z) (Fraud - other)
Pandemic Unemployment Assistance	Unemployment	COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007 ⁷	34(z) (Fraud - other)
Main Street Lending ⁸	FED MSL	FIN-2021-NTC1	34(z) (Fraud - other)

1. For more information regarding this loan program, please visit U.S. Small Business Administration (SBA), [Economic Injury Disaster Loans](#).
2. FinCEN News, "[Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered virtually at the ACAMS AML Conference](#)," (September 29, 2020).
3. For more information about EIPs, please visit Internal Revenue Service (IRS), [Economic Impact Payment Information Center](#).
4. For more information regarding the PPP, please visit SBA, [Paycheck Protection Program](#).
5. For more information about COVID-19-related unemployment insurance programs and relief, please visit the U.S. Department of Labor, [Unemployment Insurance Relief During COVID-19 Outbreak](#).
6. FinCEN Advisory, [FIN-2020-A007](#), "Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic," (October 13, 2020).
7. *Id.*
8. For more information regarding the Main Street Lending Program, please visit Board of Governors of the Federal Reserve System, [Main Street Lending Program](#).

FINCEN NOTICE

Table 2: Other COVID-19-related Crimes and Frauds

Potential Fraud or Crime	Keyword(s) for Suspicious Activity and narrative	Field 2 (Note to FinCEN)	Suspicious Activity Field(s) 32-42
Cyber crime	BEC fraud, EAC fraud, and others as warranted	COVID19-CYBER FIN-2020-A005 ⁹	34 (z) (Fraud –other) for BEC, EAC; 38 (a) account takeover; 42 (a), (b), and/or (z), as appropriate (noting the (z) “other” box the COVID-19 cyber event); 44 (a) through (j) cyber event indicators, as relevant and available
Health insurance and health care	Kickbacks, services not provided, billing schemes, and others as warranted	FIN-2021-A001 ¹⁰	34(g) (Health care – public or private health insurance)
Medical products	Fraudulent products, non-delivery scam, price gouging, hoarding	COVID19 FIN-2020-A002 ¹¹	34(z) (Fraud - other)
Vaccine-related scams and cyber crimes	Vaccine scam or vaccine ransomware	FIN-2020-NTC4 ¹²	34(z) (Fraud - other)
Money mule and imposter scams	Imposter, money mule scams	COVID19 MM FIN-2020-A003 ¹³	34(z) (Fraud - other)

9. FinCEN Advisory, [FIN-2020-A005](#), “Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic,” (July 30, 2020).
10. FinCEN Advisory, [FIN-2021-A001](#), “Advisory on COVID-19 Health Insurance- and Health Care-Related Fraud,” (February 2, 2021).
11. FinCEN Advisory, [FIN-2020-A002](#), “Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19),” (May 18, 2020).
12. FinCEN Notice, [FIN-2020-NTC4](#), “FinCEN Asks Financial Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks,” (December 28, 2020).
13. FinCEN Advisory, [FIN-2020-A003](#), “Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19),” (July 7, 2020).

FINCEN NOTICE

Table 3: Additional FinCEN COVID-19-related Publications

Field 2 (Note to FinCEN)	Title
February 1, 2021 FAQs	Paycheck Protection Program Frequently Asked Questions (FAQs)
FIN-2020-NTC3	Notice Related to the Coronavirus Disease 2019 (COVID-19)
FIN-2020-NTC2	The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic
FIN-2020-NTC1	The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity

Updates to Section 314(b) Fact Sheet and Information Sharing Documents

FinCEN updated its USA PATRIOT Act [Section 314\(b\) Fact Sheet](#) in December 2020. The Fact Sheet, which addresses safe harbor protections in connection with certain private-sector information sharing, supersedes the material concerning information sharing provided in FinCEN's May 2020 [Notice Related to the Coronavirus Disease 2019 \(COVID-19\)](#).

For Further Information

Additional COVID-19-related information, including COVID-19-related advisories and notices, is located on FinCEN's website at <https://www.fincen.gov/coronavirus>, which also contains information on how to register for [FinCEN Updates](#).

Questions or comments regarding the contents of this notice should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



Department of the Treasury Financial Crimes Enforcement Network

Guidance

FIN-2014-G001

Issued: February 14, 2014

Subject: **BSA Expectations Regarding Marijuana-Related Businesses**

The Financial Crimes Enforcement Network ("FinCEN") is issuing guidance to clarify Bank Secrecy Act ("BSA") expectations for financial institutions seeking to provide services to marijuana-related businesses. FinCEN is issuing this guidance in light of recent state initiatives to legalize certain marijuana-related activity and related guidance by the U.S. Department of Justice ("DOJ") concerning marijuana-related enforcement priorities. This FinCEN guidance clarifies how financial institutions can provide services to marijuana-related businesses consistent with their BSA obligations, and aligns the information provided by financial institutions in BSA reports with federal and state law enforcement priorities. This FinCEN guidance should enhance the availability of financial services for, and the financial transparency of, marijuana-related businesses.

Marijuana Laws and Law Enforcement Priorities

The Controlled Substances Act ("CSA") makes it illegal under federal law to manufacture, distribute, or dispense marijuana.¹ Many states impose and enforce similar prohibitions. Notwithstanding the federal ban, as of the date of this guidance, 20 states and the District of Columbia have legalized certain marijuana-related activity. In light of these developments, U.S. Department of Justice Deputy Attorney General James M. Cole issued a memorandum (the "Cole Memo") to all United States Attorneys providing updated guidance to federal prosecutors concerning marijuana enforcement under the CSA.² The Cole Memo guidance applies to all of DOJ's federal enforcement activity, including civil enforcement and criminal investigations and prosecutions, concerning marijuana in all states.

The Cole Memo reiterates Congress's determination that marijuana is a dangerous drug and that the illegal distribution and sale of marijuana is a serious crime that provides a significant source of revenue to large-scale criminal enterprises, gangs, and cartels. The Cole Memo notes that DOJ is committed to enforcement of the CSA consistent with those determinations. It also notes that DOJ is committed to using its investigative and prosecutorial resources to address the most

¹ Controlled Substances Act, 21 U.S.C. § 801, *et seq.*

² James M. Cole, Deputy Attorney General, U.S. Department of Justice, *Memorandum for All United States Attorneys: Guidance Regarding Marijuana Enforcement* (August 29, 2013), available at <http://www.justice.gov/iso/opa/resources/3052013829132756857467.pdf>.

EXHIBIT 3-A

significant threats in the most effective, consistent, and rational way. In furtherance of those objectives, the Cole Memo provides guidance to DOJ attorneys and law enforcement to focus their enforcement resources on persons or organizations whose conduct interferes with any one or more of the following important priorities (the “Cole Memo priorities”):³

- Preventing the distribution of marijuana to minors;
- Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels;
- Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
- Preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
- Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
- Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
- Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on public lands; and
- Preventing marijuana possession or use on federal property.

Concurrently with this FinCEN guidance, Deputy Attorney General Cole is issuing supplemental guidance directing that prosecutors also consider these enforcement priorities with respect to federal money laundering, unlicensed money transmitter, and BSA offenses predicated on marijuana-related violations of the CSA.⁴

Providing Financial Services to Marijuana-Related Businesses

This FinCEN guidance clarifies how financial institutions can provide services to marijuana-related businesses consistent with their BSA obligations. In general, the decision to open, close, or refuse any particular account or relationship should be made by each financial institution based on a number of factors specific to that institution. These factors may include its particular business objectives, an evaluation of the risks associated with offering a particular product or service, and its capacity to manage those risks effectively. Thorough customer due diligence is a critical aspect of making this assessment.

In assessing the risk of providing services to a marijuana-related business, a financial institution should conduct customer due diligence that includes: (i) verifying with the appropriate state authorities whether the business is duly licensed and registered; (ii) reviewing the license application (and related documentation) submitted by the business for obtaining a state license to operate its marijuana-related business; (iii) requesting from state licensing and enforcement authorities available information about the business and related parties; (iv) developing an understanding of the normal and expected activity for the business, including the types of

³ The Cole Memo notes that these enforcement priorities are listed in general terms; each encompasses a variety of conduct that may merit civil or criminal enforcement of the CSA.

⁴ James M. Cole, Deputy Attorney General, U.S. Department of Justice, *Memorandum for All United States Attorneys: Guidance Regarding Marijuana Related Financial Crimes* (February 14, 2014).

EXHIBIT 3-A

products to be sold and the type of customers to be served (e.g., medical versus recreational customers); (v) ongoing monitoring of publicly available sources for adverse information about the business and related parties; (vi) ongoing monitoring for suspicious activity, including for any of the red flags described in this guidance; and (vii) refreshing information obtained as part of customer due diligence on a periodic basis and commensurate with the risk. With respect to information regarding state licensure obtained in connection with such customer due diligence, a financial institution may reasonably rely on the accuracy of information provided by state licensing authorities, where states make such information available.

As part of its customer due diligence, a financial institution should consider whether a marijuana-related business implicates one of the Cole Memo priorities or violates state law. This is a particularly important factor for a financial institution to consider when assessing the risk of providing financial services to a marijuana-related business. Considering this factor also enables the financial institution to provide information in BSA reports pertinent to law enforcement's priorities. A financial institution that decides to provide financial services to a marijuana-related business would be required to file suspicious activity reports ("SARs") as described below.

Filing Suspicious Activity Reports on Marijuana-Related Businesses

The obligation to file a SAR is unaffected by any state law that legalizes marijuana-related activity. A financial institution is required to file a SAR if, consistent with FinCEN regulations, the financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution: (i) involves funds derived from illegal activity or is an attempt to disguise funds derived from illegal activity; (ii) is designed to evade regulations promulgated under the BSA, or (iii) lacks a business or apparent lawful purpose.⁵ Because federal law prohibits the distribution and sale of marijuana, financial transactions involving a marijuana-related business would generally involve funds derived from illegal activity. Therefore, a financial institution is required to file a SAR on activity involving a marijuana-related business (including those duly licensed under state law), in accordance with this guidance and FinCEN's suspicious activity reporting requirements and related thresholds.

One of the BSA's purposes is to require financial institutions to file reports that are highly useful in criminal investigations and proceedings. The guidance below furthers this objective by assisting financial institutions in determining how to file a SAR that facilitates law enforcement's access to information pertinent to a priority.

"Marijuana Limited" SAR Filings

A financial institution providing financial services to a marijuana-related business that it reasonably believes, based on its customer due diligence, does not implicate one of the Cole Memo priorities or violate state law should file a "Marijuana Limited" SAR. The content of this

⁵ See, e.g., 31 CFR § 1020.320. Financial institutions shall file with FinCEN, to the extent and in the manner required, a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution may also file with FinCEN a SAR with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations.

EXHIBIT 3-A

SAR should be limited to the following information: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) the fact that the filing institution is filing the SAR solely because the subject is engaged in a marijuana-related business; and (iv) the fact that no additional suspicious activity has been identified. Financial institutions should use the term “MARIJUANA LIMITED” in the narrative section.

A financial institution should follow FinCEN’s existing guidance on the timing of filing continuing activity reports for the same activity initially reported on a “Marijuana Limited” SAR.⁶ The continuing activity report may contain the same limited content as the initial SAR, plus details about the amount of deposits, withdrawals, and transfers in the account since the last SAR. However, if, in the course of conducting customer due diligence (including ongoing monitoring for red flags), the financial institution detects changes in activity that potentially implicate one of the Cole Memo priorities or violate state law, the financial institution should file a “Marijuana Priority” SAR.

“Marijuana Priority” SAR Filings

A financial institution filing a SAR on a marijuana-related business that it reasonably believes, based on its customer due diligence, implicates one of the Cole Memo priorities or violates state law should file a “Marijuana Priority” SAR. The content of this SAR should include comprehensive detail in accordance with existing regulations and guidance. Details particularly relevant to law enforcement in this context include: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) details regarding the enforcement priorities the financial institution believes have been implicated; and (iv) dates, amounts, and other relevant details of financial transactions involved in the suspicious activity. Financial institutions should use the term “MARIJUANA PRIORITY” in the narrative section to help law enforcement distinguish these SARs.⁷

“Marijuana Termination” SAR Filings

If a financial institution deems it necessary to terminate a relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, it should

⁶ Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (Question #16), *available at*: http://fincen.gov/whatsnew/html/sar_faqs.html (providing guidance on the filing timeframe for submitting a continuing activity report).

⁷ FinCEN recognizes that a financial institution filing a SAR on a marijuana-related business may not always be well-positioned to determine whether the business implicates one of the Cole Memo priorities or violates state law, and thus which terms would be most appropriate to include (i.e., “Marijuana Limited” or “Marijuana Priority”). For example, a financial institution could be providing services to another domestic financial institution that, in turn, provides financial services to a marijuana-related business. Similarly, a financial institution could be providing services to a non-financial customer that provides goods or services to a marijuana-related business (e.g., a commercial landlord that leases property to a marijuana-related business). In such circumstances where services are being provided indirectly, the financial institution may file SARs based on existing regulations and guidance without distinguishing between “Marijuana Limited” and “Marijuana Priority.” Whether the financial institution decides to provide indirect services to a marijuana-related business is a risk-based decision that depends on a number of factors specific to that institution and the relevant circumstances. In making this decision, the institution should consider the Cole Memo priorities, to the extent applicable.

EXHIBIT 3-A

file a SAR and note in the narrative the basis for the termination. Financial institutions should use the term “MARIJUANA TERMINATION” in the narrative section. To the extent the financial institution becomes aware that the marijuana-related business seeks to move to a second financial institution, FinCEN urges the first institution to use Section 314(b) voluntary information sharing (if it qualifies) to alert the second financial institution of potential illegal activity. See *Section 314(b) Fact Sheet* for more information.⁸

Red Flags to Distinguish Priority SARs

The following red flags indicate that a marijuana-related business may be engaged in activity that implicates one of the Cole Memo priorities or violates state law. These red flags indicate only possible signs of such activity, and also do not constitute an exhaustive list. It is thus important to view any red flag(s) in the context of other indicators and facts, such as the financial institution’s knowledge about the underlying parties obtained through its customer due diligence. Further, the presence of any of these red flags in a given transaction or business arrangement may indicate a need for additional due diligence, which could include seeking information from other involved financial institutions under Section 314(b). These red flags are based primarily upon schemes and typologies described in SARs or identified by our law enforcement and regulatory partners, and may be updated in future guidance.

- A customer appears to be using a state-licensed marijuana-related business as a front or pretext to launder money derived from other criminal activity (i.e., not related to marijuana) or derived from marijuana-related activity not permitted under state law. Relevant indicia could include:
 - The business receives substantially more revenue than may reasonably be expected given the relevant limitations imposed by the state in which it operates.
 - The business receives substantially more revenue than its local competitors or than might be expected given the population demographics.
 - The business is depositing more cash than is commensurate with the amount of marijuana-related revenue it is reporting for federal and state tax purposes.
 - The business is unable to demonstrate that its revenue is derived exclusively from the sale of marijuana in compliance with state law, as opposed to revenue derived from (i) the sale of other illicit drugs, (ii) the sale of marijuana not in compliance with state law, or (iii) other illegal activity.
 - The business makes cash deposits or withdrawals over a short period of time that are excessive relative to local competitors or the expected activity of the business.

⁸ Information Sharing Between Financial Institutions: Section 314(b) Fact Sheet, *available at*: http://fincen.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf.

EXHIBIT 3-A

- Deposits apparently structured to avoid Currency Transaction Report (“CTR”) requirements.
 - Rapid movement of funds, such as cash deposits followed by immediate cash withdrawals.
 - Deposits by third parties with no apparent connection to the account holder.
 - Excessive commingling of funds with the personal account of the business’s owner(s) or manager(s), or with accounts of seemingly unrelated businesses.
 - Individuals conducting transactions for the business appear to be acting on behalf of other, undisclosed parties of interest.
 - Financial statements provided by the business to the financial institution are inconsistent with actual account activity.
 - A surge in activity by third parties offering goods or services to marijuana-related businesses, such as equipment suppliers or shipping servicers.
- The business is unable to produce satisfactory documentation or evidence to demonstrate that it is duly licensed and operating consistently with state law.
 - The business is unable to demonstrate the legitimate source of significant outside investments.
 - A customer seeks to conceal or disguise involvement in marijuana-related business activity. For example, the customer may be using a business with a non-descript name (e.g., a “consulting,” “holding,” or “management” company) that purports to engage in commercial activity unrelated to marijuana, but is depositing cash that smells like marijuana.
 - Review of publicly available sources and databases about the business, its owner(s), manager(s), or other related parties, reveal negative information, such as a criminal record, involvement in the illegal purchase or sale of drugs, violence, or other potential connections to illicit activity.
 - The business, its owner(s), manager(s), or other related parties are, or have been, subject to an enforcement action by the state or local authorities responsible for administering or enforcing marijuana-related laws or regulations.
 - A marijuana-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.

EXHIBIT 3-A

- The owner(s) or manager(s) of a marijuana-related business reside outside the state in which the business is located.
- A marijuana-related business is located on federal property or the marijuana sold by the business was grown on federal property.
- A marijuana-related business's proximity to a school is not compliant with state law.
- A marijuana-related business purporting to be a "non-profit" is engaged in commercial activity inconsistent with that classification, or is making excessive payments to its manager(s) or employee(s).

Currency Transaction Reports and Form 8300's

Financial institutions and other persons subject to FinCEN's regulations must report currency transactions in connection with marijuana-related businesses the same as they would in any other context, consistent with existing regulations and with the same thresholds that apply. For example, banks and money services businesses would need to file CTRs on the receipt or withdrawal by any person of more than \$10,000 in cash per day. Similarly, any person or entity engaged in a non-financial trade or business would need to report transactions in which they receive more than \$10,000 in cash and other monetary instruments for the purchase of goods or services on FinCEN Form 8300 (Report of Cash Payments Over \$10,000 Received in a Trade or Business). A business engaged in marijuana-related activity may not be treated as a non-listed business under 31 C.F.R. § 1020.315(e)(8), and therefore, is not eligible for consideration for an exemption with respect to a bank's CTR obligations under 31 C.F.R. § 1020.315(b)(6).

* * * * *

FinCEN's enforcement priorities in connection with this guidance will focus on matters of systemic or significant failures, and not isolated lapses in technical compliance. Financial institutions with questions about this guidance are encouraged to contact FinCEN's Resource Center at (800) 767-2825, where industry questions can be addressed and monitored for the purpose of providing any necessary additional guidance.

EXHIBIT 3-A

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Financial Crimes Enforcement Network
Office of the Comptroller of the Currency
Conference of State Bank Supervisors**

Providing Financial Services to Customers Engaged in Hemp-Related Businesses

The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Financial Crimes Enforcement Network (FinCEN), and the Office of the Comptroller of the Currency in consultation with the Conference of State Bank Supervisors, are issuing this statement to provide clarity regarding the legal status of commercial growth and production of hemp and relevant requirements for banks¹ under the Bank Secrecy Act (BSA) and its implementing regulations. FinCEN will issue additional guidance after further reviewing and evaluating the U.S. Department of Agriculture (USDA) interim final rule.

Background

The Agriculture Improvement Act of 2018 (2018 Farm Bill),² which removed hemp as a Schedule I controlled substance under the Controlled Substances Act³ was signed into law on December 20, 2018. The 2018 Farm Bill directs the USDA, in consultation with the U.S. Attorney General, to regulate hemp production.⁴ The 2018 Farm Bill states that hemp production shall be subject to a hemp production regulatory plan established by the USDA, the states,⁵ or tribal governments.

On October 31, 2019, the USDA issued an interim final rule establishing the domestic hemp production regulatory program to facilitate the legal production of hemp, as set forth in the 2018 Farm Bill.⁶ Under the interim final rule, state departments of agriculture and tribal governments may submit plans for monitoring and regulating the domestic production of hemp to the USDA for approval. The interim final rule establishes a federal licensing plan for regulating hemp producers in states and tribal territories that do not have their own USDA-approved plans. In the

¹ For the purposes of this statement, the term “bank” means each agent, agency, branch or office within the United States of commercial banks, savings banks, savings and loan associations, thrift institutions, and foreign banks.

² Pub. L. 115-334, 132 Stat. 4490.

³ The term “hemp” is defined in the 2018 Farm Bill as “the plant *Cannabis sativa* L. and any part of that plant, including the seeds thereof and all derivatives, extracts, cannabinoids, isomers, acids, salts, and salts of isomers, whether growing or not, with a delta-9 tetrahydrocannabinol [THC] concentration of not more than 0.3 percent on a dry weight basis.” 7 U.S.C. 1639o(1).

⁴ 7 U.S.C. 1639r(a)(1).

⁵ The 2018 Farm Bill defines states to include a state, the District of Columbia, the Commonwealth of Puerto Rico, and any other territory or possession of the United States. 7 U.S.C. 1639o(4).

⁶ See Establishment of a Domestic Hemp Production Program, 84 *Fed. Reg.* 58522 (Oct. 31, 2019) (to be codified at 7 CFR 990).

EXHIBIT 3-A

absence of a state or tribal regulatory plan, hemp producers will be subject to regulation directly by the USDA unless the state or tribal government prohibits hemp production.

The interim final rule includes requirements for maintaining information on the land where hemp is produced, testing hemp for tetrahydrocannabinol (THC) levels, disposing of plants with more than 0.3 percent THC, and licensing for hemp producers. The USDA regulations are in effect to accommodate the 2020 planting season.

Key Points

- Consistent with the USDA interim final rule, hemp may be grown only with a valid USDA-issued license or under a USDA-approved state or tribal plan. Research and development initiatives authorized under the Agricultural Act of 2014 (2014 Farm Bill) remain in effect until one year after the effective date of the USDA interim final rule.
- A state or tribal government may prohibit the production of hemp, even though it is legal under federal law. The 2018 Farm Bill provisions related to USDA-approved state or tribal plans did not preempt state or tribal laws regarding the production of hemp that are more stringent than federal law.
- Separately, marijuana⁷ is still a controlled substance under federal law. The 2018 Farm Bill amended the definition of marijuana only to exclude hemp from the Controlled Substances Act.

BSA Considerations

Because hemp is no longer a Schedule I controlled substance under the Controlled Substances Act, banks are not required to file a Suspicious Activity Report (SAR) on customers solely because they are engaged in the growth or cultivation of hemp in accordance with applicable laws and regulations. For hemp-related customers, banks are expected to follow standard SAR procedures, and file a SAR if indicia of suspicious activity warrants.

Bank customers engaged in hemp-related business activities are responsible for complying with the requirements set forth in the 2018 Farm Bill⁸ and applicable regulations. It is generally a bank's business decision as to the types of permissible services and accounts to offer, and banks

⁷ The term "marijuana" is defined in the Controlled Substance Act at 21 U.S.C. 802.16, as amended by section 12619 of the 2018 Farm Bill.

⁸ The interim final rule governs the production of hemp under the 2018 Farm Bill. The interim final rule does not affect hemp that was or is being cultivated under the 2014 Farm Bill programs. That hemp remains subject to the requirements of the 2014 Farm Bill.

EXHIBIT 3-A

must have a BSA/AML compliance program⁹ commensurate with the level of complexity and risks involved. When deciding to serve hemp-related businesses, banks must comply with applicable regulatory requirements for customer identification,¹⁰ suspicious activity reporting,¹¹ currency transaction reporting,¹² and risk-based customer due diligence,¹³ including the collection of beneficial ownership information for legal entity customers.¹⁴

In the context of marijuana-related businesses, banks should continue following FinCEN guidance FIN-2014-G001 – BSA Expectations Regarding Marijuana-Related Businesses.¹⁵

Additional Information

For questions regarding the 2018 Farm Bill and its implementing regulations, banks may consider contacting the USDA, state departments of agriculture, or tribal governments. Additionally, the 2018 Farm Bill explicitly preserved the authority of the U.S. Food and Drug Administration (FDA) to regulate hemp products under the Federal Food, Drug, and Cosmetic Act and section 351 of the Public Health Service Act. Banks may consider contacting the FDA with hemp-related food, drug, and cosmetic questions.

⁹ See 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (Board of Governors of the Federal Reserve System); 12 CFR 326.8 (Federal Deposit Insurance Corporation); 12 CFR 21.21 (Office of the Comptroller of the Currency); and 31 CFR 1020.210 (Financial Crimes Enforcement Network).

¹⁰ See 12 CFR 208.63(b), 211.5(m), 211.24(j) (Board of Governors of the Federal Reserve System); 12 CFR 326.8 (b) (Federal Deposit Insurance Corporation); 12 CFR 21.21 (Office of the Comptroller of the Currency); and 31 CFR 1020.220 (FinCEN).

¹¹ See 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System); 12 CFR 353 (Federal Deposit Insurance Corporation); 12 CFR 21.11 and 163.180 (Office of the Comptroller of the Currency); and 31 CFR 1020.320 (FinCEN).

¹² See 31 CFR 1010.311.

¹³ See 31 CFR 1020.210(b)(5).

¹⁴ See 31 CFR 1010.230.

¹⁵ Available at: <https://www.fincen.gov/resources/statutes-regulations/guidance/bsa-expectations-regarding-marijuana-related-businesses>.



FinCEN GUIDANCE

FIN-2020-G001

Issued: June 29, 2020

Subject: **FinCEN Guidance Regarding Due Diligence Requirements under the Bank Secrecy Act for Hemp-Related Business Customers**

The Financial Crimes Enforcement Network (FinCEN) is issuing this guidance to address questions related to Bank Secrecy Act/Anti-Money Laundering (BSA/AML) regulatory requirements for hemp-related business customers. This guidance explains how financial institutions¹ can conduct due diligence for hemp-related businesses, and identifies the type of information and documentation financial institutions can collect from hemp-related businesses to comply with BSA regulatory requirements. This clarification is intended to enhance the availability of financial services for, and the financial transparency of, hemp-related businesses in compliance with federal law. This guidance supplements the December 3, 2019 interagency statement on providing financial services to customers engaged in hemp-related businesses (December Hemp Statement).²

This guidance provides financial institutions BSA/AML risk considerations only for hemp-related businesses (i.e., businesses or individuals that grow hemp, and processors and manufacturers who purchase hemp directly from such growers). This guidance does not replace or supersede FinCEN's previous guidance on the BSA expectations regarding marijuana-related businesses (2014 Marijuana Guidance).³

Background

The Agriculture Improvement Act of 2018 (the 2018 Farm Bill)⁴ removed hemp from the definition of marijuana in the Controlled Substances Act (CSA)⁵ and directed the establishment of a regulatory framework for the legal production of hemp. The 2018 Farm

1. See 31 CFR § 1010.100(t) (defining "financial institutions").
2. See "Providing Financial Services to Customers Engaged in Hemp-Related Businesses," Dec. 3, 2019, *available at* <https://www.fincen.gov/sites/default/files/2019-12/Hemp%20Guidance%20%28Final%2012-3-19%29%20FINAL.pdf>.
3. See FIN-2014-G001, "BSA Expectations Regarding Marijuana-Related Businesses," Feb. 14, 2014, *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/bsa-expectations-regarding-marijuana-related-businesses>.
4. Pub. L. 115-334, 132 Stat. 4500 (2018).
5. The term "marihuana" is defined in the Controlled Substances Act at 21 U.S.C. § 802(16), as amended by section 12619 of the 2018 Farm Bill. Also, "marihuana" refers to the currently used term "marijuana."

FINCEN GUIDANCE

Bill defines “hemp” as the plant *Cannabis sativa* L. and any part of that plant, including the seeds thereof and all derivatives, extracts, cannabinoids, isomers, acids, salts, and salts of isomers, whether growing or not, with a delta-9 tetrahydrocannabinol (THC) concentration of not more than 0.3 percent on a dry weight basis.⁶

On October 31, 2019, the U.S. Department of Agriculture (USDA) issued an interim final rule (Interim Final Rule) establishing the domestic hemp production regulatory program to facilitate the legal production of hemp, as set forth in the 2018 Farm Bill.⁷ Under the Interim Final Rule, state and tribal governments may submit plans to the USDA for approval to monitor and regulate the domestic production of hemp. The Interim Final Rule: (i) establishes a federal licensing plan for regulating hemp producers in states and tribal territories that do not have their own USDA-approved plans, and that do not prohibit hemp production; and (ii) includes requirements for maintaining information on the land where hemp is produced, testing hemp for THC levels, disposing of plants with more than 0.3 percent THC concentration, and licensing hemp producers.⁸

The 2018 Farm Bill explicitly preserved the authority of the U.S. Food and Drug Administration (FDA) to regulate products containing cannabis or cannabis-derived compounds, including hemp, under the Federal Food, Drug, and Cosmetic Act and section 351 of the Public Health Service Act.

BSA/AML Program Expectations

Financial institutions must conduct customer due diligence (CDD) for all customers, including hemp-related businesses. Financial institutions should obtain basic identifying information about hemp-related businesses through the application of the financial institutions’ customer identification programs and risk-based CDD processes, including beneficial ownership collection and verification, as they would for all customers.⁹ Financial institutions must also establish appropriate risk-based procedures for conducting ongoing CDD.

For customers who are hemp growers, financial institutions may confirm the hemp grower’s compliance with state, tribal government, or the USDA licensing requirements, as applicable, by either obtaining (1) a written attestation by the hemp grower that they are

6. Section 10113 of the 2018 Farm Bill defines “hemp” more broadly than the 2014 Farm Bill defined “industrial hemp,” thus eliminating any question that both the plants and products derived from the plants are legal, so long as the THC concentration does not exceed 0.3 percent on a dry weight basis. 2018 Farm Bill § 10113, codified at 7 U.S.C. § 1639o(1). Included within the definition of hemp in the 2018 Farm Bill is cannabidiol (CBD), a cannabinoid that is a compound extracted from the cannabis plant with a delta-9-THC concentration of not more than 0.3 percent on a dry weight basis.
7. See Establishment of a Domestic Hemp Production Program, 84 Fed. Reg. 58522 (Oct. 31, 2019) (codified at 7 CFR § 990).
8. For additional details on USDA requirements, see “Hemp Production,” <https://www.ams.usda.gov/rules-regulations/hemp> (last visited June 25, 2020).
9. See 31 CFR § 1010.230 (setting forth beneficial ownership requirements for legal entity customers).

FINCEN GUIDANCE

validly licensed, or (2) a copy of such license. The extent to which a financial institution will seek additional information beyond the steps outlined above will depend on the financial institution's assessment of the level of risk posed by each customer. Additional information might include crop inspection or testing reports, license renewals, updated attestations from the business, or correspondence with the state, tribal government, or USDA. In order to identify the risks posed, financial institutions must understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and conduct ongoing monitoring to identify and report suspicious transactions, including, on a risk basis, to maintain and update customer information.¹⁰ As with any customer, FinCEN expects financial institutions to tailor their BSA/AML programs to reflect the risks associated with the customer's particular risk profile and file reports required under the BSA.

Suspicious Activity Reporting

As noted in the December Hemp Statement, because hemp is no longer a Schedule I controlled substance under the CSA, financial institutions are not required to file a Suspicious Activity Report (SAR) on customers solely because they are engaged in the growth or cultivation of hemp in accordance with applicable laws and regulations. For hemp-related business customers, financial institutions are expected to follow standard SAR procedures and file a SAR if the financial institution becomes aware, in the normal course of business, of suspicious activity. Such suspicious activity could include, among other things, the following:

- A customer appears to be engaged in hemp production in a state or jurisdiction in which hemp production remains illegal.
- A customer appears to be using a state-licensed hemp business as a front or pretext to launder money derived from other criminal activity or derived from marijuana-related activity that may not be permitted under applicable law.
- A customer engaged in hemp production seeks to conceal or disguise involvement in marijuana-related business activity.
- The customer is unable or unwilling to certify or provide sufficient information to demonstrate that it is duly licensed and operating consistent with applicable law, or the financial institution becomes aware that the customer continues to operate (i) after a license revocation, or (ii) inconsistently with applicable law.

10. See 31 U.S.C. § 5318(h) and 31 CFR § 1010.210 for AML program requirements, and, as applied to specific types of financial institutions, 31 CFR §§ 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, and 1030.210. Customer information must include information regarding the beneficial owners of legal entity customers as defined in 31 CFR § 1010.230.

EXHIBIT 3-A

FINCEN GUIDANCE

FinCEN expects financial institutions to monitor the transactions of hemp-related businesses for signs of suspicious or unlawful activity, just as with other customers. To the extent the financial transactions of a hemp-related business are comingled with marijuana-related activities, a financial institution should apply FinCEN's 2014 Marijuana Guidance, which provides clarity on how to file SARs on marijuana-related activities. However, if the proceeds of the businesses are kept separate, or the customer and its financial institution are able to identify which proceeds are marijuana-related and which are hemp-related, then the 2014 Marijuana Guidance, including specific SAR filing, applies only to the marijuana-related part of the business.

Currency Transaction Reports and FinCEN Form 8300

Financial institutions must report currency transactions in connection with hemp-related businesses in the same manner they would for any other customers (i.e., report all currency transactions above \$10,000 in aggregate on a single business day). Similarly, any person or entity engaged in a non-financial trade or business would need to report on FinCEN Form 8300 (Report of Cash Payments Over \$10,000 Received in a Trade or Business) transactions in which the person receives more than \$10,000 in cash and other monetary instruments from a hemp-related business for the purchase of goods or services.

Additional Information

For questions regarding the 2018 Farm Bill and its implementing regulations, financial institutions should contact the USDA, state departments of agriculture, or tribal governments. For questions related to FDA-regulated products, financial institutions should contact the FDA. For questions about this guidance, financial institutions should contact FinCEN's Resource Center at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



Financial Trend Analysis

Financial Crimes Enforcement Network / FinCEN

Elders Face Increased Financial Threat from Domestic and Foreign Actors

The Financial Crimes Enforcement Network (FinCEN) is releasing this strategic analysis of Bank Secrecy Act (BSA) reporting to share information pertaining to elder financial exploitation. This information is relevant to the public, including consumers, media, and a wide range of businesses and industries. The report highlights the value of BSA information collected by regulated financial institutions. This document does not introduce a new regulatory interpretation, nor impose any new requirements on regulated entities. The research detailed in this report is one of many examples of how FinCEN and its law enforcement, regulatory, and national security partners may analyze and use BSA reporting, but it is not intended as guidance for financial institutions. For formal guidance to financial institutions on reporting elder financial exploitation incidents, please refer to FinCEN's resource page on advisories, at <https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets>.

Executive Summary: FinCEN analysis of elder financial exploitation Suspicious Activity Reports (SARs) filed between October 2013 and August 2019 indicates elders face an increased threat to their financial security by both domestic and foreign actors.

- Total numbers of filings and total suspicious activity amounts increased 20 percent and 30 percent, respectively, each year during the time period.^a
- Money Services Business (MSB) reporting indicated elders fell victim to scams in which they sent money overseas, most often to receivers in African and Asian countries.
- Depository institution and securities and futures reporting identified family members and caregivers as most often responsible for theft from elders.

Scope and Methodology: FinCEN examined elder financial exploitation SARs filed between October 2013 and August 2019 to determine trends. The full data set consisted of 298,601 SARs. For portions of this report, FinCEN also analyzed a randomly selected, statistically representative sample of SAR narratives from elder financial exploitation filings between October 2013 and September 2017.

a. Calculations based on partial data through August 2019.

EXHIBIT 3-A

FinCEN Financial Trend Analysis

Elder Financial Exploitation Received Increased Filer Attention

Elder financial exploitation SAR filings increased dramatically over the six-year study period, reaching a peak of nearly 7,500 filings per month in August 2019. This potentially reflects an increase in elder financial exploitation activity, perhaps driven by an increase in the elder population and attention drawn to the issue by state legislatures and federal agencies. For example, the National Conference of State Legislatures reported that 36 states, the District of Columbia, and Puerto Rico addressed elder financial exploitation in their 2018 legislative sessions, up from 33 states in 2016.^b At the federal level, the Consumer Financial Protection Bureau (CFPB) published an updated advisory for financial institutions in July 2019, and, prior to that, a joint memorandum with FinCEN in August 2017, on how to detect and respond to this issue.^{c,d} In cooperation with FinCEN, the CFPB also published a report on elder financial exploitation SAR trends in February 2019.^e The Department of Justice orchestrated several law enforcement “sweeps” of elder financial fraud cases in 2018 and 2019.^f All of these events may have influenced financial institutions’ awareness of elder financial exploitation issues, and their reporting of it in SARs.

MSBs and depository institutions accounted for the majority of the filings and of the increase, while casino, insurance company, securities and futures, and “other” filers’ reporting trended upward, but accounted for substantially fewer filings per month. Depository institution and securities and futures SARs saw a steady upward filing trend, while MSB SAR filings trended down in 2018 and early 2019.

- MSB SAR filings fluctuated over the time period, with the highest number reported in 2016 and 2017, averaging over 2,000 per month. This compared with fewer than 1,000 per month in 2013 and 2014, and fewer than 2,000 per month in late 2018 to early 2019. This was not attributable to a single large filer.
- Depository institutions’ filings saw a steady upward trend between 2013 and 2019, with 3,000 to 4,000 filed per month in 2019, compared with 1,000 to 2,000 filed per month in 2013 and 2014.
- Securities and futures filings also saw a steady upward trend between 2013 and 2019, with 50 to 100 filed per month in 2013, compared with 200 to 250 filed per month in late 2019.

b. “Financial Crimes Against the Elderly 2018 Legislation,” The National Conference of State Legislatures Press Release, 3 January 2019, <http://www.ncsl.org/research/financial-services-and-commerce/financial-crimes-against-the-elderly-2018-legislation.aspx>, accessed 26 November 2019.

c. “Reporting of Suspected Elder Financial Exploitation by Financial Institutions,” Consumer Financial Protection Bureau (CFPB), July 2019, https://files.consumerfinance.gov/f/documents/cfpb_suspected-elder-financial-exploitation-financial-institutions_report.pdf, accessed 26 November 2019.

d. “Memorandum on Financial Institution and Law Enforcement Efforts to Combat Elder Financial Exploitation,” Consumer Financial Protection Bureau (CFPB) and Financial Crimes Enforcement Network (FinCEN), August 2017, https://www.fincen.gov/sites/default/files/2017-08/8-25-2017_FINAL_CFPB%2BTreasury%2BFinCEN%20Joint%20Memo.pdf, accessed 26 November 2019.

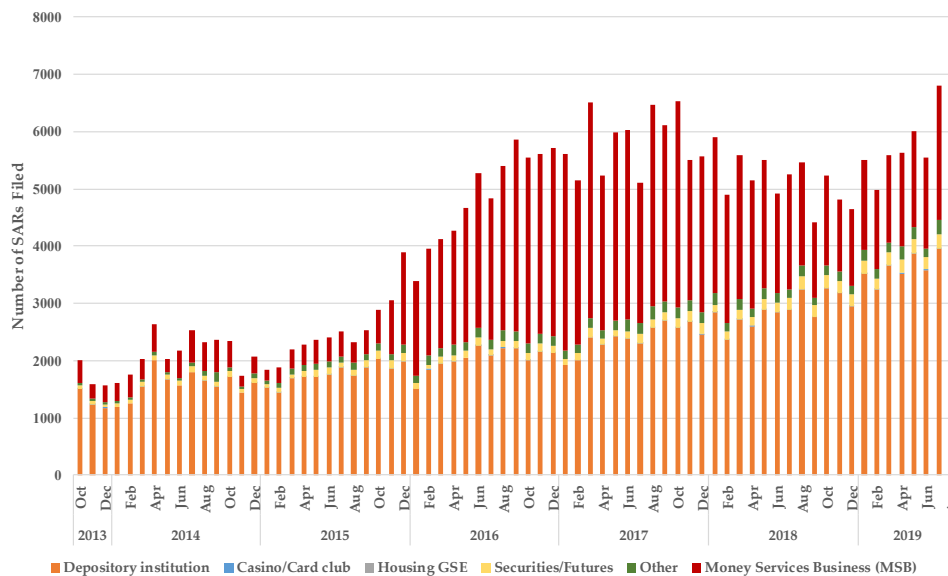
e. “Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends,” Consumer Financial Protection Bureau (CFPB), February 2019, https://files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf, accessed 26 November 2019.

f. “Justice Department Coordinates Largest-Ever Nationwide Elder Fraud Sweep,” U.S. Department of Justice Press Release, 7 March 2019, <https://www.justice.gov/opa/pr/justice-department-coordinates-largest-ever-nationwide-elder-fraud-sweep-0>, accessed 26 November 2019.

EXHIBIT 3-A

FinCEN Financial Trend Analysis

Figure 1. Monthly Elder Financial Exploitation Filings Approach 7,500 in August 2019



Yearly Suspicious Activity Amounts Potentially Indicate Rising Elder Threat

The yearly dollar amount of suspicious activity reported for elder financial exploitation also trended upward during the study period, potentially indicating increased financial threat to elders. In 2014, the total suspicious activity amount reported was \$2.2 billion. In 2019, with only a partial year of data, the total amount rose to \$5 billion through August. Suspicious activity reported in elder financial exploitation SARs amounted to \$21.8 billion for the period between October 2013 and August 2019. The suspicious activity amount reported may reflect the amount at risk of being lost, or an actual loss to an individual or financial institution, depending on how the filer reports.

Figure 2. Elder Financial Exploitation Suspicious Activity Amounts by Year

Time-period	Suspicious Activity Amount Total
October 2013-December 2013	\$821,928,748
2014	\$2,205,167,799
2015	\$2,243,662,333
2016	\$2,983,001,672
2017	\$4,802,762,284
2018	\$3,738,805,523
January 2019-August 2019	\$5,048,710,020
	Total: \$21,844,038,379

December 2019

3

EXHIBIT 3-A

FinCEN Financial Trend Analysis

The yearly average total suspicious activity amount reported per SAR fluctuated over time, with the highest average amount of \$70,809 reported for 2015, and the lowest average amount of \$40,790 reported in 2017. The fluctuation in amounts likely also reflects the fluctuation in SARs filed by MSBs, which have a lower filing threshold than other industries.^g

Figure 3. Elder Financial Exploitation Average Total Suspicious Activity Amount per SAR by Year^h

Year	2013	2014	2015	2016	2017	2018	2019
Average Total Suspicious Activity Amount per SAR	\$63,119	\$66,806	\$70,809	\$47,657	\$40,790	\$54,756	\$62,232

Scams and Theft are Main Threats to Elders

SAR narratives indicate that elder financial exploitation most often involves money transfer scams conducted through MSBs and theft perpetrated through depository and securities and futures institutions.ⁱ Filers also categorized 17 percent of SARs in the sample as elder financial exploitation, but left details of the activity unspecified or vaguely explained. The text and figures in this and subsequent report sections reflect FinCEN's categorization of SARs based on filer language in sample narratives.

- MSBs most often are used to transfer the proceeds of elder fraud, and banking institutions most often are used in theft activity. Of the SARs that FinCEN noted as describing scams, MSBs filed 77 percent and depository institutions filed 21 percent. Of the SARs that FinCEN categorized as describing theft, depository institutions filed 86 percent, securities and futures filed 5 percent, MSBs filed 5 percent, and "Other" filed 3 percent.
- Of the securities and futures SARs in the sample, 73 percent reported theft, 9 percent reported scam activity, 9 percent reported physical abuse, and the remaining 9 percent did not specify the activity.

g. Depending on the type of MSB and transaction, the threshold for filing is either \$2,000 or \$5,000, versus \$5,000 to \$25,000, depending on the circumstances, for depository institutions.

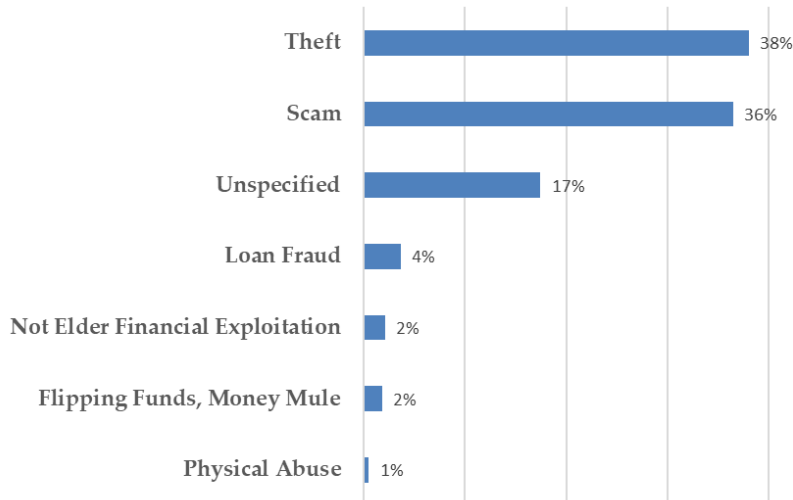
h. The average total suspicious activity amounts per SAR in the table come from partial data in years 2013 and 2019.

i. The SAR narratives forming the basis for this analysis are a statistically representative sample from elder financial exploitation filings between October 2013 and September 2017.

EXHIBIT 3-A

FinCEN Financial Trend Analysis

Figure 4. Suspicious Activity Breakdown in Sample SAR Narratives



Elder Fraud Victims Often Transfer Funds Overseas through MSBs

SAR narratives indicated that elders most often fell victim to lottery, person-in-need, and romance scams, and sent their money abroad to receivers with whom the elders had no in-person relationship, or whom the filer did not identify. Elders most often used MSBs to send money transfers to scammers.

- Of the scam-related SARs, 66 percent reported elders transferring money to a receiver in a foreign location; 44 percent lacked relationship details between the elder and money transfer receiver; and 31 percent reported no in-person relationship with the scammer.
- Filers recorded elder victims sending money transfers in amounts as small as \$500 to as large as \$513,855 (aggregated over time and location).
- The average activity amount in the scam-related SARs was \$25,432, while the median was \$6,105.

Some especially useful SARs described not only how scammers reached victims, but also provided details that offered insight into how the perpetrators manipulated their victims. Filers reported both their suspicions of a client being scammed and when law enforcement, a family member, or victim contacted the filing institution to report a scam. Examples of useful descriptions from filers follow.

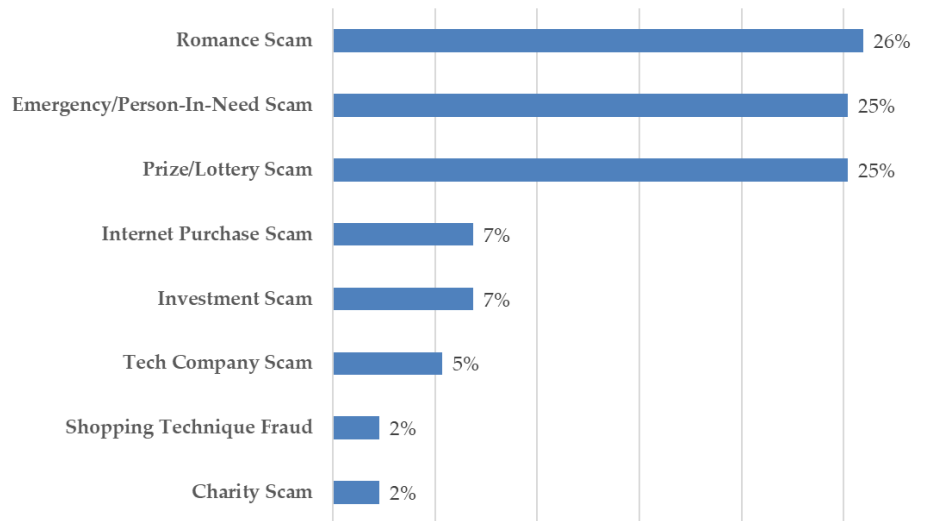
- An MSB reported it suspected a money transfer scam and interviewed the victim at the time of the transaction, who stated she was sending the money to a family member to meet financial needs. The MSB then received a call days later from the victim, who admitted she received a call indicating she won a prize, was sending funds to pay taxes on it, and was coached to lie about her relationship with the receiver and the purpose of the transaction.

EXHIBIT 3-A

FinCEN Financial Trend Analysis

- A teller working at an MSB observed that a customer was attempting to hurriedly send money to an African country and, after asking him relevant questions, advised against sending the money. The customer expressed concern that he was a fraud victim, but sent the money anyway. He returned later that day to disclose that he was a scam victim, had believed a family member was in Africa because of an email he had received, but had confirmed this was untrue since sending the money. His money could not be recalled.

Figure 5. Types of Elder Scams Described in SARs



Most Prevalent Elder Scams in SAR Narratives

Romance: Scammers establish a romantic relationship with their victims and then request money for “hardships” they experience, or to “visit” the victim (but never do).

Emergency/Person-in-need: Scammers prey on victims’ emotional vulnerability by claiming to be a loved one who needs money quickly to help with an emergency.

Prize/Lottery: Scammers coerce their victims into sending an “import tax” or “fee” in order to receive the money they have supposedly won in a lottery.

The Department of Justice Transnational Elder Fraud Strike Force [provided descriptions](#) of additional common scam typologies to which seniors fall victim.

EXHIBIT 3-A

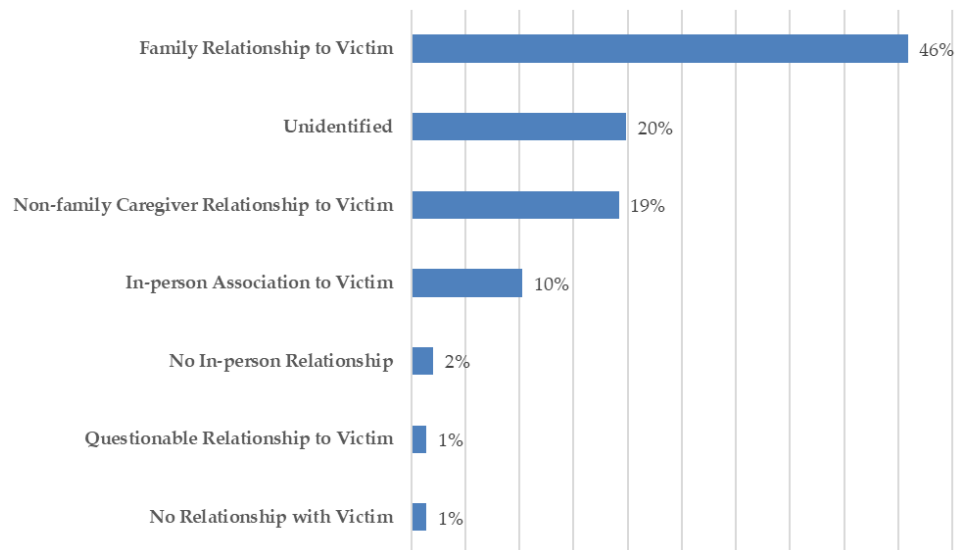
FinCEN Financial Trend Analysis

Elder Fraud Involving Theft Often Committed by Trusted Persons

Sample narratives indicated family members and non-family member caregivers most often stole from elders, indicating elders' finances are most vulnerable to theft from individuals they know or rely on for their well-being. Reporting also frequently identified banking clients as suffering from some type of incapacitation, such as dementia or paralysis. SARs indicate the average amounts reported for theft were more than double that for scams.

- Amounts stolen or at risk of being stolen ranged from \$52 to \$1,186,437 (aggregated), with \$50,084 as the average activity amount and \$15,964 as the median amount.
- SARs indicated that theft by family members and caregivers often occurred over time in relatively small amounts, but totaled amounts that likely represented a major portion of an elder person's wealth.

Figure 6. Family Members Are Most Often Involved in Reported Elder Theft



Losses are Potentially Devastating to Elders

When suspicious activity amounts represent actual loss to an individual, FinCEN assesses they reflect substantial financial hardship for elders. As reported above, the median suspicious activity amount from the sample scam-related SARs was \$6,105, and for theft-related SARs it was \$15,964.

- These amounts represent 16 and 41 percent, respectively, of the \$38,515 that the U.S. Census Bureau reported as the median income of households maintained by individuals 65 and over in 2015.
- Excluding equity in a home, these amounts represent 11 percent and 28 percent, respectively, of the median net worth of households maintained by individuals aged 65 years and over, according to median figures the U.S. Census Bureau calculated for 2013.

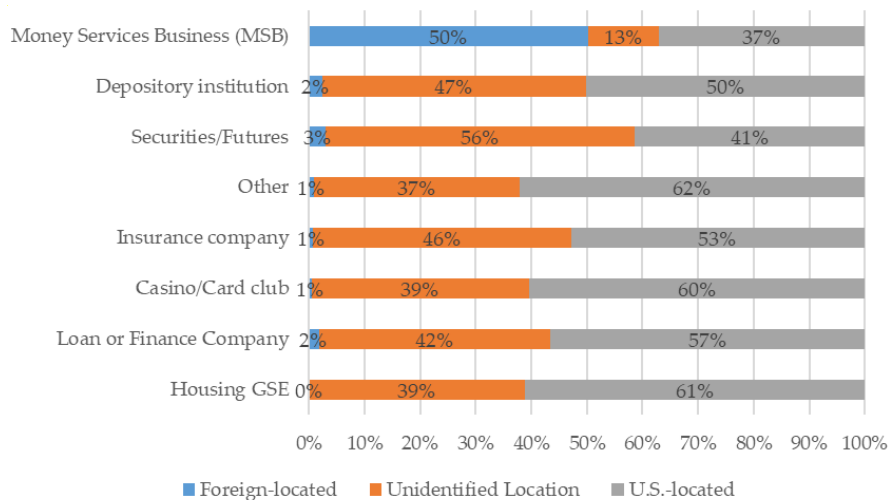
EXHIBIT 3-A

FinCEN Financial Trend Analysis

Foreign Scammers, Domestic Thieves

For the total SAR population studied, the majority of MSB SAR subjects were foreign-located, while a majority of subjects filed on by all other industries were U.S.-located. This corroborated the narrative findings that scam victims sent money abroad through MSBs. MSB filings identified 50 percent of subjects with foreign address locations. Depository institution filings identified 50 percent of subjects with foreign address locations. Depository institution filings identified 50 percent of subjects with U.S. addresses, and other industries' subjects ranged from roughly 40 to 60 percent U.S. addresses.

Figure 7. Subject Location by Filing Institution Type (measured as a percentage)



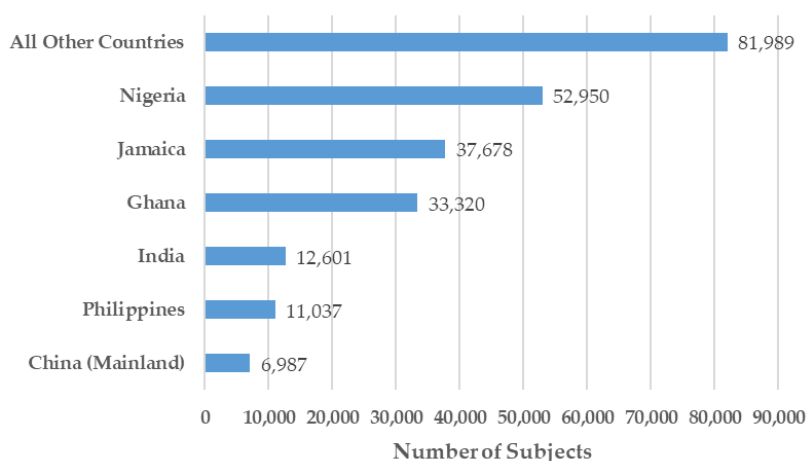
MSB SAR Subjects Located in Africa and Asia

The largest numbers of MSB SAR subjects were located in African and Asian countries, likely indicating most scammers operate, or at least conduct the money-receiving part of their schemes, in these locations. Scammers operating in foreign countries benefit from money transfers that are immediately available and received in cash, which prevents recall of the money when fraud is reported. Furthermore, U.S. law enforcement cannot easily pursue scammers who live and operate abroad.

EXHIBIT 3-A

FinCEN Financial Trend Analysis

Figure 8. Top Foreign-located Subject Countries in MSB Filings (full dataset)^j



FinCEN Collaborates to Protect Elders from Financial Exploitation

FinCEN has collaborated, and will continue to do so, with other governmental bodies, financial institutions, and the public to identify, prevent, and combat elder financial exploitation. Financial institutions are a front line of defense against elders being exploited financially and most routinely issue information about fraud to their clients. Additionally, employees of financial institutions may be well-situated to caution seniors against potentially exploitative transactions, which could help prevent financial losses to elders.^k Financial institutions also are often positioned to report concerns to local adult protective services and law enforcement offices, in addition to filing SARs, without necessarily disclosing the existence of SARs. FinCEN cannot overstate the usefulness of SAR information from financial institutions to generate leads for governmental enforcement agencies, such as the Department of Justice and state and local law enforcement agencies. Elder related SARs also are invaluable for regulatory customers, such as the CFPB and the bank and broker-dealer regulators, who often are able to provide research insights and industry-specific guidance to financial institutions.

What the Public Can do to Combat Elder Financial Exploitation

FinCEN strongly encourages elders, if they suspect that they have been victims of financial exploitation, to report the incident to their financial institution, local law enforcement, and local adult protective services officials. Victims also can report the incident to federal authorities, as it could become important evidence in a larger federal law enforcement case. Financial

j. In the graph, “all other countries” consists of 211 countries. Graph also excludes subjects located in the U.S. and where a location was unidentified.

k. “Exposed to scams: What separates victims from non-victims,” Financial Industry Regulatory Authority, September 2019, https://www.finrafoundation.org/sites/finrafoundation/files/exposed-to-scams-what-separates-victims-from-non-victims_0_0.pdf, accessed 26 November 2019.

EXHIBIT 3-A

FinCEN Financial Trend Analysis

exploitation is a crime and no victim should feel too embarrassed about the circumstances under which they lose money to report it to those who can assist them or catch the perpetrators. The following are government resources where victims can report crime:

- The Department of Justice has an [interactive tool](#) for elders who have been financially exploited to help determine to which agency they should report their incident.
- The Federal Bureau of Investigation's Internet Crime Complaint Center receives complaints at this [website](#) or by calling 1-800-225-5324.
- The Federal Trade Commission has a [website](#) and a phone number (1-877-382-4357) where victims can file complaints that then are made available to law enforcement.

FinCEN also encourages those who care for or work with elderly or vulnerable persons to be mindful of the risks to such persons' finances and to avail themselves of resources supplied by governmental bodies. Below are government resources available for elders who have been financially exploited and for those who work with elders.

- The Administration for Community Living, part of the Department of Health and Human Services, has an [excellent resource](#) for finding services specifically for elders and their families.
- The Consumer Financial Protection Bureau website has [information](#) on how to protect older adults from fraud and financial exploitation.
- FINRA published [a report](#) created in collaboration with the BBB Institute for Marketplace Trust, the Stanford Center on Longevity, and the Federal Trade Commission that explored how cognitive and behavioral variables are often the difference between scam victims and non-victims.



FinCEN ADVISORY

FIN-2020-A002

May 18, 2020

Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)

Detecting, preventing, and reporting COVID-19-related scams and illicit activity is critical to our national security, safeguarding legitimate relief efforts, and protecting innocent people from harm.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**COVID19 FIN-2020-A002**" and select SAR field 34(z) (Fraud-other). Additional guidance for filing SARs appears near the end of this advisory.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to rising medical scams related to the COVID-19 pandemic. This advisory contains descriptions of COVID-19-related medical scams, case studies, red flags, and information on reporting suspicious activity.¹

This is the first of several advisories FinCEN intends to issue concerning financial crimes related to the COVID-19 pandemic. These advisories are based on FinCEN's analysis of COVID-19-related information obtained through public reports, Bank Secrecy Act (BSA) data, and law enforcement partners. FinCEN will issue financial analyses and intelligence, as appropriate, to financial institutions to help them detect, prevent, and report suspected illicit activity.² Additionally, FinCEN has temporarily expanded its Rapid Response Program, which supports law enforcement and financial institutions in the recovery of funds stolen via fraud, theft, and other financial crimes related to COVID-19.

1. While this advisory focuses on medical-related scams, financial institutions should note that criminal actors may use similar fraudulent methods involving non-medical-related goods or services. Many COVID-19-related scams are similar to those observed before the pandemic, and illicit actors have modified their schemes to take advantage of, and profit from, the pandemic by victimizing innocent people and businesses.
2. For up-to-date information on FinCEN COVID-19-related releases, please visit FinCEN Coronavirus Updates at <https://www.fincen.gov/coronavirus>.

FINCEN ADVISORY

Financial Red Flag Indicators of COVID-19 Fraudulent Activity

BSA data, as well as information from other federal agencies, foreign government partners, and public sources indicate possible illicit activities related to the COVID-19 pandemic regarding (1) fraudulent cures, tests, vaccines, and services; (2) non-delivery scams; and (3) price gouging and hoarding of medical-related items, such as face masks and hand sanitizer. FinCEN identified the following red flag indicators to help financial institutions identify COVID-19-related medical scams, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic.

As no single red flag is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple indicators, before determining if a transaction is suspicious or otherwise indicative of fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate. Some of these red flags are common indicators of fraudulent merchant activity committed by shell or fraudulent retail or wholesale business operators. Additionally, some of the red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities.









Medical-Related Frauds, Including
Fraudulent Cures, Tests, Vaccines, and Services

Several federal agencies have detected fraudulent COVID-19-related cures, tests, vaccines, and associated services being offered to the public.³ Examples of fraudulent medical services include claims related to purported vaccines or cures for COVID-19, claims related to products that purportedly disinfect homes or buildings, and the distribution of fraudulent or unauthorized at-home COVID-19 tests. Some of these scams may be perpetrated by illicit actors who recently formed unregistered or unlicensed medical supply companies. Financial indicators of these scams may include:

3. See Department of Justice (DOJ) Press Release, "[Georgia resident arrested for selling illegal products claiming to protect against viruses](#)," (April 9, 2020); U.S. Department of Homeland Security News Release, "[ICE HSI arrests Georgia resident for selling illegal pesticide, claiming it protects against coronavirus](#)," (April 14, 2020); U.S. Customs and Border Protection (CBP) National Media Release, "[CBP Officers Seize Fake COVID-19 Test Kits at LAX](#)," (March 14, 2020); FTC Press Release, "[FTC, FDA Send Warning Letters to Seven Companies about Unsupported Claims that Products Can Treat or Prevent Coronavirus](#)," (March 9, 2020); and Federal Bureau of Investigation (FBI) Press Releases, "[FBI Warns of Emerging Health Care Fraud Schemes Related to COVID-19 Pandemic](#)," (April 13, 2020); and "[FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment](#)," (March 27, 2020).

EXHIBIT 3-A

FINCEN ADVISORY

-  1 U.S. authorities, such as the Federal Trade Commission (FTC), the Food and Drug Administration (FDA), or the DOJ, have identified the company, merchant, or business owners as selling fraudulent products.⁴
-  2 A web-based search or review of advertisements indicates that a merchant is selling at-home COVID-19 tests,⁵ vaccines, treatments, or cures.
-  3 The customer engages in transactions to or through personal accounts related to the sale of medical supplies, which could indicate that the selling merchant is an unregistered or unlicensed business or is conducting fraudulent medical-related transactions.
-  4 The financial institution's customer has a website with one or more indicia of suspicion, including a name/web address similar to real and well-known companies, a limited internet presence, a location outside of the United States, and/or the ability to purchase pharmaceuticals without a prescription when one is usually required.
-  5 The product's branding images found in an online marketplace appear to be slightly different from the legitimate product's images, which may indicate a counterfeit product.
-  6 The merchant is advertising the sale of highly sought-after goods related to the COVID-19 pandemic and response at either deeply discounted or highly inflated prices.
-  7 The merchant is requesting payments that are unusual for the type of transaction or unusual for the industry's pattern of behavior. For example, instead of a credit card payment, the merchant requires a pre-paid card, the use of a money services business, convertible virtual currency, or that the buyer send funds via an electronic funds transfer to a high-risk jurisdiction.
-  8 Financial institutions might detect patterns of high chargebacks and return rates in their customer's accounts. These patterns can be indicative of merchant fraud in general.

[Case Study: U.S. Authorities Take Action Against Fraudulent COVID-19 Tests and Treatments](#)






4. For current lists of COVID-19-related warning letters and fraudulent products, visit FDA: "[Fraudulent Coronavirus Disease 2019 \(COVID-19\) Products](#)" and FTC: "[FTC Coronavirus Warning Letters to Companies](#)." For information pertaining to COVID-19-related DOJ actions, visit: "[Coronavirus Fraud News](#)."
5. At the time of this publication, the FDA has authorized three at-home tests: the "LabCorp COVID-19 RT-PCR," the Rutgers Clinical Genomics Laboratory's molecular Laboratory Developed Test, and the Everlywell COVID-19 Test Home Collection Kit. See FDA News Release, "[Coronavirus \(COVID-19\) Update: FDA Authorizes First Test for Patient At-Home Sample Collection](#)," (April 21, 2020); FDA News Release, "[Coronavirus \(COVID-19\) Update: FDA Authorizes First Diagnostic Test Using At-Home Collection of Saliva Specimens](#)," (May 8, 2020); and FDA News Release, "[FDA Authorizes First Standalone At-Home Sample Collection Kit that can be used with Certain Authorized Tests](#)," (May 16, 2020).

EXHIBIT 3-A

FINCEN ADVISORY

Non-Delivery Fraud of Medical-Related Goods Scams

The COVID-19 pandemic has disrupted global shipping and created sudden and substantial demand for certain goods, especially medical-related goods. This demand creates a situation where criminals may defraud consumers and companies through non-delivery of merchandise. In these non-delivery scams, a customer pays a company for goods the customer will never receive. These bogus companies advertise test kits, masks, drugs, and other goods they never intend to deliver, and sometimes never possess at all. Victims can include unsuspecting companies, hospitals, governments, and consumers. These fraudulent transactions occur through websites, robocalls, or on the Darknet. Some schemes involve shell companies⁶ to facilitate transactions. In its March 27, 2020 warning to the health care industry, the FBI asked the medical community to exercise due diligence and appropriate caution when dealing with unfamiliar vendors and when relying on unidentified third-party brokers in the supply chain.⁷ Financial indicators of these scams may include:





-  The merchant does not appear to have a lengthy corporate history (e.g., the business was established within the last few months), lacks physical presence or address, or lacks an Employer Identification Number. Additionally, if the merchant has an address, there are noticeable discrepancies between the address and a public record search for the company or the street address, multiple businesses at the same address, or the merchant is located in a high-risk jurisdiction or a region that is not usually associated with the merchandise they are selling.
-  Searches in corporate databases reveal that the merchant's listing contains a vague or inappropriate company name, multiple unrelated names, a suspicious number of name variations, multiple "doing business as" (DBA) names, or does not align with its business model.
-  Merchants are reluctant to provide the customer or the financial institution that is processing the transactions with invoices or other documentation supporting the stated purpose of trade-related payments.
-  The financial institution does not understand the merchant's business model, and has difficulty determining the true nature of the company and its operations.
-  The merchant cannot provide shipment-tracking numbers to the customer or proof of shipment to a financial institution so it may process related financial transactions.

6. Shell companies are defined as non-publicly traded corporations or limited liability companies (LLCs) that have no physical presence beyond a mailing address and generate little to no independent economic value. See FinCEN Guidance, [FIN-2006-G014](#) "Potential Money Laundering Risks Related to Shell Companies," (November 2006); and Suspicious Activity Reports (SAR) Activity Review: [Issue 1](#) (October 2000), [Issue 2](#) (June 2001), and [Issue 7](#) (August 2004).

7. See FBI Press Release, "[FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment](#)," (March 27, 2020).

EXHIBIT 3-A

FINCEN ADVISORY

-  14 The merchant claims several last minute and suspicious delays in shipment or receipt of goods. For example, the merchant claims that the equipment was seized at port or by authorities, that customs has not released the shipment, or that the shipment is delayed on a vessel and cannot provide any additional information about the vessel to the customer or their financial institution.
-  15 The merchant cannot explain the source of the goods or how the merchant acquired bulk supplies of highly sought-after goods related to the COVID-19 pandemic.
-  16 Domestic or foreign governments have identified the merchant or its owners/incorporators as being associated with fraudulent and criminal activities.
-  17 A newly-opened account receives a large wire transaction that the accountholder failed to mention during the account opening process.

[Case Study: A Virginia Financial Institution Alerted the U.S. Secret Service \(USSS\) and Successfully Helped Prevent a \\$317 Million Non-Delivery Scam](#)

Price Gouging and Hoarding of Medical-Related Items






FinCEN and DOJ have received numerous reports of suspected hoarding and price gouging related to the COVID-19 pandemic. DOJ established the Hoarding and Price Gouging Task Force on March 24, 2020, to address COVID-19-related market manipulation, hoarding, and price gouging. According to DOJ, hoarding and price gouging are defined as the act by any person or company of accumulating an unreasonable amount of any of these materials for their personal use, or accumulating any of these materials for purposes of selling them far above prevailing market prices.⁸ In many cases, individuals have been selling surplus items or newly acquired bulk shipments of goods, such as masks, disposable gloves, isopropyl alcohol, disinfectants, hand sanitizers, toilet paper, and other paper products at inflated prices because of the COVID-19 pandemic. Payment methods vary by scheme and can include the use of pre-paid cards, money services businesses, credit card transactions, wire transactions, or electronic fund transfers. On March 23, 2020, President Trump issued Executive Order (E.O.) 13910, pursuant to section 102 of the Defense Production Act, which prohibits hoarding of designated items.⁹ Financial indicators of these scams may include:

8. See DOJ, "[Department of Justice COVID-19 Hoarding and Price Gouging Task Force](#)," (March 24, 2020).

9. See E.O. 13910, "[Executive Order on Preventing Hoarding of Health and Medical Resources to Respond to the Spread of COVID-19](#)," (March 23, 2020). The E.O. does not define hoarding. The E.O. delegates the authority to prevent hoarding to the Secretary of Health and Human Services and to designate materials "the supply of which would be threatened by persons accumulating the material either in excess of reasonable demands of business, personal, or home consumption, or for the purpose of resale at prices in excess of prevailing market prices." Furthermore, the Attorney General of the United States stated that the "Department will investigate and prosecute those who acquire vital medical supplies in excess of what they would reasonably use or for the purpose of charging exorbitant prices to the healthcare workers and hospitals who need them." See DOJ, "[Department of Justice COVID-19 Hoarding and Price Gouging Task Force](#)," (March 24, 2020).

EXHIBIT 3-A

F I N C E N A D V I S O R Y

-  In addition to the use of personal accounts for business purposes (*see* indicator number 3 above), a customer begins using their personal accounts for business-related transactions after January 2020, and sets up a medical supply company or is selling highly sought-after COVID-19-related goods online, such as hand sanitizer, toilet paper, masks, and anti-viral or disinfectant cleaning supplies.
-  The customer begins using their money services or bank account differently. For example, prior to January 2020, the customer never linked their account to the sale of goods on the internet. Since the COVID-19 pandemic began, however, the customer is receiving deposits with payment messages indicating that they are for the sale of medical goods, disinfectants, sanitizers, and paper products sold on the internet.
-  The customer's accounts are receiving or sending electronic fund transfers (EFT) to/from a newly established company that has no known physical or internet presence.
-  The customer's account is used in transactions for COVID-19-related goods, such as masks and gloves, with a company that is not a medical supply distributor, is involved in other non-medical-related industries, or is not known to have repurposed its manufacturing to create medical-related goods. For example, the company is currently selling medical and sanitary supplies, and prior to January 2020, the company was listed as an automotive shop, a lumberyard, or a restaurant.
-  The customer makes unusually large deposits that are inconsistent with the customer's profile or account history. Upon further investigation, the customer states, or open-source research indicates, that the customer was selling COVID-19-related goods not usually sold by the customer.

[Case Study: FBI Arrests Brooklyn Man for Possession and Sale of Scarce Medical Equipment](#)

EXHIBIT 3-A

FINCEN ADVISORY

Case Studies¹⁰

Medical-Related Frauds, Including Fraudulent Cures, Tests, Vaccines, and Services¹¹

U.S. Authorities Take Action Against Fraudulent COVID-19 Tests and Treatments

On March 12, 2020, CBP officers at Los Angeles International Airport (LAX) intercepted a package containing suspected counterfeit or fraudulent COVID-19 test kits arriving from the United Kingdom (U.K.). The officers found six plastic bags containing various vials manifested as “Purified Water Vials,” and filled with a white liquid labeled as “Corona Virus 2019nconv (COVID-19)” and “Virus1 Test Kit.”¹² The seizure triggered a joint U.S.-U.K. investigation and additional seizures.¹³

In a separate case, DOJ charged and arrested a U.K. national for shipping from the U.K. to California and Utah mislabeled drugs purported to be a COVID-19 treatment. In the scheme, the fraudster created packages labeled “Trinity COVID-19 SARS Antipathogenic Treatment” kits, even though the kits had not been approved by the FDA to treat COVID-19 or for any other use. This matter was investigated jointly by the FDA’s Office of Criminal Investigation and Homeland Security Investigations, with assistance from CBP and the United States Postal Inspection Service.¹⁴

10. See Financial Action Tasks (FATF) publication, “[COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses](#),” (May 2020), which identifies FATF countries’ challenges, good practices, and policy responses to money laundering and terrorist financing threats and vulnerabilities arising from the COVID-19 pandemic.
11. Other U.S. law enforcement actions include COVID-19-related arrests made by the law enforcement partners of the National Intellectual Property Rights Coordination Center (IPR Center). These arrests related to shipping mislabeled and unapproved “treatments” for patients suffering from COVID-19. See IPR Center [Newsroom](#), DOJ Press Release, “[U.K. National Charged with Shipping Mislabeled and Unapproved ‘Treatments’ for Patients Suffering from COVID-19](#),” (April 1, 2020), and FDA, “[Coronavirus Disease 2019 \(COVID-19\)](#).” During a weeklong operation held March 3-10, 2020, INTERPOL, the World Customs Organization (WCO), and Europol, in collaboration with United States and partners, seized more than 37,000 counterfeit medical devices, counterfeit surgical masks, and illicit pharmaceuticals, and they identified more than 2,000 websites with false advertisements and online marketplaces selling counterfeit goods. See INTERPOL News, “[Global operation sees a rise in fake medical products related to COVID-19](#),” (March 19, 2020), and WCO Newsroom, “[COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment](#),” (March 23, 2020).
12. See CBP National Media Release, “[CBP Officers Seize Fake COVID-19 Test Kits at LAX](#),” (March 14, 2020).
13. See WCO Newsroom, “[COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment](#),” (March 23, 2020).
14. See DOJ Press Release, “[U.K. National Charged with Shipping Mislabeled and Unapproved ‘Treatments’ for Patients Suffering from COVID-19](#),” (April 1, 2020).

FINCEN ADVISORY

Non-Delivery Fraud Scams

A Virginia Financial Institution Alerted the U.S. Secret Service (USSS) and Successfully Helped Prevent a \$317 Million Non-Delivery Scam

A foreign government contacted a reliable New York-based law firm for help procuring 30-50 million N95 masks for the foreign country's national police department. The New York firm reached out to a healthcare/telemedicine telemarketing company (Company A), which in turn reached out to Company B, purportedly representing "a conglomerate of doctors" that had purchased millions of masks. Company B supplied Company A with contracts falsely claiming that Company B had 50 million masks stored in a warehouse in Houston, Texas, and requiring a payment of \$317 million into an escrow account.

To execute the transactions, the foreign government sent \$317 million to New York for further transfer to Company A's account held at a Virginia financial institution. The Virginia financial institution became suspicious that Company A's account had only been opened the previous day, and the account owner never mentioned to the financial institution that the owner was expecting a \$317 million wire transaction. The Virginia financial institution contacted the USSS.

The USSS reviewed BSA data and interviewed the accountholder for Company A. The investigation revealed that, although Company A had suspicions about Company B, Company A appeared to be a victim, hired as a "broker" for the \$317 million non-delivery scam. USSS interviewed the Chief Executive Officer (CEO) of Company B who admitted that there were no masks and that he never had possession of 50 million masks.

Price Gouging and Hoarding of Medical-Related Items

FBI Arrests Brooklyn Man for Possession and Sale of Scarce Medical Equipment

On March 30, 2020, FBI agents arrested a resident of Brooklyn, New York, for lying to them about his hoarding and sale of surgical masks, medical gowns, and other medical supplies.¹⁵

The individual allegedly sold certain designated materials, including N95 respirators, to doctors and nurses at inflated prices. In one instance, a doctor in New Jersey contacted the individual via a WhatsApp chat group labeled "Virus2020!" The individual agreed to sell to the doctor approximately 1,000 N95 masks and other assorted materials for \$12,000, an approximately 700 percent markup from the normal price charged for those materials. The individual directed the doctor to an auto repair shop in Irvington, New Jersey, to pick up the order. According to the doctor, the repair shop contained enough materials, including hand sanitizers, disinfecting products, chemical cleaning supply agents, and surgical supplies, to outfit an entire hospital. In another instance, the individual allegedly offered to sell surgical gowns to a nurse and directed the nurse to his residence in Brooklyn.

15. See DOJ Press Release, "[Brooklyn Man Arrested for Assaulting FBI Agents and Making False Statements About His Possession and Sale of Scarce Medical Equipment](#)," (March 30, 2020).

FINCEN ADVISORY

Information on Reporting Suspicious Activity*Suspicious Activity Report (SAR) Filing Instructions*

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying possible financial crimes related to the COVID-19 pandemic, as well as unrelated frauds and financial crimes associated with foreign and domestic political corruption, money laundering, terrorist financing, and other illicit finance. Financial institutions should provide all pertinent available information in the SAR form and narrative. Adherence to the filing instructions below will improve FinCEN and law enforcement's ability to effectively identify and pull actionable SARs and information from the FinCEN Query systems to support COVID-19-related cases.

- FinCEN requests that financial institutions reference this advisory by including the key term "COVID19 FIN-2020-A002" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- Financial institutions should also select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include the type of fraud and/or name of the scam or product (e.g., Product Fraud – non delivery scam) in SAR field 34(z).
- Please refer to FinCEN's Notice Related to the Coronavirus Disease 2019 (COVID-19) [May 18 Notice Related to COVID-19](#), which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



FinCEN NOTICE

May 18, 2020

Notice Related to the Coronavirus Disease 2019 (COVID-19)

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice as part of FinCEN's COVID-19-related response. This Notice contains pertinent information regarding reporting COVID-19-related criminal and suspicious activity and reminds financial institutions of certain Bank Secrecy Act (BSA) obligations. FinCEN intends to issue multiple COVID-19-related advisories. Each advisory will refer financial institutions to this Notice.

COVID-19-Related Updates to Financial Institutions

FinCEN has published notices on its website that provide information to assist financial institutions in complying with their BSA obligations during the COVID-19 pandemic, which include a direct contact mechanism for urgent COVID-19-related issues. FinCEN encourages financial institutions to monitor FinCEN's website and the Department of the Treasury's website on The Coronavirus Aid, Relief, and Economic Security (CARES) Act for up-to-date information concerning compliance with BSA obligations.¹

BSA Reporting Obligations

Compliance with the BSA remains crucial to protecting our national security by combating money laundering and related crimes, including terrorism and its financing. FinCEN expects financial institutions to continue following a risk-based approach and to diligently adhere to their BSA obligations. FinCEN also appreciates that financial institutions are taking actions to protect employees, their families, and others in response to the COVID-19 pandemic. FinCEN recognizes that current circumstances may create challenges with respect to certain BSA obligations, including the timing requirements for certain BSA report filings. FinCEN will continue outreach to regulatory partners and financial institutions to ensure risk-based compliance with the BSA, and FinCEN will issue additional information as appropriate.²

1. For up-to-date information on FinCEN's COVID-19-related releases, please visit FinCEN's Coronavirus Updates at <https://www.fincen.gov/coronavirus>. Those interested in receiving notifications from FinCEN may sign up for [FinCEN Updates](#), at no charge, to receive updates with links to new information when content is added to FinCEN's website for any of the enrolled user's selected categories. For up-to-date information concerning the Department of the Treasury's CARES Act information, please visit <https://home.treasury.gov/policy-issues/cares>.
2. See FinCEN Notice, "[The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 \(COVID-19\) Pandemic](#)" (April 3, 2020).

EXHIBIT 3-A

FINCEN NOTICE

Financial institutions that wish to communicate their organizational COVID-19-related concerns, such as issues with the timely filing of BSA reports, should go to www.fincen.gov, click on “Need Assistance,” and select “COVID19” in the subject drop-down list.

SAR Filing Instructions

In light of the COVID-19 pandemic, some financial institutions have added COVID-19 statements to their disclaimers or are using SAR narratives to address COVID-19’s impact on their SAR filing abilities. Financial institutions should not include in the SAR narrative their challenges during the pandemic; the SAR narrative should include COVID-19 when it is tied to suspicious activity only. However, filers who have already included references to COVID-19 in matters not related to the pandemic do not need to file corrected reports.

Provision of SAR Supporting Documentation to Law Enforcement and FinCEN

In order to effectively respond to and combat fraud schemes, (e.g. those exploiting the COVID-19 pandemic), law enforcement and FinCEN require full details related to SAR filings, including supporting documentation, as quickly as possible.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.³ Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.⁴ When requested to provide supporting documentation, financial institutions should verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency.

Disclosure of SARs and supporting documentation to appropriate law enforcement and supervisory agencies is protected by the safe harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions.⁵

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving fraud schemes, including those related to COVID-19. Financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information relating to transactions that the institution suspects may

3. See 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), and 1026.320(d).

4. *Id.* See also FinCEN Guidance, [FIN-2007-G003](#), “Suspicious Activity Report Supporting Documentation,” (June 13, 2007).

5. See 31 U.S.C. § 5318(g)(3).

EXHIBIT 3-A

FINCEN NOTICE

involve the proceeds of one or more specified unlawful activities (“SUAs”) and such an institution will still remain protected from civil liability under the section 314(b) safe harbor. The SUAs listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including fraud against individuals or the government. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs.⁶

Reporting COVID-19-Related Criminal Activity

There are a variety of U.S. government agencies positioned to assist in investigating and combating COVID-19-related criminal activity. Financial institutions and their customers should consider reporting COVID-19 crimes to the following agencies:

COVID-19-Related Fraud Schemes: Department of Justice (DOJ) urges the public to report suspected fraud schemes related to COVID-19 by calling the National Center for Disaster Fraud (NCDF) hotline (1-866-720-5721).⁷ The NCDF can receive and enter complaints into a centralized system that can be accessed by all U.S. Attorney Offices, as well as DOJ law enforcement components, to identify, investigate, and prosecute fraud schemes. The NCDF coordinates complaints with 16 additional federal law enforcement agencies, as well as state Attorneys General and local authorities. The public may also report CARES Act-related fraud or other COVID-19-related financial crime to the U.S. Secret Service (USSS) by [contacting their local USSS field office](#). Additionally, Department of Homeland Security (DHS) (including Homeland Security Investigations (HSI) and Immigration and Customs Enforcement) encourages the reporting of COVID-19 financial, cyber, and import/export fraud via the [Operation Stolen Promise website](#) / [intake email address](#).

Cyber- and Internet-related Crime: Federal Bureau of Investigation’s (FBI) Crime Complaint Center (IC3),⁸ the DHS’s CISA [National Cybersecurity Communications and Integration Center \(NCCIC\)](#); and HSI’s [Operation Stolen Promise fraud intake](#).⁹

Identity Theft and Fraud: [The Federal Trade Commission](#) and the Social Security Administration fraud hotline (1-800-269-0271).

Federal Tax Fraud: Fraud involving payment of federal taxes should be reported to the [Treasury Inspector General for Tax Administration](#).

6. For further guidance related to the 314(b) Program, see FinCEN [Fact Sheet](#), “Section 314(b)” (November 2016) and FinCEN Guidance, [FIN-2009-G002](#), “Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act,” (June 16, 2009).

7. See DOJ Press Release, “[Attorney General William P. Barr Urges American Public to Report COVID-19 Fraud](#),” (March 20, 2020).

8. See the FBI’s IC3 website, <https://www.ic3.gov/>.

9. See HSI “Operation Stolen Promise” website, HSI COVID-19 Fraud website, <https://www.ice.gov/topics/operation-stolen-promise>.

EXHIBIT 3-A

FINCEN NOTICE

Response and Recovery of Funds

To better assist the public during the COVID-19 pandemic, FinCEN has temporarily expanded its Rapid Response Program to support law enforcement and financial institutions in the recovery of funds stolen via fraud, theft, and other financial crimes related to COVID-19. FinCEN has already been involved in multiple Rapid Response matters involving allegations of COVID-19 fraud, to include assisting in the recovery of \$300 million in one case. To request immediate assistance in recovering cybercrime- and COVID-19-related stolen funds, financial institutions should file a complaint with the FBI's IC3, contact their local FBI field office, or contact the nearest USSS field office. Contacting law enforcement for fund recovery assistance does not relieve a financial institution from its SAR filing obligations.

FinCEN, in partnership with the FBI, the USSS, HSI, and the U.S. Postal Inspection Service, as well as counterpart Financial Intelligence Units abroad, can help financial institutions recover funds stolen as the result of business email compromise (BEC) and cybercrime schemes through its Rapid Response Program. Through these partnerships, FinCEN has successfully assisted in the recovery of approximately \$900 million with the assistance of 64 countries. While FinCEN does not ensure recovery of BEC stolen funds, FinCEN has achieved greater success in recovering funds when victims or financial institutions report BEC-unauthorized and fraudulently induced wire transfers to law enforcement within 24 hours.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



FinCEN ADVISORY

FIN-2020-A003

July 7, 2020

Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)

Detecting, preventing, and reporting consumer fraud and other illicit activity related to COVID-19 is critical to our national security, safeguarding legitimate relief efforts, and protecting innocent people from harm.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**COVID19 MM FIN-2020-A003**" and select SAR field 34(z) (Fraud - other). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to potential indicators of imposter scams and money mule schemes, which are two forms of consumer fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of imposter scams and money mule schemes, financial red flag indicators for both, and information on reporting suspicious activity.

This advisory is intended to aid financial institutions in detecting, preventing, and reporting potential COVID-19-related criminal activity. This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners. FinCEN will issue COVID-19-related information to financial institutions to help enhance their efforts to detect, prevent, and report suspected illicit activity on its website at <https://www.fincen.gov/coronavirus>, which also contains information on registering to receive [FinCEN Updates](#).

FINCEN ADVISORY

Financial Red Flag Indicators of COVID-19 Imposter Scams and Money Mule Schemes

Consumer frauds include imposter scams and money mule schemes, where actors deceive victims by impersonating federal government agencies, international organizations, or charities. FinCEN identified the financial red flag indicators described below to alert financial institutions to these frauds and to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic.

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple indicators, before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional inquiries and investigations where appropriate. Additionally, some of the financial red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities.

Imposter Scams

In imposter scams, criminals impersonate organizations such as government agencies, non-profit groups, universities, or charities to offer fraudulent services or otherwise defraud victims. While imposter scams can take multiple forms, the basic methodology involves an actor (1) contacting a target under the false pretense of representing an official organization, and (2) coercing or convincing the target to provide funds or valuable information, engage in behavior that causes the target's computer to be infected with malware, or spread disinformation.¹ In the case of schemes connected to COVID-19, imposters may pose as officials or representatives from the Internal Revenue Service (IRS),² the Centers for Disease Control and Prevention (CDC),³ the World Health Organization (WHO), other healthcare or non-profit groups, and academic institutions.⁴

1. See Federal Trade Commission (FTC) Business Blog, "[Seven Coronavirus Scams Targeting Your Business](#)," (March 25, 2020).
2. For information on IRS imposter scams in general, see FTC's "[IRS Imposter Scams Infographic](#)," (January 2020).
3. See Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) Public Service Announcement "[FBI Sees Rise in Fraud Schemes Related to the Coronavirus \(COVID-19\) Pandemic](#)," (March 20, 2020).
4. FTC maintains links to resources concerning scams and the current trends it has observed. See FTC's "[Coronavirus Advice for Consumers](#)."

EXHIBIT 3-A

FINCEN ADVISORY

Illicit actors can use imposter scams to defraud and deceive the vulnerable, including the elderly and unemployed, through the solicitation of payments (such as digital payments and virtual currency), donations, or personal information via email, robocalls, text messages,⁵ or other communication methods. For example, an imposter may contact potential victims by phone, email, or text to imply that the victim must verify personal information or send payments to scammers in return for COVID-19-related stimulus payments or benefits, including Economic Impact Payments (EIP)⁶ under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.⁷ Another instance includes imposters contacting victims and posing as government or health care representatives engaged in COVID-19 contact tracing activities, implying that a victim must share personal or financial information as part of contact tracing efforts.⁸ Multiple examples include phishing schemes, where imposters send communications appearing to come from legitimate sources, to collect victims' personal and financial data and potentially infect their devices by convincing the target to download a malicious attachment or click malicious links.⁹

Scammers may also impersonate legitimate charities or create sham charities, taking advantage of the generosity of the public and embezzling donations intended for COVID-19 response efforts.¹⁰






5. For information about COVID-19-related imposter scams conducted by text messages and phone calls, see the Federal Communications Commission (FCC), ["COVID-19 Consumer Warnings and Safety Tips,"](#) (May 20, 2020). The FTC and the FCC have sent warning letters to multiple Voice over Internet Protocol (VoIP) service providers for allegedly routing illegal pandemic-related scam telemarketing or robocalls. See FTC Press Release, ["FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls,"](#) (May 20, 2020).
6. EIP may take the form of Automated Clearing House (ACH) deposits, U.S. Treasury checks, or prepaid debit cards. See U.S. Department of the Treasury (Treasury) Press Release ["Treasury is Delivering Millions of Economic Impact Payments by Prepaid Debit Card,"](#) (May 18, 2020).
7. The FTC, the IRS, and the Treasury Inspector General for Tax Administration (TIGTA) each published information about imposter scams, particularly as they relate to EIP. See FTC Blog, ["Want to Get Your Coronavirus Relief Check? Scammers do too,"](#) (April 1, 2020) and ["Coronavirus Checks: Flattening the Scam Curve,"](#) (April 8, 2020); IRS News Release, ["IRS Issues Warning About Coronavirus-related Scams; Watch Out For Schemes Tied To Economic Impact Payments,"](#) (April 2, 2020) and the IRS's [Economic Impact Payment Information Center](#), (April 8, 2020); and TIGTA Press Release, ["TIGTA Urges Taxpayers to 'Be On High Alert' For Coronavirus Relief Payment Scams,"](#) (April 7, 2020).
8. See Department of Justice (DOJ) Press Release ["U.S. Attorney Warns Public of COVID-19 Contact Tracing Frauds,"](#) (May 28, 2020).
9. See Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's (U.K.) National Cyber Security Centre (NCSC) Alert, ["COVID-19 Exploited by Malicious Cyber Actors"](#) (April 8, 2020); and DHS, ["Common Scams: Know How to Spot a Fake."](#) Additionally, see WHO Cybersecurity, ["Beware of Criminals Pretending to be WHO,"](#) (April 2020). See also FTC Blog, ["COVID-19 Scams Targeting College Students,"](#) (May 27, 2020); and DOJ Press Release, ["Federal Law Enforcement Encourages the Public to Remain Vigilant to Covid-19 Scams,"](#) (April 22, 2020).
10. Multiple U.S. Attorneys' Offices (USAOs) warn of criminals who may seek to exploit legitimate relief efforts for their own illicit gain by soliciting donations to sham charities or crowdfunding sites. See USAO for the Southern District of Georgia, ["U.S. Attorney Warns of Coronavirus Scams Targeting Vulnerable Victims,"](#) (March 25, 2020); USAO for the Eastern District of Oklahoma, ["Department of Justice Requests Citizens be Aware of And Report COVID-19 Fraud,"](#) (March 24, 2020); and USAO for the Middle District of Tennessee, ["U.S. Attorney and FBI Urge the Public to Report Suspected Fraud Related to Tornado Destruction and COVID-19,"](#) (March 23, 2020). Additionally, the U.S. Securities and Exchange Commission (SEC) noted the potential for charity investment frauds, where actors falsely claim that investments will provide financial support or medical treatment to people in need, with the money instead stolen. See SEC Investor Alerts and Bulletins, ["Frauds Targeting Main Street Investors -- Investor Alert,"](#) (April 10, 2020). See also FTC's information to avoid charity scams, ["Make Your Coronavirus Donations Count,"](#) (May 5, 2020).

EXHIBIT 3-A

FINCEN ADVISORY

Criminals often use social media accounts, door-to-door collections, flyers, mailings, telephone and robocalls, text messages, websites, and emails mimicking legitimate charities and non-profits to defraud the public. These operations may include words like “relief,” “fund,” “donation,” and “foundation” in their titles to give the illusion that they are a legitimate organization.¹¹

Given that many scammers may be targeting customers as opposed to financial institutions directly, financial institutions, when interacting with their customers, should remain on the alert for potential suspicious activities. Financial red flag indicators of imposter scams may include:

-  1 A customer indicating that a person claiming to represent a government agency contacted him or her by phone, email, text message, or social media asking for personal or bank account information to verify, process, or expedite EIPs, unemployment insurance, or other benefits.¹² In particular, be alert to communications emphasizing “stimulus check” or “stimulus payment” in solicitations to the public, sometimes claiming that the fraudulent entity can expedite the “stimulus check” or other government payment on behalf of the beneficiary for a fee paid by gift card or prepaid card.
-  2 Receipt of a document that appears to be a check or a prepaid debit card from the U.S. Treasury, often in an amount less than the expected EIP, with instructions to contact the fraudulent government agency, via a phone number or online, to verify personal information in order to receive the entire benefit.
-  3 Unsolicited communications from purported trusted sources or government programs related to COVID-19, instructing readers to open embedded links or files or to provide personal or financial information, including account credentials (e.g., usernames and passwords).
-  4 Email addresses in COVID-19 correspondence that do not match the name of the sender, contain misspellings, or do not end in the corresponding domain of the organization from which the message allegedly was sent. For example, government agencies will use “.gov” or “.mil.” Many legitimate charities will use “.org.” WHO emails will contain “@who.int.” Fraudsters, however, may use “.com” or “.biz” in place of the expected domain.
-  5 Email correspondence that contains subject lines that government or industry have identified as being associated with phishing campaigns, or that contains embedded links or webpage addresses for purported COVID-19 resources that have irregular URLs (e.g., slight variations in domain extensions like “.com,” “.org,” and “.us”). Examples of U.S. government-identified COVID-19 phishing email subject lines include “2020 Coronavirus Updates,” “Coronavirus Updates,” “2019-nCov: New confirmed cases in your City,” and “2019-nCov: Coronavirus outbreak in your city (Emergency).”¹³



11. See FTC, “[How to Donate Wisely and Avoid Charity Scams](#).”

12. For more information on EIPs, visit IRS, “[Economic Impact Payment Information Center](#),” (June 30, 2020).

13. See DHS CISA and U.K. NCSC Alert, “[COVID-19 Exploited by Malicious Cyber Actors](#),” (April 8, 2020).

EXHIBIT 3-A

FINCEN ADVISORY

-  Solicitations where the person, email, or social media advertisement seeks donations on behalf of a reputable organization, but is not affiliated with the reputable organization (e.g., the solicitor is not recognized or endorsed as an employee or volunteer by the organization, the email address is misspelled or not connected to the organization, or the social media advertisement directs individuals to an unaffiliated website).
-  A charitable organization soliciting donations that (1) does not have an in-depth history, financial reports, IRS annual returns, documentation of their tax-exempt status, or (2) cannot be verified by using various internet-based resources that may assist in confirming the group's existence and its nonprofit status.

Money Mule Schemes

A money mule is “a person who transfers illegally acquired money on behalf of or at the direction of another.”¹⁴ Money mule schemes, including those related to the COVID-19 pandemic, span the spectrum of using unwitting, witting, or complicit money mules.¹⁵ An **unwitting** or **unknowing** money mule is an individual who is “unaware that he or she is part of a larger criminal scheme.” The individual is motivated by his/her trust in the actual romance, job position or proposition.¹⁶ A **witting** money mule is an individual who “chooses to ignore obvious red flags or acts willfully blind to his/her money movement activity.” The individual is motivated by financial gain or an unwillingness to acknowledge his/her role.¹⁷ A **complicit** money mule is an individual who is “aware of his/her role as a money mule and is complicit in the larger criminal scheme.” The individual is motivated by financial gain or loyalty to a criminal group.¹⁸ During the COVID-19 pandemic, U.S. authorities

14. See FBI, “[Money Mule Awareness](#)” (July 2019). For more information on money mules in general, see FinCEN, “[Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes](#),” (July 16, 2019); “[FinCEN Analysis: Bank Secrecy Act Reports Filed by Financial Institutions Help Protect Elders from Fraud and Theft of Their Assets](#),” (December 4, 2019); and DOJ, “[Justice Department Announces Landmark Money Mule Initiative](#),” (December 4, 2019).

15. For more information about unwitting, witting, and complicit individuals involved in money mule scams, see FBI, “[Money Mule Awareness](#)” (July 2019).

16. For examples of how an unwitting money mule is recruited and used, see *id.*, p. 4.

17. For examples of how a witting money mule is recruited and used, see *id.*, p. 5.






18. For examples of how a complicit money mule is recruited and used, see *id.*

EXHIBIT 3-A

FINCEN ADVISORY

have detected recruiters using money mule schemes, such as good-Samaritan, romance, and work-from-home schemes.¹⁹ U.S. authorities also have identified criminals using money mules to exploit unemployment insurance programs during the COVID-19 pandemic.²⁰

Financial red flag indicators of COVID-19 money mule schemes may include:







-  The customer's personal bank account starts to receive transactions that do not fit his or her transactional history profile, including overseas transactions, the purchase of large sums of convertible virtual currency, or transactions in large fiat amounts, or the account generally had a low balance until the customer became involved in a money mule scheme. When asked about the changes in transactions, the customer declines requests for "know your customer" documents or inquiries regarding sources of funds, and may mention COVID-19, relief work, or a "work-from-home" opportunity as the source of the income.
-  The customer opens a new bank account in the name of a business and, shortly thereafter, someone transfers the funds out of the account. The person transferring the funds could be the registered account holder or someone else, and may keep a portion of the money he or she transferred (per instruction of the scammer). While this activity, in and of itself, may not be suspicious, it may become so if the individual provides unsatisfactory answers to the financial institution's inquiries, declines to provide essential "know your customer" documents, or mentions COVID-19, relief work, or "work from home" opportunities as the source of the funds.
-  The customer opens accounts in his or her name at multiple banks so he or she may receive money from various individuals or businesses, then moves the money to other accounts at the direction of the customer's purported employer.
-  The customer receives multiple state unemployment insurance payments to his or her account, or to multiple accounts held at the same financial institution, within the same disbursement timeframe (e.g., weekly or biweekly payments) issued from one or multiple states.
-  The customer's account(s) receives an unemployment deposit from a different state in which he or she reportedly resides or has previously worked.

19. The FBI has released information on how criminals are taking advantage of the COVID-19 pandemic to steal money, access personal and financial information, and use individuals as money mules. See FBI Press Release, "[FBI Warns of Money Mule Schemes Exploiting the COVID-19 Pandemic](#)" (April 6, 2020). In work-from-home schemes, for example, COVID-19 money mule recruiters, under a false charity or company label, may approach targets with a seemingly legitimate offer of employment under the pretense of work-from-home jobs, often through internet or social media advertisements, emails, or text messages. Once the target accepts the "employment," he or she receives instructions to move funds through accounts or to set up a new account in the target's name for the "business." The target (i.e., the money mule) earns money by taking a percentage of the funds that he or she helps to transfer per the instructions of the "employer." For more information on fraudulent job offers, see FTC Blog, "[Looking for work after Coronavirus layoffs?](#)" (April 13, 2020).

20. See Washington State Employment Security Department, "[Statement from Commissioner Suzi LeVine on the rise in unemployment imposter fraud attempts](#)," (May 14, 2020) and "[Update on imposter fraud from Commissioner Suzi LeVine](#)," (May 18, 2020).

EXHIBIT 3-A

FINCEN ADVISORY

-  13 The customer's account receives unemployment insurance payments for numerous employees or the accountholder name and ACH payment "remit to" name do not match.
-  14 Deposited funds are quickly diverted via wire transaction to foreign accounts located within countries known for having poor anti-money laundering controls.
-  15 The customer makes one or more atypical transactions involving an overseas account, especially through unusual payment methods for the customer. When asked about the transaction, the customer indicates it is for a person located overseas who is in need of financial assistance because of the COVID-19 pandemic.
-  16 Documentation from the customer shows that the purported employer or recruiter uses a common web-based, free email service instead of a company-specific email. For example, instead of a company- or organization-specific email address, such as [first.lastname@ABCcompany.com](#) or [lastname@XYZ_NGO.org](#), the email address is from a common and free email address provider.
-  17 The customer provides information that his or her purported employer asked the customer to receive funds into his or her personal bank account, so that the employer can then process or transfer funds via wire transfer, ACH, mail, or money services businesses out of the customer's personal account.
-  18 The customer states, or information shows, that an individual, whom the customer may not have known previously, requested financial assistance to send/receive funds through the customer's personal account, including requests by individuals claiming to be a:
 - a. U.S. Service member who is reportedly stationed abroad;
 - b. U.S. citizen working or traveling abroad; or
 - c. U.S. citizen quarantined abroad.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping financial crimes, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent and available information in the SAR and narrative. Adherence to the filing instructions below will improve FinCEN's and law enforcement's abilities to effectively identify actionable SARs using the FinCEN Query system and pull information to support COVID-19- related investigations.

EXHIBIT 3-A

FINCEN ADVISORY

- FinCEN requests that financial institutions reference this advisory by including the key term “COVID19 MM FIN-2020-A003” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- Financial institutions should also select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include the type of fraud and/or name of the scam or product (e.g., imposter scam or money mule scheme) in SAR field 34(z). In addition, FinCEN encourages financial institutions to report certain types of imposter scams and money mule schemes using fields such as SAR field 34(l) (Fraud- Mass-marketing), or SAR field 38(d) (Other Suspicious Activities- Elder Financial Exploitation), as appropriate with the circumstances of the suspected activity.
- Please refer to FinCEN’s [Notice Related to the Coronavirus Disease 2019](#) (COVID-19), which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



FinCEN ADVISORY

FIN-2020-A005

July 30, 2020

Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic

Detecting, preventing, and reporting illicit transactions and cyber activity will help protect legitimate relief efforts for the COVID-19 pandemic and help protect financial institutions and their customers against malicious cybercriminals and nation-state actors.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**COVID19-CYBER FIN-2020-A005**" and select SAR field 42 (Cyber Event). Additional guidance on filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to potential indicators of cybercrime and cyber-enabled crime observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of COVID-19-related malicious cyber activity and scams, associated financial red flag indicators, and information on reporting suspicious activity.

This advisory is intended to aid financial institutions in detecting, preventing, and reporting potential COVID-19-related criminal activity. This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners. FinCEN will continue issuing COVID-19-related information to financial institutions to help enhance their efforts to detect, prevent, and report suspected illicit activity on its website at <https://www.fincen.gov/coronavirus>, which also contains information on how to register to receive [FinCEN Updates](#).

FINCEN ADVISORY

Financial Red Flag Indicators of Cybercrime and Cyber-Enabled Crime Exploiting COVID-19

This advisory addresses the primary means by which cybercriminals and malicious state actors are increasingly exploiting the COVID-19 pandemic in cyber-enabled crime through malware and phishing schemes, extortion, business email compromise (BEC) fraud, and exploitation of remote applications, especially against financial and healthcare systems.¹

FinCEN has identified the following red flag indicators of COVID-19 cyber-enabled crimes² to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic. As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple indicators, before determining if a transaction is suspicious or otherwise indicative of potential fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional inquiries and investigations where appropriate. Additionally, some of the financial red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities. Given that many scammers may be directly targeting customers, financial institutions should remain on the alert for potential suspicious activities involving their customers.

Targeting and Exploitation of Remote Platforms and Processes

The significant migration toward remote access in the pandemic environment presents opportunities for criminals to exploit financial institutions' remote systems and customer-facing processes. Cybercriminals and malicious state actors are targeting vulnerabilities in remote

1. See Department of Justice (DOJ) Press Release, "[Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams](#)," (April 22, 2020); the United Kingdom (U.K.) National Cyber Security Centre (NCSC) Press Release, "[Public Urged to Flag Coronavirus Related Email Scams as Online Security Campaign Launches](#)," (April 21, 2020); Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Notification, "[Defending Against COVID-19 Cyber Scams](#)," (March 6, 2020); Europol Report, "[Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis](#)," (March 27, 2020); DHS CISA and Federal Bureau of Investigation (FBI) Public Service Announcement, "[People's Republic of China \(PRC\) Targeting of COVID-19 Research Organizations](#)," (May 13, 2020); FBI's Internet Crime Complaint Center (IC3) Public Service Announcement, "[Increased Use of Mobile Banking Apps Could Lead to Exploitation](#)," (June 10, 2020); and DHS CISA, National Security Agency, NCSC, and Canada Communications Security Establishment Joint Advisory, "[APT29 Targets COVID-19 Vaccine Development](#)," (July 16, 2020).
2. For the purpose of this advisory, cyber-enabled crime refers to illegal activities (e.g., fraud, identity theft, etc.) carried out or facilitated by electronic systems and devices, such as networks and computers. See FinCEN Advisory, [FIN-2016-A005](#), "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," (October 25, 2016).




EXHIBIT 3-A

FINCEN ADVISORY

applications and virtual environments to steal sensitive information, compromise financial activity, and disrupt business operations.³ Remote identity processes⁴ also face significant risks, which may include:

- *Digital Manipulation of Identity Documentation:* Criminals often seek to undermine online identity verification processes through the use of fraudulent identity documents, which can be created by manipulating digital images of legitimate government-issued identity documents to alter the information and/or photos displayed.⁵
- *Leveraging Compromised Credentials Across Accounts:* Cybercriminals commonly undermine weak authentication processes in attempted account takeovers via methods such as credential stuffing attacks. In these attacks, cybercriminals generally use lists of stolen account credentials (typically usernames or email addresses, and associated passwords) to conduct automated login attempts to gain unauthorized access to victim accounts.







Financial red flag indicators of this sort of activity may include:⁶

-  The spelling of names in account information does not match the government-issued identity documentation provided for online onboarding.
-  Pictures in identity documentation, especially areas around faces, are blurry or low resolution, or have aberrations. Pictures in identity documentation or other images of persons in remote identity verification⁷ show visual signs indicating possible image manipulation (e.g., incongruences in coloration near the edge of the face, or double edges or lines on delineated facial features).
-  Images of identity documentation have visual irregularities that indicate digital manipulation of the images, especially around information fields likely to have been changed to conduct synthetic identity fraud (e.g., name, address, and other identifiers).

3. For information related to publicly disclosed cybersecurity vulnerabilities and exposures, see U.S. Department of Commerce, National Institute for Standards and Technology (NIST), "[National Vulnerability Database](#);" MITRE, "[Common Vulnerabilities and Exposures: CVE List Home](#);" and FBI IC3 Public Service Announcements, "[Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments](#)," (April 1, 2020) and "[Increased Use of Mobile Banking Apps Could Lead to Exploitation](#)," (June 10, 2020). See also FinCEN Director Kenneth A. Blanco's, prepared remarks delivered at the Consensus Blockchain Conference, "[Consensus Blockchain Conference \(Virtual\)](#)," (May 13, 2020).
4. For the purposes of this advisory, "remote identity processes" include remote processes for customer onboarding and identity verification, as well as authentication of customers for account access purposes. For more information on digital identity standards, see NIST, "[Digital Identity Guidelines](#)," (December 1, 2017), and the Financial Action Task Force (FATF), "[Guidance on Digital Identity](#)," (March 6, 2020).
5. Criminals exploiting identity verification processes will typically use either information associated with a real individual's identity (i.e., identity theft) or create a new fabricated identity that usually consists of a real identifier, such as a social security number or driver's license number, with other fake information (i.e., synthetic identity fraud). For more information on example typologies and financial red flag indicators involving identity theft and identity fraud, see FinCEN Report, "[Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports](#)," (October 2010).
6. *Id.* See also Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, 16 CFR Part 681, app. A.
7. Images in identity verification other than identity documentation may include pictures or video of the customer (e.g., "selfie" images) taken as part of the financial institution's onboarding process.

EXHIBIT 3-A

FINCEN ADVISORY

-  4 A customer's physical description on identity documentation does not match other images of the customer.
-  5 A customer refuses to provide supplemental identity documentation or delays producing supplemental documentation.
-  6 Customer logins occur from a single device or Internet Protocol (IP) address across multiple seemingly unrelated accounts, often within a short period of time.
-  7 The IP address associated with logins does not match the stated address in identity documentation.
-  8 Customer logins occur within a pattern of high network traffic with decreased login success rates and increased password reset rates.
-  9 A customer calls a financial institution to change account communication methods and authentication information, then quickly attempts to conduct transactions to an account that never previously received payments from the customer.

Phishing, Malware, and Extortion

FinCEN and U.S. law enforcement have observed significant increases in broad-based and targeted phishing campaigns that are attempting to lure companies, especially healthcare and pharmaceutical providers, with offers of COVID-19 information and supplies.⁸ Phishing scams target individuals with communications appearing to come from legitimate sources to collect victims' personal and financial data and potentially infect their devices by convincing the target to download malicious programs.⁹ Cybercriminals usually send these phishing communications by email but may also use phone calls or text messages.

In these new schemes, phishing scammers will often reference COVID-19 themes, such as payments related to the Coronavirus Aid, Relief, and Economic Security (CARES) Act,¹⁰ in the subjects and bodies of emails. Some phishing emails lure victims by advertising ways to make money, such as through investing in convertible virtual currencies (CVCs) or via domain names that mimic names of organizations, including those that provide or enable teleworking capabilities.¹¹ Cybercriminals

8. The U.S. Secret Service (USSS) and DHS CISA have noted an increase in malware, phishing, and extortion campaigns related to COVID-19. See USSS Press Release, "[Secret Service Issues COVID-19 \(Coronavirus\) Phishing Alert](#)" (March 9, 2020).

9. See DHS CISA and U.K. NCSC Joint Alert (AA20-099A), "[COVID-19 Exploited by Malicious Cyber Actors](#)," (April 8, 2020); and DHS, "[Common Scams: Know How to Spot a Fake](#)."

10. Pub. L. [116-136](#), 116th Congress (2020).

11. Since January 2020, tens of thousands of new domains have been registered with terms related to COVID-19 and/or disaster and healthcare response efforts (e.g., "quarantine," "vaccine," and "CDC"), many including or mimicking names of companies that provide or enable teleworking capabilities. U.S. law enforcement agencies have disrupted hundreds of malicious domains used to exploit the pandemic. See FinCEN Advisory, [FIN-2020-A003](#), "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020). See also, FBI Press Release, "[FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic](#)," (April 13, 2020).



EXHIBIT 3-A

FINCEN ADVISORY

are also distributing malware,¹² including ransomware, through phishing emails, malicious websites and downloads, domain name system (DNS) hijacking or spoofing attacks, and fraudulent mobile applications. These techniques can be applied in broader campaigns involving social media, such as the recent exploit targeting Twitter and prominent users of the platform.¹³ Financial institutions dealing in CVC should be especially alert to the potential use of their institutions to launder proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes and take appropriate risk mitigating steps consistent with their BSA obligations.

FinCEN assesses that instances of extortion will also continue to grow in the wake of the COVID-19 pandemic. So far in 2020, FinCEN has received numerous suspicious activity reports (SARs) involving ransomware¹⁴ targeting medical centers and municipalities. Much of this ransomware was delivered by exploiting the COVID-19 lures described above. We expect criminals to continue targeting entities that are vulnerable due to their involvement in pandemic response, such as researchers working on medical treatments or manufacturers of personal protective equipment. In other instances of extortion, criminals are threatening to expose victims and their families to COVID-19 if they do not pay the extortion fee. In almost all cases, criminals require ransomware-related extortion payments to be made in CVC.¹⁵

Financial red flag indicators of this sort of activity may include the following:

-  Information technology enterprise activity related to transaction processes or information is connected to cyber indicators that have been associated with possible illicit activity. Malicious cyber activity may be evident in system log files, network traffic, or file information.¹⁶
-  Email addresses purportedly related to COVID-19 do not match the name of the sender or the corresponding domain of the company allegedly sending the message.

12. Malware can enable criminals to access compromised computers and computer systems to steal credentials, exfiltrate sensitive information through mechanisms like screenshots or keylogging, alter account information, and conduct fraudulent transactions.

13. See FinCEN Alert, [FIN-2020-Alert001](#), “FinCEN Alerts Financial Institutions to Convertible Virtual Currency Scam Involving Twitter,” (July 16, 2020).






14. Ransomware, a specific type of malware, typically encrypts data on systems in the interest of extorting ransom payment from victims in exchange for decrypting the information and giving victims access to their systems again.

15. Financial institutions dealing in CVC should be especially alert to the laundering of proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes. See FinCEN Advisory, [FIN-2019-003](#), “Advisory on Illicit Activity Involving Convertible Virtual Currency,” (May 9, 2019).

16. Because cyber indicators are helpful red flag indicators that financial institutions can use to identify related suspicious financial activity, FinCEN, DHS CISA, and the U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) offer a broad range of helpful cyber indicator resources, including, but not limited to: FinCEN’s Cyber Indicator Lists (CILs), shared through the FinCEN Secure Information Sharing System; OCCIP’s CILs and circulars, available upon request; and DHS CISA’s [cyber analytic products and services](#), including a comprehensive list of COVID-19-related indicators of compromise in [CSV](#) or [STIX-formatted XML](#) formats, the [Cyber Information Sharing and Collaboration Program \(CISCP\)](#), and the [Automated Indicator Sharing \(AIS\) program](#). Public-private and industry partnerships, such as the [Financial Services Information Sharing and Analysis Center](#), and open source and commercial cyber threat feeds can also be useful resources.

EXHIBIT 3-A


FINCEN ADVISORY

-  Unsolicited emails related to COVID-19 from untrusted sources encourage readers to open embedded links/files or to provide personal or financial information, such as usernames and passwords or other account credentials.
-  Emails from untrusted sources or addresses similar to legitimate telework vendor accounts offer remote application software, often advertised at no or reduced cost.
-  Emails contain subject lines identified by government or industry as associated with phishing campaigns (e.g., “Coronavirus Updates,” “2019-nCov: New confirmed cases in your City,” and “2019-nCov: Coronavirus outbreak in your city (Emergency)”).
-  Text messages have embedded links purporting to be from or associated with government relief programs and payments.
-  Embedded links or webpage addresses for purported COVID-19 resources have irregular uniform resource locators (URLs) that do not match that of the expected destination site or are similar to legitimate sites but with slight variations in the domain (e.g., variations in domain extensions like “.com,” “.org,” and “.us”) or web address spelling.

Business Email Compromise (BEC) Schemes

Cybercriminals have increasingly exploited the COVID-19 pandemic by using BEC schemes, particularly targeting municipalities and the healthcare industry supply chain. A common BEC scheme involves criminals convincing companies to redirect payments to new accounts, while claiming the modification is due to pandemic-related changes in business operations. BEC criminals often use spoofed or compromised email accounts to communicate these urgent, last-minute payment changes. In the COVID-19 environment, criminals insert themselves into communications by impersonating a critical player in a business relationship or transaction, typically posing as providers of healthcare supplies, to intercept or fraudulently induce a payment for critically needed supplies.¹⁷

Financial red flag indicators of this sort of activity may include the following:¹⁸




-  A customer’s transaction instructions contain different language, timing, and amounts in comparison to prior transaction instructions, especially regarding transactions involving healthcare providers or supplies purchases.

17. See FBI Press Release, “[FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic](#),” (April 6, 2020). See also Europol Press Release, “[Corona Crimes: Suspect Behind €6 Million Face Masks and Hand Sanitisers Scam Arrested Thanks to International Police Cooperation](#),” (April 6, 2020).

18. For general BEC-scheme financial red flag indicators, see FinCEN Advisories, [FIN-2016-A003](#), “Advisory to Financial Institutions on E-mail Compromise Fraud Schemes,” (September 6, 2016), and [FIN-2019-A005](#), “Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes,” (July 16, 2019).

EXHIBIT 3-A

FINCEN ADVISORY

-  Transaction instructions, typically involving a healthcare-sector counterparty or referencing purchase of healthcare or emergency response supplies, originate from an email account closely resembling, but not identical to, a known customer's email account.
-  Emailed transaction instructions direct payment to a different account for a known beneficiary. The transmitter may claim a need to change the destination account as part of a COVID-19 pandemic response, such as moving the account to a financial institution in a jurisdiction less affected by the disease, and assert urgency to conduct the transaction.
-  Emailed transaction instructions request to move payment methods from checks to ACH transfers as a response to the pandemic.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping financial crimes, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent available information in the SAR and narrative. Adherence to the filing instructions below will improve FinCEN and law enforcement's ability to effectively identify and pull actionable SARs and information from the FinCEN Query system to support COVID-19-related cases.

- FinCEN requests that financial institutions reference this advisory by including the key term **"COVID19-CYBER FIN-2020-A005"** in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- Financial institutions that suspect fraudulent COVID-19-related activity should mark all appropriate check boxes on the SAR form to indicate a connection between COVID-19 and the suspicious activity being reported. For example, if the activity includes a COVID-19-related account takeover involving an ACH transfer, financial institutions can select SAR field 38a and 38z, and note in the "other" box, "COVID-19 account takeover fraud – ACH."¹⁹
- Financial institutions should also include any relevant technical cyber indicators related to cyber events and associated transactions reported in a SAR within the available structured cyber event indicator fields. For example, for a COVID-19-related cyber event against a financial institution, financial institutions can select SAR fields 42a and 42z (noting in the

19. For additional guidance on identifying account takeover activity and related SAR filing instructions, see FinCEN Advisory, [FIN-2011-A016](#), "Account Takeover Activity," (December 19, 2011).

EXHIBIT 3-A

FINCEN ADVISORY

“other” box the COVID-19-related cyber event), and SAR fields 44(a)-(j), (z), including email or CVC wallet addresses, malicious domains or URLs, and any other known cyber event indicators.

- For cyber-enabled crime involving fraud driven by COVID-19, financial institutions should select SAR field 34z (Fraud – other) as the associated suspicious activity type. Additionally, financial institutions should include the type of cybercrime or scheme as a keyword (e.g., “COVID 19 BEC Fraud,” “EAC fraud,” or “BEC data theft”) in SAR field 34(z).
- Please refer to FinCEN’s May 18, 2020 [Notice Related to the Coronavirus Disease 2019](#), which contains information regarding reporting COVID-19-related crime and FinCEN’s Rapid Response Program, and reminds financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



FinCEN ADVISORY

FIN-2020-A006

October 1, 2020

Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Detecting and reporting ransomware payments are vital to prevent and deter cybercriminals from deploying malicious software to extort individuals and businesses and hold ransomware attackers accountable for their crimes.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- Chief Information Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "CYBER FIN-2020-A006" and select SAR field 42 (Cyber Event). Additional guidance on filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. This advisory provides information on: (1) the role of financial intermediaries in the processing of ransomware payments; (2) trends and typologies of ransomware and associated payments; (3) ransomware-related [financial red flag indicators](#); and (4) reporting and sharing information related to ransomware attacks.

The information contained in this advisory is derived from FinCEN's analysis of cyber- and ransomware-related Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data.¹ In some cases, in addition to the attack, the perpetrators threaten to publish sensitive files belonging to the victims, which can be individuals or business entities

1. Both extortion and computer fraud and abuse are specified unlawful activities and predicate offenses to money laundering. See 18 USC § 1956(c)(7).

(including financial institutions). The consequences of a ransomware attack can be severe and far-reaching—with losses of sensitive, proprietary, and critical information and/or loss of business functionality.

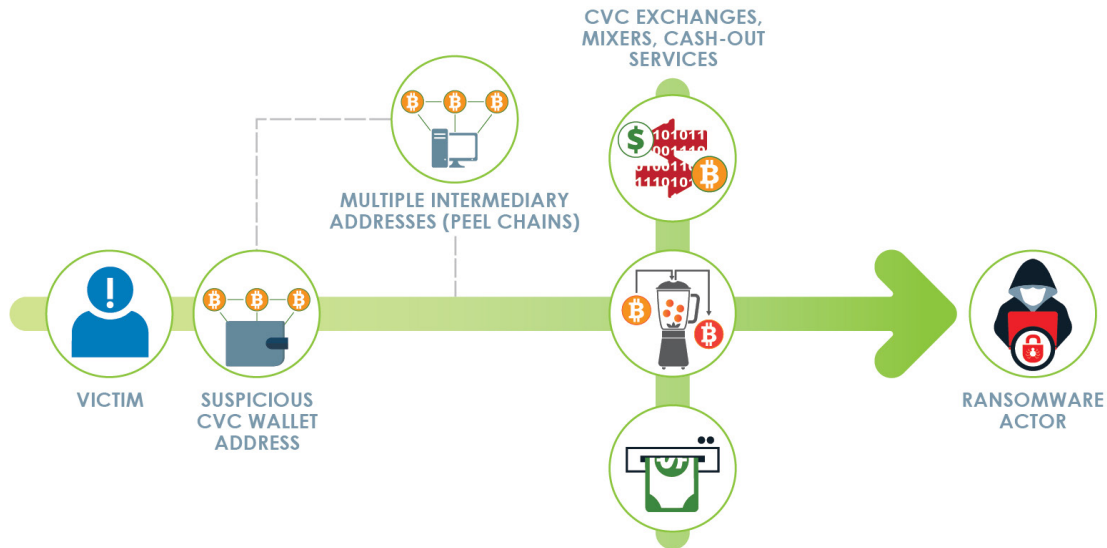
The Role of Financial Intermediaries in Facilitating Ransomware Payments

Ransomware attacks are a growing concern for the financial sector because of the critical role financial institutions play in the collection of ransom payments. Processing ransomware payments is typically a multi-step process that involves at least one depository institution and one or more money services business (MSB). Many ransomware schemes involve convertible virtual currency (CVC), the preferred payment method of ransomware perpetrators. Following the delivery of the ransom demand, a ransomware victim will typically transmit funds via wire transfer, automated clearinghouse, or credit card payment to a CVC exchange to purchase the type and amount of CVC specified by the ransomware perpetrator. Next, the victim will send the CVC, often from a wallet hosted² at the exchange, to the perpetrator's designated account or CVC address. The perpetrator then launders the funds through various means, including mixers and tumblers³ to convert funds into other CVCs, smurfing⁴ transactions across many accounts and exchanges, and/or moving the CVC to foreign-located exchanges and peer-to-peer (P2P) exchangers⁵ in jurisdictions with weak anti-money laundering and countering financing of terrorism (AML/CFT) controls.

2. "Hosted wallets" are CVC wallets where the CVC exchange receives, stores, and transmits the CVCs on behalf of their accountholders. See FinCEN Guidance, [FIN-2019-G001](#), "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," (May 9, 2019).
3. Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC.
4. Smurfing refers to a layering technique in money laundering that involves breaking total amounts of funds into smaller amounts to move through multiple accounts before arriving at the ultimate beneficiary.
5. P2P exchangers are individuals or entities offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency. P2P exchangers usually operate informally, typically advertising and marketing their services through online classified advertisements or fora, social media, and by word of mouth. See FinCEN Advisory, [FIN-2019-A003](#), "Advisory on Illicit Activity Involving Convertible Virtual Currency," (May 9, 2019).

FINCEN ADVISORY

Figure 1. Movement of CVC in Ransomware Attacks



Involvement of Digital Forensics and Incident Response
and Cyber Insurance Companies in Ransomware Payments

The prevalence of ransomware attacks has led to the creation of companies that provide protection and mitigation services to victims of ransomware attacks. Among these entities are digital forensics and incident response (DFIR) companies and cyber insurance companies (CICs). Some DFIR companies and CICs, as well as some MSBs that offer CVCs, facilitate ransomware payments to cybercriminals, often by directly receiving customers' fiat funds, exchanging them for CVC, and then transferring the CVC to criminal-controlled accounts. Depending on the particular facts and circumstances, this activity could constitute money transmission. Entities engaged in money services business activities (such as money transmission) are required to register as an MSB with FinCEN, and are subject to BSA obligations, including filing suspicious activity reports (SARs).⁶ Persons involved in ransomware payments must also be aware of any Office of Foreign Assets Control (OFAC)-related obligations that may arise from that activity. Today, OFAC issued an [advisory](#) highlighting the sanctions risks associated with facilitating ransomware payments on behalf of victims targeted by malicious cyber-enabled activities.

6. See generally 31 C.F.R. Part 1022 and 31 CFR § 1010.100(ff).

FINCEN ADVISORY

Trends and Typologies of Ransomware and Associated Payments

The severity and sophistication of ransomware attacks continue to rise⁷ across various sectors, particularly across governmental entities, and financial, educational, and healthcare institutions.⁸ Ransomware attacks on small municipalities and healthcare organizations have increased, likely due to the victims' weaker cybersecurity controls, such as inadequate system backups and ineffective incident response capabilities.⁹

Cybercriminals using ransomware often resort to common tactics, such as wide-scale phishing and targeted spear-phishing campaigns that induce victims to download a malicious file or go to a malicious site, exploit remote desktop protocol endpoints and software vulnerabilities, or deploy "drive-by" malware attacks that host malicious code on legitimate websites. Proactive prevention through effective cyber hygiene, cybersecurity controls, and business continuity resiliency is often the best defense against ransomware.¹⁰

Increasing Sophistication of Ransomware Operations

Big Game Hunting Schemes: Ransomware actors are increasingly engaging in selective targeting of larger enterprises to demand bigger payouts – commonly referred to as "big game hunting."¹¹

Ransomware Criminals Forming Partnerships and Sharing Resources: Many cybercriminals are sharing resources to enhance the effectiveness of ransomware attacks, such as ransomware exploit kits that come with ready-made malicious codes and tools. These kits can be purchased, although they are also offered free of charge. Some ransomware groups are also forming partnerships to share advice, code, trends, techniques, and illegally-obtained information over shared platforms.

"Double Extortion" Schemes: Ransomware criminals are increasingly engaging in "double extortion schemes," which involve removing sensitive data from the targeted networks and encrypting the system files and demanding ransom. The criminals then threaten to publish or sell the stolen data if the victim fails to pay the ransom.

7. The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 37% more reports of ransomware incidents in 2019 than in 2018, with a 46% increase in associated financial losses. BSA reporting shows a stark increase in financial losses per ransomware incident, with the average dollar amount in financial institution SARs on ransomware increasing approximately \$87,000 from 2018 to 2019 (\$417,000 to \$504,000) and \$280,000 from 2019 to thus far in 2020 (\$504,000 to \$783,000). See FBI IC3, "[2019 Internet Crime Report](#)," (2019); and FBI IC3, "[2018 Internet Crime Report](#)," (2018).
8. See FinCEN Advisory, [FIN-2020-A005](#), "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020).
9. Multi-State Information Sharing and Analysis Center (MS-ISAC), "[Security Primer – Ransomware](#)," (May 2020).
10. For more information about ransomware risk, see Federal Financial Institutions Examination Council (FFIEC), Press Release, "[FFIEC Releases Statement on Cyber Attacks Involving Extortion](#)," (November 3, 2015); Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), "[Security Tip \(ST19-001\): Protecting against Ransomware](#)," (April 11, 2019); and DHS CISA, MS-ISAC, National Governors Association (NGA), and National Association of State Chief Information Officers (NASCIO), Joint Alert, "[CISA, MS-ISAC, NGA & NASCIO Recommend Immediate Action to Safeguard against Ransomware](#)," (July 29, 2019).
11. See FBI Public Service Announcement, [Alert No. I-100219-PSA](#), "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," (October 2, 2019).




FINCEN ADVISORY

Use of Anonymity-Enhanced Cryptocurrencies (AECs): Cybercriminals usually require ransomware payments to be denominated in CVCs, most commonly in bitcoin (see Figure 1). However, they are also increasingly requiring or incentivizing victims to pay in AECs that reduce the transparency of CVC financial flows, including ransomware payments, through anonymizing features, such as mixing and cryptographic enhancements.¹² Some ransomware operators have even offered discounted rates to victims who pay their ransoms in AECs.

Use of “Fileless” Ransomware: Fileless ransomware is a more sophisticated tool that can be challenging to detect because the malicious code is written into the computer’s memory rather than into a file on a hard drive, which allows attackers to circumvent off-the-shelf antivirus and malware defenses.¹³

Financial Red Flag Indicators of Ransomware and Associated Payments

FinCEN has identified the following financial red flag indicators of ransomware-related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks. As no single financial red flag indicator is indicative of illicit or suspicious activity, financial institutions should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.¹⁴

-  1 IT enterprise activity is connected to cyber indicators that have been associated with possible ransomware activity or cyber threat actors known to perpetrate ransomware schemes. Malicious cyber activity may be evident in system log files, network traffic, or file information.¹⁵
-  2 When opening a new account or during other interactions with the financial institution, a customer provides information that a payment is in response to a ransomware incident.
-  3 A customer’s CVC address, or an address with which a customer conducts transactions, appears on open sources, or commercial or government analyses have linked those addresses to ransomware strains, payments, or related activity.

12. See FinCEN Advisory, [FIN-2019-A003](#), “Advisory on Illicit Activity Involving Convertible Virtual Currency,” (May 9, 2019).








13. The MS-ISAC observed a 153% increase of reported instances of ransomware targeting state, local, tribal, and territorial governments from 2018 to 2019. See MS-ISAC, “[Security Primer – Ransomware](#),” (May 2020).

14. For more information about red flags of illicit CVC use, see FinCEN Advisory, [FIN-2019-A003](#), “Advisory on Illicit Activity Involving Convertible Virtual Currency,” (May 9, 2019).

15. For example cyber indicators of compromise on specific ransomware threats, see DHS CISA Technical Alerts, “[Ransomware Alerts](#).” For other cyber indicator resources, see also FinCEN’s Cyber Indicator Lists (CILs), shared through the FinCEN Secure Information Sharing System; the U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection’s CILs and circulars, available upon request; and DHS CISA’s [cyber analytic products and services](#), including a comprehensive list of COVID-19-related indicators of compromise in [CSV](#) or [STIX-formatted XML](#) formats, the [Cyber Information Sharing and Collaboration Program \(CISCP\)](#), and the [Automated Indicator Sharing \(AIS\) program](#). Public-private and industry partnerships, such as the [Financial Services Information Sharing and Analysis Center](#), and open source and commercial cyber threat feeds can also be useful resources.

EXHIBIT 3-A

FINCEN ADVISORY

-  4 A transaction occurs between an organization, especially an organization from a sector at high risk for targeting by ransomware (e.g., government, financial, educational, healthcare), and a DFIR or CIC, especially one known to facilitate ransomware payments.
-  5 A DFIR or CIC customer receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a CVC exchange.
-  6 A customer shows limited knowledge of CVC during onboarding or via other interactions with the financial institution, yet inquires about or purchases CVC (particularly if in a large amount or rush requests), which may indicate the customer is a victim of ransomware.
-  7 A DFIR, CIC, or other company that has no or limited history of CVC transactions sends a large CVC transaction, particularly if outside a company's normal business practices.
-  8 A customer that has not identified itself to the CVC exchanger, or registered with FinCEN as a money transmitter, appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions between various CVCs, which may indicate that the customer is acting as an unregistered MSB.
-  9 A customer uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.
-  10 A customer initiates multiple rapid trades between multiple CVCs, especially AECs, with no apparent related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.

Reminder of Regulatory Obligations for U.S. Financial Institutions Regarding Suspicious Activity Reporting Involving Ransomware and USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

Financial institutions can play an important role in protecting the U.S. financial system from ransomware threats through compliance with their BSA obligations. Financial institutions should determine if filing a SAR is required or appropriate when dealing with an incident of ransomware conducted *by, at, or through* the financial institution, including ransom payments made by financial institutions that are victims of ransomware. As a reminder, a financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves or aggregates to \$5,000 (or, with one exception, \$2,000 for MSBs)¹⁶ or more in funds or other assets and involves

16. See 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above \$2,000. See also 31 C.F.R. § 1022.320(a)(2).

EXHIBIT 3-A

FINCEN ADVISORY

funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity. Reportable activity can involve transactions, including payments made by financial institutions, related to criminal activity like extortion and unauthorized electronic intrusions that damage, disable, or otherwise affect critical systems. SAR obligations apply to both *attempted and successful* transactions, including both attempted and successful initiated extortion transactions.¹⁷

Financial institutions are required to file complete and accurate reports that incorporate *all relevant information available*, including cyber-related information. When filing a SAR regarding suspicious transactions that involve cyber events (including ransomware), financial institutions should provide all pertinent available information on the event and associated with the suspicious activity, including cyber-related information and technical indicators, in the SAR form and narrative. When filing is not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector. Valuable cyber indicators for law enforcement investigations for ransomware can include relevant email addresses, Internet Protocol (IP) addresses with their respective timestamps, login information with location and timestamps, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), malware hashes, malicious domains, and descriptions and timing of suspicious electronic communications.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.¹⁸ Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.¹⁹ When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or anti-money laundering program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.²⁰

17. FinCEN assesses that ransomware-related activity is under-reported.

18. See 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), and 1026.320(d).

19. *Id.* See also FinCEN Guidance, [FIN-2007-G003](#), "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

20. FinCEN Guidance, [FIN-2007-G003](#), "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

FINCEN ADVISORY

SAR Filing Instructions

FinCEN requests that financial institutions reference this advisory by including the key term:

“CYBER-FIN-2020-A006”

in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and ransomware-related activity.

Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type, as well as select SAR field 42z (Cyber event - Other) while including “ransomware” as keywords in SAR field 42z, to indicate a connection between the suspicious activity being reported and possible ransomware activity. Additionally, financial institutions should include any relevant technical cyber indicators related to the ransomware activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)-(j), (z).

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving ransomware schemes. Financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities (“SUAs”) and such an institution will still remain protected from civil liability under the section 314(b) safe harbor. The SUAs listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including extortion and computer fraud and abuse. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs.²¹

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

21. For further guidance related to the 314(b) Program, see FinCEN [Fact Sheet](#), “Section 314(b)” (November 2016) and FinCEN Guidance, [FIN-2009-G002](#), “Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act,” (June 16, 2009).



FinCEN ADVISORY

FIN-2020-A008

October 15, 2020

Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity

Human traffickers and their facilitators exploit the innocent and most vulnerable of our society for financial gain, employing an evolving range of money laundering tactics to evade detection, hide their proceeds, and grow their criminal enterprise.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer-Facing Staff
- Money Services Businesses
- Casinos

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: **"HUMAN TRAFFICKING FIN-2020-A008"** and selecting **SAR Field 38(h)** (human trafficking). Additional guidance appears near the end of this advisory.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to help save lives, and to protect the most vulnerable in our society from predators and cowards who prey on the innocent and defenseless for money and greed. This advisory supplements the 2014 FinCEN Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags ("2014 Advisory").¹

Human traffickers and their facilitators exploit adults and children in the United States, and around the world, for financial gain, among other reasons. Victims are placed into forced labor, slavery, involuntary servitude, and peonage, and/or forced to engage in commercial sex acts. Anyone can be a victim regardless of origin, sex, age, or legal status.² And anyone can be a trafficker, from a single individual, such as a family member, to a criminal network, terrorist organization, or corrupt government regime.³ The global COVID-19 pandemic can exacerbate the conditions that contribute to human trafficking, as the support structures for potential victims collapse, and

1. FinCEN Advisory, [FIN-2014-A008](#), "Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags," (September 11, 2014).
2. See U.S. Department of Homeland Security, Blue Campaign, "[What is Human Trafficking?](#)"
3. See U.S. Department of State, "[Trafficking in Persons Report](#)," (June 2019); see also Financial Action Task Force, "[Financial Flows from Human Trafficking](#)," p. 15 (July 2018).

EXHIBIT 3-A

FINCEN ADVISORY

traffickers target those most impacted and vulnerable.⁴ Other effects of the pandemic (e.g., travel limitations, shelter-in-place orders, teleworking) also may affect the typologies and red flag indicators provided below.

Unfortunately, in addition to the horrific toll on victims and their families, their very lives, dignity, and livelihood, human trafficking is now one of the most profitable and violent forms of international crime, generating an estimated \$150 billion worldwide per year.⁵ In the United States, human trafficking now occurs in a broad range of licit and illicit industries (e.g., hospitality, agricultural, janitorial services, construction, restaurants, care for persons with disabilities, salon services, massage parlors, retail, fairs and carnivals, peddling and begging, child care, domestic work, and drug smuggling and distribution).⁶ Transactions involving proceeds generated by human trafficking can be the basis for federal criminal charges and asset forfeiture, as human trafficking and associated crimes constitute specified unlawful activities (SUAs) for the crime of money laundering.⁷

Since the 2014 Advisory, FinCEN collaborated with law enforcement to identify 20 new financial and behavioral indicators of labor and sex trafficking, and four additional typologies. This advisory provides: (i) new information to assist in identifying and reporting human trafficking, and to aid the global effort to combat this crime; and (ii) two illustrative recent case studies. The 2014 Advisory remains relevant, and provides information related to human smuggling, in addition to human trafficking.

Human Smuggling

Acts or attempts to bring unauthorized aliens to or into the United States, transport them within the U.S., harbor unlawful aliens, encourage entry of illegal aliens, or conspire to commit these violations, knowingly or in reckless disregard of illegal status.⁸

Human Trafficking

The act of recruiting, harboring, transporting, providing or obtaining a person for forced labor or commercial sex acts through the use of force, fraud, or coercion.⁹

4. Polaris, "[COVID-19 May Increase Human Trafficking in Vulnerable Communities](#)," (April 7, 2020). See also U.S. Department of State, "[Trafficking in Persons Report](#)," (June 2019) (discussing the vulnerabilities that traffickers target globally).
5. International Labour Organization, "[Profits and Poverty: The Economics of Forced Labour](#)," p. 13, (May 20, 2014). See also U.S. Department of the Treasury, "[Combatting Human Trafficking](#)," (January 29, 2020).
6. See U.S. Department of State, "[Trafficking in Persons Report](#)," pp. 491–492 (June 2019). Relatedly, goods that are produced by forced or child labor can be illegally imported into the United States. The U.S. Customs and Border Protection issues [Withhold and Release Orders](#) against imported merchandise suspected of being produced from forced or child labor. The U.S. Department of Labor maintains a [list of goods and their source countries](#), which it has reason to believe are produced by forced or child labor in violation of international standards.
7. SUAs relevant to human trafficking cases include a variety of offenses listed under 18 U.S.C. §§ 1956(c)(7) and 1961(1), such as those listed in Title 18, unless otherwise specified.
8. See 8 U.S.C. § 1324. See also, U.S. Department of State, "[Human Trafficking and Migrant Smuggling: Understanding the Difference](#)," (June 27, 2017).
9. See generally 18 U.S.C. §§ 1581, 1584, 1589, 1590, 1591, 2421, 2422, 2423, and 2425; 22 U.S.C. §§ 7102(4) and (11); The Victims of Trafficking and Violence Protection Act of 2000 (Pub. L. No. 106-386); applicable state laws; and U.S. Department of State, "[Report on U.S. Government Efforts to Combat Trafficking in Persons](#)," (December 1, 2017).

FINCEN ADVISORY

In contrast to human smuggling, human trafficking does not require movement. Human traffickers can exploit individuals within the border of a country, and even in a victim's own home. Human trafficking can also begin as human smuggling, as individuals who enter a country voluntarily and illegally are inherently vulnerable to abuse and exploitation, and often owe a large debt to their smuggler.¹⁰

Because the information financial institutions collect and report is vital to identifying human trafficking and stopping the growth of this crime, it is imperative that financial institutions enable their detection and reporting of suspicious transactions by becoming aware of the current methodologies that traffickers and facilitators use. It is also critical that customer-facing staff are aware of behavioral indicators that may indicate human trafficking, as the only outside contact for victims of human trafficking may occur when visiting financial institutions.

I. New Typologies of Human Trafficking

To evade detection, hide their illicit proceeds, and profit off the backs of victims, human traffickers employ a variety of evolving techniques. Below are four typologies, identified in Bank Secrecy Act (BSA) data since FinCEN issued the 2014 Advisory, that human traffickers and facilitators have used to launder money.

1. *Front Companies*

Human traffickers routinely establish and use front companies, sometimes legal entities, to hide the true nature of a business, and its illicit activities, owners, and associates. Front companies are businesses that combine illicit proceeds with those gained from legitimate business operations. Examples of front companies used by human traffickers for labor or sex trafficking include massage businesses, escort services, bars, restaurants, and cantinas.¹¹ In the case of businesses that act as a front for human trafficking, typically the establishment appears legitimate with registrations and licenses. The front company generates revenue from sales of alcoholic beverages and cover charges. Patrons, however, also can obtain illicit sexual services from trafficked individuals, usually elsewhere in the establishment.¹² In addition, illicit massage businesses or nail and hair salons can offer sexual services under the guise of legitimate businesses and/or exploit individuals for the purpose of forced labor.¹³ Often, these establishments will appear to be a single storefront, yet are part of a larger network. Payments for these illicit services are usually in cash, and traffickers may invest the illicit proceeds in high-value assets, such as real estate and cars.

10. See U.S. Immigrations and Customs Enforcement, "[Human Trafficking vs Human Smuggling](#)," (Summer 2017); and see also U.S. Department of State, "[Human Trafficking and Migrant Smuggling: Understanding the Difference](#)," (June 27, 2017).

11. An establishment that provides food, drinks, dancing, and music, and is typically found in Latin American communities.

12. See Financial Action Task Force, "[Financial Flows from Human Trafficking](#)," p. 54 (July 2018). See also U.S. Department of Justice, "[Sex Trafficking Ring Leader Gets Life in Federal Prison](#)," (January 20, 2016).

13. U.S. Department of Justice, "[What is Human Trafficking?](#)" (January 6, 2017).

EXHIBIT 3-A

FINCEN ADVISORY

2. *Exploitative Employment Practices*

Some seemingly legitimate businesses use exploitative employment schemes, such as visa fraud and wage retention, to amass profit from labor and sex trafficking. For instance, some labor recruiters mislead or defraud victims, taking advantage of workers before and after they enter the United States. Some labor recruiters also mislead workers about the conditions and nature of a job, engage in contract switching, and confiscate or destroy workers' identity documents.¹⁴ Foreign nationals who have legitimate temporary work or student visas also can be exploited.¹⁵

Another common practice is to charge exploitative fees to workers by withholding their salary or paying less than promised. The trafficker claims that the fees cover the costs of recruitment or access to job opportunities.¹⁶ Recruitment fees can range from hundreds of dollars to tens of thousands of dollars, and take years to repay.¹⁷ Victims' salaries are transferred to the traffickers or their co-conspirators via teller checks or wire transfers. Proceeds also can be "disguised" as a legitimate business expense, such as a cleaning service. Financial institutions may see multiple employees receiving their salaries in the same account, or payment for employment may be followed by immediate withdrawal or transfer into another account.¹⁸

3. *Funnel Accounts*

Funnel accounts generally involve an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.¹⁹ Human traffickers may use interstate funnel accounts to transfer funds between geographic areas, move proceeds rapidly, and maintain anonymity.²⁰ In labor and sex trafficking schemes, human traffickers may open accounts in their name, or escort victims to a bank, and force them to open an account.²¹ Traffickers maintain control of the victims' bank accounts through coercion, and direct victims to deposit money into their accounts and other accounts that the traffickers can access.²² In some cases, victims also are coerced or forced to wire proceeds via money services businesses (MSBs) to facilitate the funneling of proceeds.

-
14. U.S. Department of State, "[Paying to Work: The High Cost of Recruitment Fees](#)," (June 27, 2017); *see also* U.S. Department of Justice, "[Brothers Sentenced to 20 Years for Running Violent Human Trafficking Enterprise](#)," (February 25, 2016).
 15. U.S. Department of Justice, Journal of Federal Law and Practice, "[Human Trafficking](#)," Executive Office of United States Attorneys, pp. 5 and 28, (November 2017).
 16. For more information *see* U.S. Department of Justice, "[Leader of Human Trafficking Organization Sentenced to Over 15 Years for Exploiting Guatemalan Migrants at Ohio Egg Farms](#)," (June 27, 2016); and U.S. Department of Justice, "[Brothers Sentenced to 20 Years for Running Violent Human Trafficking Enterprise](#)," (February 25, 2016).
 17. *See* U.S. Department of State, "[Paying to Work: The High Cost of Recruitment Fees](#)," (June 27, 2017).
 18. Financial Action Task Force, "[Financial Flows from Human Trafficking](#)," p. 28, (July 2018).
 19. FinCEN Advisory, [FIN-2014-A005](#), "Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML," p. 1, (May 28, 2014).
 20. *See* U.S. Immigration and Customs Enforcement, "[Using a Financial Attack Strategy to Combat Human Trafficking](#)," (January 29, 2015).
 21. For additional behavioral indicators of human trafficking, *see* Section II, *infra*.
 22. Policies of certain large national banks to restrict third-party cash deposits for private customer accounts seem to have lessened the use of funnel account activity.

FINCEN ADVISORY

[Case Study: Funnel Accounts Facilitate International Thai Sex Trafficking Ring](#)*4. Alternative Payment Methods*

In addition to payment via cash, traffickers also have accepted payment via credit cards, prepaid cards,²³ mobile payment applications, and convertible virtual currency.²⁴ Buyers of commercial sex use prepaid cards—a method of payment using funds paid in advance, which can be acquired anonymously with cash or on darknet websites—to register with escort websites and to purchase sexual services, flights, throw-away phones, and hotel rooms.²⁵

Illicit actors also use virtual currency to advertise commercial sex online. For example, human traffickers have purchased prepaid cards, and then used the cards to purchase virtual currency on a peer-to-peer exchange platform. Human traffickers then use the virtual currency to buy online advertisements that feature commercial sex acts to obtain customers.²⁶

FinCEN also has identified transactions in which human traffickers use third-party payment processors (TPPPs) to wire funds, which gives the appearance that the TPPP is the originator or beneficiary of the wire transfer and conceals the true originator or beneficiary. For example, human traffickers facilitate payments via TPPPs for the operation of online escort services and online streaming services that use voice-over Internet protocol technology. Human traffickers and their facilitators use TPPPs to wire funds to individuals or businesses both domestically and abroad.²⁷

[Case Study: Trafficking Involving Prepaid Cards and Bitcoin](#)

II. Behavioral and Financial Red Flag Indicators of Human Trafficking

In applying the red flags below and the red flags in the 2014 Advisory, financial institutions are advised that no single red flag is a clear indicator of human trafficking activity, although each can be indicative of forced labor and/or sex trafficking. Given that human trafficking is a predicate offense to money laundering, the financial red flags also may be indicative of other money laundering-related offenses. Financial institutions should consider additional factors, such as a customer's previous financial activity and the existence of typologies or other red flags, when determining whether transactions may be associated with human trafficking.

23. See U.S. Department of the Treasury, "[National Money Laundering Risk Assessment](#)," p. 15-16, (2018).

24. For more information about illicit activity involving convertible virtual currency see FinCEN Advisory, [FIN-2019-A003](#), "Advisory on Illicit Activity Involving Convertible Virtual Currency," (May 9, 2019).

25. See New York County District Attorney Cyrus Vance Jr.'s testimony, "[Following the Money: How Human Traffickers Exploit the U.S. Financial Markets: Hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services of the U.S. House of Representatives](#)," (January 30, 2018). See also U.S. Department of Homeland Security, "[Using a Financial Attack Strategy to Combat Human Trafficking](#)," (January 29, 2015); and U.S. Department of the Treasury, "[National Money Laundering Risk Assessment](#)," p. 15-16, (2018).

26. See New York County District Attorney Cyrus Vance Jr.'s testimony, "[Following the Money: How Human Traffickers Exploit the U.S. Financial Markets: Hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services of the U.S. House of Representatives](#)," (January 30, 2018); and Financial Action Task Force, "[Financial Flows from Human Trafficking](#)," p. 55-56, (July 2018).

27. See, e.g., Financial Action Task Force, "[Financial Flows from Human Trafficking](#)," pp. 20-26, (July 2018).











EXHIBIT 3-A

FINCEN ADVISORY

Behavioral Indicators

Many victims of human trafficking do not have regular contact with anyone other than their traffickers. The only outside contact they may have is when visiting financial institutions such as bank branches, check cashing counters, or money wiring services. Consequently, it is important that customer-facing staff consider the following behavioral indicators when conducting transactions,²⁸ particularly those that also present financial indicators of human trafficking schemes discussed below. As appropriate, such information should be incorporated into Suspicious Activity Report (SAR) filings and/or reported to law enforcement.²⁹ When incorporated into SAR filings, it is important that behavioral indicators, and the staff who witnessed them, are included in the SAR narrative so that information may be effectively searched for, and later used by, law enforcement.

This list is not exhaustive and is only a selection of behavioral indicators:³⁰

-  1 A third party speaks on behalf of the customer (a third party may insist on being present and/or translating).
-  2 A third party insists on being present for every aspect of the transaction.
-  3 A third party attempts to fill out paperwork without consulting the customer.
-  4 A third party maintains possession and/or control of all documents or money.
-  5 A third party claims to be related to the customer, but does not know critical details.
-  6 A prospective customer uses, or attempts to use, third-party identification (of someone who is not present) to open an account.
-  7 A third party attempts to open an account for an unqualified minor.
-  8 A third party commits acts of physical aggression or intimidation toward the customer.
-  9 A customer shows signs of poor hygiene, malnourishment, fatigue, signs of physical and/or sexual abuse, physical restraint, confinement, or torture.
-  10 A customer shows lack of knowledge of their whereabouts, cannot clarify where they live or where they are staying, or provides scripted, confusing, or inconsistent stories in response to inquiry.

28. Additional resources discussing human trafficking and the role of financial institutions include the U.S. Department of Homeland Security, Blue Campaign, "[Resources Page](#)"; U.S. Department of the Treasury, "[Combatting Human Trafficking](#)," (January, 29, 2020); U.S. Department of State, "[Tracking Suspicious Financial Activity to Address Human Trafficking](#)," (June 28, 2018); U.S. Immigration and Customs Enforcement, "[Using a Financial Attack Strategy to Combat Human Trafficking](#)," (January 29, 2015); and Financial Action Task Force, "[Financial Flows from Human Trafficking](#)," (July 2018).

29. To report suspicious activity indicative of human trafficking to the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Tip Line, call 1-866-DHS-2-ICE (1-866-347-2423) 24 hours a day, seven days a week, every day of the year. The Tip Line is also accessible outside the United States by calling 802-872-6199.











30. See Organization for Security and Co-operation in Europe, "[Following the Money: Compendium of Resources and Step-by-step Guide to Financial Investigations into Trafficking in Human Beings](#)," (November 7, 2019).

EXHIBIT 3-A

FINCEN ADVISORY

Financial Indicators

To help identify and report transactions possibly associated with human trafficking, FinCEN has identified 10 new financial red flag indicators. These red flags do not replace the red flags identified in the 2014 Advisory, all of which remain relevant.³¹ The Financial Action Task Force report on the “Financial Flows from Human Trafficking” also provides numerous indicators of money laundering related to human trafficking.³²

-  **11** Customers frequently appear to move through, and transact from, different geographic locations in the United States. These transactions can be combined with travel and transactions in and to foreign countries that are significant conduits for human trafficking.³³
-  **12** Transactions are inconsistent with a customer’s expected activity and/or line of business in an apparent effort to cover trafficking victims’ living costs, including housing (e.g., hotel, motel, short-term rentals, or residential accommodations), transportation (e.g., airplane, taxi, limousine, or rideshare services), medical expenses, pharmacies, clothing, grocery stores, and restaurants, to include fast food eateries.
-  **13** Transactional activity largely occurs outside of normal business operating hours (e.g., an establishment that operates during the day has a large number of transactions at night), is almost always made in cash, and deposits are larger than what is expected for the business and the size of its operations.
-  **14** A customer frequently makes cash deposits with no Automated Clearing House (ACH) payments.
-  **15** An individual frequently purchases and uses prepaid access cards.
-  **16** A customer’s account shares common identifiers, such as a telephone number, email, and social media handle, or address, associated with escort agency websites and commercial sex advertisements.
-  **17** Frequent transactions with online classified sites that are based in foreign jurisdictions.
-  **18** A customer frequently sends or receives funds via cryptocurrency to or from darknet markets or services known to be associated with illicit activity. This may include services that host advertising content for illicit services, sell illicit content, or financial institutions that allow prepaid cards to pay for cryptocurrencies without appropriate risk mitigation controls.
-  **19** Frequent transactions using third-party payment processors that conceal the originators and/or beneficiaries of the transactions.
-  **20** A customer avoids transactions that require identification documents or that trigger reporting requirements.

31. FinCEN Advisory, [FIN-2014-A008](#), “Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags,” (September 11, 2014).

32. Financial Action Task Force, “[Financial Flows from Human Trafficking](#),” pp. 65-70, (July 2018).

33. For information on specific countries, and whether they are conduits for human trafficking, see U.S. Department of State, “[Trafficking in Persons Report](#),” (June 2019).

Case Studies

Funnel Accounts Facilitate International Thai Sex Trafficking Ring

In December 2018, 36 defendants were found guilty in St. Paul, Minnesota, for their various roles in operating an international sex trafficking ring, i.e., traffickers, house bosses, money launderers, and facilitators. Traffickers based in Thailand lured women to the United States through false promises of a better life. To facilitate the transport of the victims, the organization engaged in visa fraud by creating false identification documents, and forced many of the victims to enter into fraudulent marriages and debt bondage. In exchange, each victim incurred a debt of \$55,000, which far exceeded actual expenses. Once in the United States, the victims were sent to various cities, isolated in a residence, and forced to pay off their debt by engaging in commercial sex acts.³⁴

To conceal and redistribute the proceeds of the sex trafficking business, victims were forced to open U.S. bank accounts in Los Angeles in their own names. Once an account was opened, however, traffickers based in the United States took control of the account, kept a percentage of the cash generated, and sent the remainder back to the traffickers in Thailand. Other members of the organization, the “facilitators,” rented the houses, apartments, and hotels, and facilitated the transport of victims.

The organization used funnel accounts to launder money deposited in cities across the United States to third-party launderers who made cash withdrawals in Los Angeles.³⁵ According to data made available to FinCEN, deposits were made in cash, and were just enough to cover account debits. To move funds to and from Thailand, the organization employed third-party money launderers who made bank accounts available and coordinated cash deposits and withdrawals.

Bulk cash smuggling was another scheme used to physically transport proceeds to Thailand. According to law enforcement, individuals were recruited to carry large volumes of cash in suitcases and transport the money to Thailand. To evade detection, the trafficking organization paid flight attendants to keep quiet, and in some limited instances, to transport bulk cash in their own luggage. Money also was concealed in clothing and dolls that were shipped to Thailand. To date, law enforcement has recovered \$1.5 million in cash, and testimony revealed that more than \$40 million was sent to Thailand by one money launderer alone.

34. For information on this case, see U.S. Department of Justice, [“Twenty-One Additional Defendants Indicted for their Roles in Thai Sex Trafficking Enterprise,”](#) (May 25, 2017); see also U.S. Department of Justice, [“Thirty-Six Defendants Guilty for their Roles in International Thai Sex Trafficking Organization,”](#) (December 13, 2018).

35. For a definition of third-party money launderers see U.S. Department of Homeland Security, [“Third Party Money Launderers,”](#) (Summer 2017).

EXHIBIT 3-A

FINCEN ADVISORY

Trafficking Involving Prepaid Cards and Bitcoin

In April 2016, law enforcement agents from HSI in El Paso, Texas, responded to a call made to local police regarding a woman who was being forcibly held by an individual identified as “Tae” at a motel. Officers discovered two adult victims when they searched the motel room. Police located William “Tae” Harris, who was stopped while driving a suspect vehicle in the area. He possessed a semi-automatic firearm. Harris and his passenger, Dean Hall, were members of the West Side City Crips gang from Phoenix, Arizona.

The subsequent HSI investigation revealed that Harris and Hall brought the victims to Texas from Arizona, where the victims were forced into prostitution, beaten, and suffered threats of violence. HSI determined that at least three other West Side City Crips were operating a prostitution scheme in El Paso. During a forensic extraction of Harris’ mobile phone, HSI discovered bitcoin transaction data and was able to exploit Harris’ bitcoin wallet information. Evidence revealed that the group’s illicit activity revolved around the purchase of Vanilla Visa prepaid credit cards, which were then used to purchase bitcoin on the Paxful virtual currency exchange. Those bitcoin were used to purchase prostitution ads on Backpage.com. Furthermore, during Harris’ prosecution, HSI uncovered and disrupted an attempted murder-for-hire in which Harris planned to have a key witness and her sister murdered.

In January 2018, Hall and Harris were convicted and sentenced for violating several anti-trafficking statutes. Hall was sentenced to 90 months’ imprisonment and five years of supervised release, and Harris was sentenced to 180 months’ imprisonment and ten years of supervised release.

Guidance to U.S. Financial Institutions

Customer Due Diligence and Identification of Beneficial Owners of New Legal Entity Accounts

As of May 11, 2018, FinCEN’s Customer Due Diligence (CDD) Rule requires banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.³⁶ Identifying and verifying the beneficial owners of legal entities could facilitate the identification of the beneficiaries of the illicit proceeds.

36. See 31 CFR § 1010.230 (describing beneficial ownership requirements for legal entity customers).

FINCEN ADVISORY

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving fraud schemes. Financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information relating to transactions that the institution suspects may involve the proceeds of one or more SUAs and such an institution still will remain protected from civil liability under section 314(b) safe harbor. The SUAs listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including fraud against individuals or the government. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs.³⁷

Suspicious Activity Reporting (SAR)

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.³⁸

SAR Filing Instructions

Financial institutions should provide all pertinent available information in the SAR form and narrative. A potential victim of human trafficking should not be reported as the subject of a SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR. **FinCEN further requests that financial institutions reference this advisory by including the key term:**

“HUMAN TRAFFICKING FIN-2020-A008”

in SAR field 2 (Filing Institution Note to FinCEN) to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory. Additional information to include behavioral indicators, email addresses, phone numbers, and IP addresses also should be included when possible to aid law enforcement investigations.

37. For further guidance related to the 314(b) Program, see FinCEN [Section 314\(b\) Fact Sheet](#) (November 2016), and FinCEN Guidance [FIN-2009-G002](#), “Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act,” (June 16, 2009).

38. 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

EXHIBIT 3-A

FINCEN ADVISORY

Financial institutions that suspect human trafficking activity should also mark the check box for human trafficking (SAR Field 38(h)) on the SAR form.

38 Other Suspicious Activities		
a <input type="checkbox"/> Account takeover	h <input type="checkbox"/> Human trafficking	o <input type="checkbox"/> Suspicious use of multiple transaction locations
b <input type="checkbox"/> Bribery or gratuity	i <input type="checkbox"/> Identity theft	p <input type="checkbox"/> Transaction with no apparent economic, business, or lawful purpose
c <input type="checkbox"/> Counterfeit instruments	j <input type="checkbox"/> Little or no concern for product performance penalties, fees, or tax consequences	q <input type="checkbox"/> Transaction(s) involving foreign high risk jurisdiction
d <input type="checkbox"/> Elder financial exploitation	k <input type="checkbox"/> Misuse of position or self-dealing	r <input type="checkbox"/> Two or more individuals working together
e <input type="checkbox"/> Embezzlement/theft/disappearance of funds	l <input type="checkbox"/> Suspected public/private corruption (domestic)	s <input type="checkbox"/> Unlicensed or unregistered MSB
f <input type="checkbox"/> Forgeries	m <input type="checkbox"/> Suspected public/private corruption (foreign)	z <input type="checkbox"/> Other <input type="text"/>
g <input type="checkbox"/> Human smuggling	n <input type="checkbox"/> Suspicious use of informal value transfer system	

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

EXHIBIT 3-A



FIN-2014-A008

September 11, 2014

Advisory

Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags

FinCEN identifies “red flags” to assist financial institutions in identifying and reporting suspicious financial activity connected to human smuggling and human trafficking.

To support law enforcement efforts to fight human smuggling and human trafficking, the Financial Crimes Enforcement Network (FinCEN) seeks to advise financial institutions on how to detect and report suspicious financial activity that may be related to human smuggling and/or human trafficking. Financial institutions, large and small, can play a critical role in identifying and reporting transactions related to these unlawful activities based on their observations when interacting with customers and their monitoring processes.

FinCEN, in collaboration with law enforcement agencies, non-governmental organizations and members of the financial industry, has identified financial indicators, or “red flags,” that may indicate financial activity related to human smuggling or human trafficking. In addition to identifying red flags, this advisory provides common terms that financial institutions may use when reporting activity related to these crimes. The use of common terms will assist law enforcement in better identifying possible cases of human smuggling or human trafficking reported through Suspicious Activity Reports (SARs).

Human Smuggling

Acts or attempts to bring unauthorized aliens to or into the United States, transport them within the U.S., harbor unlawful aliens, encourage entry of illegal aliens, or conspire to commit these violations, knowingly or in reckless disregard of illegal status.¹

Human Trafficking

The act of recruiting, harboring, transporting, providing or obtaining a person for forced labor or commercial sex acts through the use of force, fraud or coercion.²

1. See, 8 U.S.C. § 1324.

2. See generally, 18 U.S.C. §§ 1581, 1584, 1589, 1590, 1591, 24121, 2422, 2423 and 2425, The Victims of Trafficking and Violence Protection Act of 2000 (Pub. L. No. 106-386), applicable State laws and the [President’s Interagency Task Force – Progress in Combating Trafficking in Persons: The U.S. Government Response to Modern Slavery](#).

EXHIBIT 3-A

F I N C E N A D V I S O R Y

Difference between Human Smuggling and Human Trafficking

Human Smuggling	Human Trafficking
(i) Involves persons choosing to immigrate illegally.	(i) Involves the use of force or coercion and the exploitation of victims.
(ii) Is limited to illegal migration or the harboring of undocumented aliens.	(ii) Includes, but is not limited to, involuntary servitude, forced labor, debt bondage, peonage and sexual exploitation.
(iii) Involves foreign nationals.	(iii) Anyone can be a victim regardless of origin, sex, age or legal status.
(iv) The crime involves an illegal border crossing or the harboring of someone that illegally crossed the border.	(iv) There is no need for a person to cross a border to be trafficked; individuals can be trafficked within the borders of a country.

Understanding How Human Smuggling and Human Trafficking Work

There are a number of identifiable stages involved in human smuggling and in human trafficking during which traffickers may need to interact with the financial system. This advisory includes below a brief description of these stages to provide financial institutions with the necessary context to appropriately identify potential human smuggling and/or human trafficking-related transactions. Financial indicators, including those described in Appendices A and B, may reflect transactions associated with actions that facilitate one or more of the stages of human smuggling and/or human trafficking.

How Human Smuggling Works

Stages of Human Smuggling generally include:

Solicitation: A potential migrant may seek the services of a local facilitator/smuggler. Local facilitators/smugglers are often part of a larger smuggling network that works to bring migrants across a country border. In the United States, illegal migrants often originate from Mexico and Central America, but they may originate from anywhere in the world.

Transportation: Migrants may be smuggled through a number of different routes and transportation modes to avoid detection. The person may be transported by air, sea and/or land over an international border.

EXHIBIT 3-A

F I N C E N A D V I S O R Y

Payment: Payment to smugglers or to smuggling networks are generally conducted in one of three ways.

1. *Pay In Advance:* The migrant or the migrant's relatives provide full payment to the smuggler before traveling. This method of payment is often used by relatives of unaccompanied minors for their migration.
2. *Partial Payment:* A portion of the smuggling fees is paid prior to departure, with the remaining due upon arrival; final payment is often made by relatives of the migrant in the United States.
3. *On Arrival:* After the migrant is successfully smuggled, the migrant's relatives pay the full fee to the smuggler. This method of payment is often used by relatives of unaccompanied minors for their migration.

How Human Trafficking Works

Stages of Human Trafficking generally include:

Recruitment or Abduction: Traffickers obtain their victims through deception or force. For instance, traffickers may recruit victims through the use of kidnapping, false marriages, or advertisements offering employment or study abroad. Individuals from countries and geographic areas that have been affected by economic hardship, armed conflicts or natural disasters are particularly vulnerable to these tactics.

Transportation: After being collected, victims are transported to locations where they are exploited or sold to other traffickers. Victims may originate from abroad or within the United States and may be transported by air, sea and/or land domestically or internationally.

Exploitation: During this stage, traffickers profit from exploiting victims through forced labor, sexual exploitation, involuntary participation in crimes or other activity. Businesses in the service and manual labor industries (e.g., massage parlors, restaurants, farms, construction companies, domestic services) have been frequently used to exploit trafficked individuals.³ In contrast to the one-time illicit proceeds of human smuggling, this final phase of human trafficking may generate ongoing criminal proceeds.

3. To view the industry sectors particularly vulnerable to human trafficking, please see the [U.S. Department of State Trafficking in Persons Annual Report](#) and the July 2011 [FATF Report: Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants](#).

FINCEN ADVISORY

How to Identify Human Smuggling and Human Trafficking Transactions

To help identify and report transactions possibly associated with human smuggling and human trafficking, FinCEN has identified a number of red flags (see [Appendices A and B](#)) that financial institutions may consider incorporating into their monitoring programs. In applying these red flags, financial institutions are advised that no single transactional red flag is a clear indicator of human smuggling or trafficking-related activity. Accordingly, financial institutions should consider additional factors, such as a customer's expected financial activity, when determining whether transactions may be associated with human trafficking.

The red flags described in Appendices A and B may be associated with one or more of the stages of human smuggling or trafficking described above and may be considered by all financial institutions. Some red flags may be common to several types of financial institutions (e.g., banks, money transmitters, credit unions) while other red flags may be unique to a specific type of financial institution. Appendices A and B describe the human smuggling/trafficking stages and/or types of financial institutions most closely associated with each red flag.

In order to more effectively evaluate transactional activity, financial institutions may consider reviewing transactions at the relationship level rather than at the account level. Relationship level reviews allow financial institutions to analyze a customer's transactions across multiple accounts instead of reviewing transactions that are conducted solely through one account. This approach may also be applied when monitoring for any type of suspicious activity to offer financial institutions a more comprehensive perspective on the customer's behavior and activity.

Finally, direct interactions by branch or floor personnel with customers during the course of daily transactions can also alert financial institutions to human smuggling or trafficking-related activity. In many cases, smugglers and traffickers and/or their victims may hold accounts or receive services from financial institutions. Observations made by branch or floor personnel can lead to the identification of anomalous activity that could alert a financial institution to initiate a review of a customer's transactions.

FinCEN Guidance to Financial Institutions

Due to some similarities with legitimate financial activities, financial institutions may consider evaluating indicators of potential human smuggling or trafficking activity in combination with other red flags and factors, such as expected transaction activity, before making determinations of suspiciousness. No one transaction or red flag by itself is a clear indicator of human smuggling or trafficking. Additionally, in making a determination of suspiciousness, financial institutions are encouraged to use previous FinCEN advisories

EXHIBIT 3-A

FINCEN ADVISORY

and guidance as a reference when evaluating potential suspicious activity. For instance, in May 2014 FinCEN published an advisory on the use and structure of funnel accounts,⁴ one of the red flags identified in [Appendices A](#) and [B](#) of this advisory. Financial institutions may consider incorporating the guidance outlined in this advisory in a manner that is commensurate with their risk profile and business model.

In evaluating whether certain transactions are suspicious and/or related to human smuggling or trafficking, financial institutions are encouraged to share information with one another, as appropriate, under Section 314(b) of the USA PATRIOT Act.⁵ Section 314(b) establishes a voluntary information sharing mechanism allowing financial institutions to share information with one another regarding possible terrorist activity or money laundering and provides financial institutions with the benefit of a safe harbor from liability that might not otherwise exist with respect to the sharing of such information.⁶ Thus, suspected money laundering involving the proceeds of human smuggling or human trafficking activity could be shared amongst financial institutions under Section 314(b).

Suspicious Activity Reporting

SARs continue to be a valuable avenue for financial institutions to report suspected human smuggling or trafficking. Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Chapter X, if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should file a Suspicious Activity Report.

To assist law enforcement in targeting instances of human smuggling and trafficking, FinCEN requests that financial institutions include one or both of the below key term(s) in the Narrative and the Suspicious Activity Information:⁷

“ADVISORY HUMAN SMUGGLING” and/or **“ADVISORY HUMAN TRAFFICKING”**

Financial institutions should include one or both terms to the extent that financial institutions are able to distinguish between human smuggling and human trafficking. The narrative should also include an explanation of why the institution knows, suspects, or has reason to

4. See, FinCEN (May, 2014) Advisory [FIN-2014-A005](#) for a detailed description of funnel accounts.
5. Pub. L. No. 107-56, § 314(b). See also, 31 CFR 1010.540.
6. For further guidance related to the 314(b) Program, please see FinCEN’s [Section 314\(b\) Fact Sheet](#) and [FIN-2009-G002](#) (June, 2009), Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act.
7. Financial institutions may include any relevant key terms in the “Other” fields of items 29 through 38, as applicable, of Part II (Suspicious Activity Information) of the SAR.

EXHIBIT 3-A

FINCEN ADVISORY

suspect that the activity is suspicious. It is important to note that a potential victim of human smuggling or trafficking should not be reported as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.


















Questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Resource Center at (800) 767-2825 or (703) 905-3591. ***Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

EXHIBIT 3-A

APPENDIX A: Human Smuggling Red Flags

Financial institutions may choose to use this appendix as a handout for their investigations staff and/or branch personnel. No one transaction or red flag by itself is a clear indicator of human smuggling; accordingly, financial institutions may consider applying these red flags in combination with other factors, such as a customer's profile and expected transaction activity.

Transactional and Customer Red Flags	Who would most likely see the Red Flag?
 Multiple wire transfers, generally kept below the \$3,000 reporting threshold, sent from various locations across the United States to a common beneficiary located in a U.S. or Mexican city along the Southwest Border. ¹	 Money Transmitters  Banks/Credit Unions
 Multiple wire transfers conducted at different branches of a financial institution to or from U.S. or Mexican cities along the Southwest Border on the same day or on consecutive days.	 Money Transmitters/Prepaid Card Providers  Banks/Credit Unions
 Money flows that do not fit common remittance patterns: <ul style="list-style-type: none"> Wire transfers that originate from countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) are directed to beneficiaries located in a U.S. or Mexican city along the Southwest Border. Beneficiaries receiving wire transfers from countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) who are not nationals of those countries. 	 Money Transmitters  Banks/Credit Unions
 Unusual currency deposits into U.S. financial institutions, followed by wire transfers to countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) in a manner that is inconsistent with expected customer activity. This may include sudden increases in cash deposits, rapid turnover of funds and large volumes of cash deposits with unknown sources of funds.	 Money Transmitters  Banks/Credit Unions
 Multiple, apparently unrelated, customers sending wire transfers to the same beneficiary, who may be located in a U.S. or Mexican city along the Southwest Border. These wire senders may also use similar transactional information including but not limited to common amounts, addresses and phone numbers. When questioned to the extent circumstances allow, the wire senders may have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.	 Money Transmitters  Banks/Credit Unions
 A customer's account appears to function as a funnel account, ² where cash deposits (often kept below the \$10,000 reporting threshold) occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.	 Banks/Credit Unions














1. The Southwest Border is generally described as the U.S. – Mexico land border.

2. See, FinCEN (May, 2014) Advisory [FIN-2014-A005](#) for a detailed description of funnel accounts.

EXHIBIT 3-A

APPENDIX A: Human Smuggling Red Flags

continued...

Transactional and Customer Red Flags	Who would most likely see the Red Flag?	
 Checks deposited from a possible funnel account appear to be pre-signed, bearing different handwriting in the signature and payee fields. ³		Banks/Credit Unions
 Frequent exchange of small-denomination for larger denomination bills by a customer who is not in a cash intensive industry. This type of activity may occur as smugglers ready proceeds for bulk cash shipments. ⁴	 Casinos	 Banks/Credit Unions
 When customer accounts near the Southwest Border are closed due to suspicious activity, new customers may begin transacting on behalf of those customers whose accounts have been closed. This may be done as a means to continue illicit activities. In this case, new accounts often reflect activity similar to that of the closed accounts where transactions may be frequently-occurring, currency-intensive and involve individuals that used to receive/send funds from/to accounts previously-closed due to suspicious activity.		 Banks/Credit Unions
 Unexplained/unjustified lifestyle incommensurate with employment or business line. Profits/deposits significantly greater than that of peers in similar professions/business lines.	 Casinos/ Money Transmitters/ Check Cashers/ Prepaid Card Providers	 Banks/Credit Unions
 Inflows are largely received in cash where substantial cash receipts are inconsistent with the customer's line of business. Extensive use of cash to purchase assets and to conduct transactions.	 Money Transmitters/ Check Cashers	 Banks/Credit Unions



























3. See, FinCEN (May, 2014) Advisory [FIN-2014-A005](#) for a detailed description of funnel accounts.

4. See, FinCEN (April, 2006) Advisory [FIN-2006-A003](#) for a detailed description of repatriation of currency smuggled into Mexico from the United States.

EXHIBIT 3-A

APPENDIX B: Human Trafficking Red Flags

Financial institutions may choose to use this appendix as a handout for their investigations staff and/or branch personnel. No one transaction or red flag by itself is a clear indicator of financial institutions may consider applying these red flags in combination with other factors, such as a customer's profile and expected transaction activity.

Transactional Red Flags: Behaviors observed as part of account activity	Who would most likely see the Red Flag?	When most likely to see the Red Flag?
 A business customer does not exhibit normal payroll expenditures (e.g., wages, payroll taxes, social security contributions). Payroll costs can be non-existent or extremely low for the size of the customer's alleged operations, workforce and/or business line/model.	 Banks/Credit Unions	 Exploitation Stage
 Substantial deductions to wages. To the extent a financial institution is able to observe, a customer with a business may deduct large amounts from the wages of its employees alleging extensive charges (e.g., housing and food costs), where the employees only receive a small fraction of their wages; this may occur before or after the payment of wages.	 Check Cashers/ Prepaid Card Providers  Banks/Credit Unions	 Exploitation Stage
 Cashing of payroll checks where the majority of the funds are kept by the employer or are deposited back into the employer's account. This activity may be detected by those financial institutions that have access to paystubs and other payroll records.	 Money Transmitters/ Check Cashers/ Prepaid Card Providers  Banks/Credit Unions	 Exploitation Stage
 The following two red flags may signal anomalous customer activity; however, they should be applied in tandem with other indicators when determining whether transactions are linked to human trafficking. <ul style="list-style-type: none"> Transactional activity (credits and/or debits) inconsistent with a customer's alleged employment, business or expected activity, or where transactions lack a business or apparent lawful purpose. Cash deposits or wire transfers are kept below \$3,000 or \$10,000 in apparent efforts to avoid record keeping requirements or the filing of Currency Transaction Reports (CTRs), respectively. 	 Casinos/ Money Transmitters/ Check Cashers/ Prepaid Card Providers  Banks/Credit Unions	 Recruitment Stage  Transportation Stage  Exploitation Stage
 Frequent outbound wire transfers, with no business or apparent lawful purpose, directed to countries at higher risk for human trafficking ¹ or to countries that are inconsistent with the customer's expected activity.	 Money Transmitters  Banks/Credit Unions	 Recruitment Stage  Transportation Stage  Exploitation Stage
 A customer's account appears to function as a funnel account, ² where cash deposits occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.	 Banks/Credit Unions	 Exploitation Stage

- To view the countries of origin, transit and destination of human trafficking victims, please refer to the [U.S. Department of State Trafficking in Persons Annual Report](#) and the July 2011 [FATF Report: Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants](#).
- See, FinCEN (May, 2014) Advisory [FIN-2014-A005](#) for a detailed description of funnel accounts.

EXHIBIT 3-A

APPENDIX B: Human Trafficking Red Flags

continued...

 Multiple, apparently unrelated, customers sending wire transfers to the same beneficiary. These wire senders may also use similar transactional information including but not limited to a common address and phone number. When questioned to the extent circumstances allow, the wire senders may have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.	 Money Transmitters  Banks/Credit Unions	 Exploitation Stage
 Transactions conducted by individuals, escorted by a third party (e.g., under the pretext of requiring an interpreter), to transfer funds (that may seem to be their salaries) to other countries.	 Money Transmitters/Check Cashers  Banks/Credit Unions	 Exploitation Stage
 Frequent payments to online escort services for advertising, including small posting fees to companies of online classifieds as well as more expensive, higher-end advertising and website hosting companies.	 Money Transmitters/Prepaid Card Providers  Banks/Credit Unions	 Exploitation Stage
 Frequent transactions, inconsistent with expected activity and/or line of business, carried out by a business customer in apparent efforts to provide sustenance to individuals (e.g., payment for housing, lodging, regular vehicle rentals, purchases of large amounts of food).	 Money Transmitters/Prepaid Card Providers  Banks/Credit Unions	 Transportation Stage  Exploitation Stage
 Payments to employment or student recruitment agencies that are not licensed/registered or that have labor violations.	 Money Transmitters/Check Cashers/Prepaid Card Providers  Banks/Credit Unions	 Recruitment Stage  Transportation Stage  Exploitation Stage
Customer Interaction Red Flags: Behaviors observed while interacting with the public	Who would most likely see the Red Flag?	When most likely to see the Red Flag?
 A customer establishes an account or visits a branch to conduct transactions while always escorted by a third party (e.g., under the pretext of requiring an interpreter). Correspondingly, the third party escorting the customer may always have possession of the customer's ID.	 Money Transmitters/Check Cashers  Banks/Credit Unions	 Exploitation Stage
 Common signer(s)/custodian(s) in apparently unrelated business and/or personal accounts. Similarly, common information (e.g., address, phone number, employment information) used to open multiple accounts in different names.	 Banks/Credit Unions	 Exploitation Stage
 Accounts of foreign workers or students where the employer or employment agency serves as a custodian.	 Banks/Credit Unions	 Exploitation Stage
 Unexplained/unjustified lifestyle incommensurate with employment or business line. Profits/deposits significantly greater than that of peers in similar professions/business lines.	 Casinos/Money Transmitters/Check Cashers/Prepaid Card Providers  Banks/Credit Unions	 Recruitment Stage  Transportation Stage  Exploitation Stage
 Inflows are largely received in cash where substantial cash receipts are inconsistent with the customer's line of business. Extensive use of cash to purchase assets and to conduct transactions.	 Money Transmitters/Check Cashers  Banks/Credit Unions	 Recruitment Stage  Transportation Stage  Exploitation Stage



FinCEN ADVISORY

FIN-2020-A007

October 13, 2020

Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic

Detecting and preventing unemployment insurance fraud and other illicit activity related to COVID-19 are critical to safeguarding the integrity of government relief efforts.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: **“COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007”** and select SAR field 34(z) (Fraud - other). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to unemployment insurance (UI) fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of COVID-19-related UI fraud, associated financial red flag indicators, and information on reporting suspicious activity.

This advisory is based on FinCEN’s analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Financial Red Flag Indicators of Unemployment Insurance Fraud Related to COVID-19 Relief

As unemployment claims in the United States have surged due to the pandemic, U.S. law enforcement and financial institutions have detected numerous instances of COVID-19-related UI fraud. The following are representative types of this illicit activity:

- *Fictitious employer-employee fraud:* filers falsely claim they work for a legitimate company, or create a fictitious company and supply fictitious employee and wage records to apply for UI payments;

EXHIBIT 3-A

FINCEN ADVISORY

- *Employer-employee collusion fraud*: the employee receives UI payments while the employer continues to pay the employee reduced, unreported wages;
- *Misrepresentation of income fraud*: an individual returns to work and fails to report the income in order to continue receiving UI payments, or in an effort to receive higher UI payments, an applicant claims higher wages than he/she previously earned;
- *Insider fraud*: state employees use credentials to inappropriately access or change UI claims, resulting in the approval of unqualified applications, improper payment amounts, or movement of UI funds to accounts that are not on the application; or
- *Identity-related fraud*: filers submit applications for UI payments using stolen or fake identification information to perpetrate an account takeover.¹

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider all surrounding facts and circumstances before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent activities related to COVID-19. In line with a risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate.

FinCEN identified the financial red flag indicators described below to alert financial institutions to fraud schemes targeting UI programs, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such fraud.

Financial red flag indicators of UI fraud may include:












Account(s) held at the financial institution receive(s):

- a. UI payments from a state other than the state in which the customer reportedly resides or has previously worked;
- b. Multiple state UI payments within the same disbursement timeframe;
- c. UI payments in the name of a person other than the accountholder, or in the names of multiple unemployment payments recipients;
- d. UI payments and regular work-related earnings, via direct deposit or paper checks;
- e. Numerous deposits or electronic funds transfers (EFTs) that indicate they are UI payments from one or more states to persons other than the accountholder(s);
- f. A higher amount of UI payments in the same timeframe than similarly situated customers received.

1. See, FinCEN Advisory, [FIN-2020-A005](#), "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020). In some situations, fraudsters use the stolen identification information to perpetrate an account takeover. For additional information on identifying account takeover activity, see FinCEN Advisory, [FIN-2011-A016](#), "Account Takeover Activity," (December 19, 2011).

EXHIBIT 3-A

FINCEN ADVISORY

-  2 The customer withdraws the disbursed UI funds in a lump sum by cashier's checks, by purchasing a prepaid debit card, or by transferring the funds to out-of-state accounts.
-  3 The customer's UI payments are quickly diverted via wire transfer to foreign accounts, particularly to accounts in countries with weak anti-money laundering controls.
-  4 The customer receives or sends UI payments to a peer-to-peer (P2P) application or app. The funds are then wired to an overseas account, or withdrawn using a debit card, in a manner that is inconsistent with the spending patterns of similarly situated customers.
-  5 Individuals quickly withdraw disbursed UI funds via online bill payments addressed to an individual(s), as opposed to businesses, as payee(s), with some individual payees receiving multiple online bill paychecks over a short time period.
-  6 The IP address associated with logins for an account conducting suspected UI-fraud activities does not map to the general location of stated address in identity documentation for the customer or where the UI payment originated.
-  7 Individuals direct UI-related EFTs, or deposit UI checks into suspected shell/front company accounts, which may be indicative of money mules transferring these funds in and out of the accounts.
-  8 Multiple accounts receiving UI payments at one or more financial institutions are associated with the same free, web-based email account that may appear in more than one UI application.
-  9 A newly opened account, or an account that has been inactive for more than thirty days, starts to receive numerous UI deposits. After a financial institution suspects UI fraud and requests additional identification documentation to verify the identity(ies) of the customer(s), queried individuals provide documents that are incorrect or forged, which may be an indicator of an account takeover or identity theft.
-  10 After a financial institution suspects UI fraud and conducts due diligence, it determines that the customer does not have a history of living at, or being associated with, the address to which the UI check or UI debit card is sent, or within the geographical area in which the registered debit card is being used.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping unemployment insurance fraud related to the COVID-19 pandemic. Financial institutions should provide all pertinent and available information in the SAR and narrative.

EXHIBIT 3-A

FINCEN ADVISORY

- FinCEN requests that financial institutions reference this advisory by including the key term “COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- Financial institutions also should select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. When addressing unemployment fraud in a SAR, financial institutions should include the keywords “unemployment fraud” in SAR field 34(z).
- When filing a SAR, in addition to standard transaction data, providing the following information is highly valuable to law enforcement: relevant email addresses, IP addresses with their respective timestamps, login information with location and timestamps, cyber-related information and technical indicators, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI)), phone numbers, monikers, and description and timing of suspicious electronic communications.
- Please refer to FinCEN’s [Notice Related to the Coronavirus Disease 2019 \(COVID-19\)](#), which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov. To report suspected illicit activity please visit our website at <https://www.fincen.gov/coronavirus>, which also contains information on registering to receive [FinCEN Updates](#).

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



FinCEN NOTICE

FIN-2020-NTC4

December 28, 2020

FinCEN Asks Financial Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to alert financial institutions about the potential for fraud, ransomware attacks, or similar types of criminal activity related to COVID-19 vaccines and their distribution.¹ As of December 28, 2020, the U.S. Food and Drug Administration (FDA) has issued two emergency use authorizations for COVID-19 vaccines in the United States.² This Notice also provides specific instructions for filing Suspicious Activity Reports (SARs) regarding such suspicious activity related to COVID-19 vaccines and their distribution.

COVID-19 vaccine fraud may include the sale of unapproved and illegally marketed vaccines, the sale of counterfeit versions of approved vaccines, and illegal diversion of legitimate vaccines.³ Already, fraudsters have offered, for a fee, to provide potential victims with the vaccine sooner than permitted under the applicable vaccine distribution plan.⁴

In addition, cybercriminals, including ransomware operators, will continue to exploit the COVID-19 pandemic alongside legitimate efforts to develop, distribute, and administer vaccines. FinCEN is aware of ransomware directly targeting vaccine research, and FinCEN asks financial institutions to stay alert to ransomware targeting vaccine delivery operations as well as the supply chains required to manufacture the vaccines. Financial institutions and their customers should also be alert to phishing schemes luring victims with fraudulent information about COVID-19 vaccines.

1. For additional information, see FinCEN Advisory, [FIN-2020-A002](#), "Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," (May 18, 2020); FinCEN Advisory, [FIN-2020-A006](#), "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," (October 1, 2020); and FinCEN Advisory, [FIN-2020-A005](#), "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020).
2. For current information on COVID-19-related vaccines, see FDA "[COVID-19 Vaccines](#)."
3. See Federal Bureau of Investigation (FBI) Press Release, "[Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines](#)" (December 21, 2020); FDA, "[Beware of Fraudulent Coronavirus Tests, Vaccines and Treatments](#)," (Last update, December 15, 2020); U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) News Release, "[ICE Pivots to Combat COVID-19 Vaccine Fraud with Launch of Operation Stolen Promise 2.0](#)," (November 30, 2020); INTERPOL News Release, "[INTERPOL Warns of Organized Crime Threat to COVID-19 Vaccines](#)," (December 2, 2020); and Europol Early Warning Notification, "[Vaccine-related Crime During the COVID-19 Pandemic](#)," (December 4, 2020).
4. For more information about fraudsters targeting vaccine distribution in the United States, see FBI Press Release, "[Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines](#)" (December 21, 2020); and Federal Trade Commission, "[COVID-19 Vaccines are in the Pipeline. Scammers Won't be Far Behind](#)," (December 8, 2020).

EXHIBIT 3-A

FINCEN NOTICE

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of Bank Secrecy Act (BSA) compliance requirements by financial institutions, is crucial to identifying and stopping fraud, cybercrime, and cyber-enabled crime, including those related to the COVID-19 vaccine. Financial institutions should provide all pertinent information in the SAR.

- FinCEN requests that financial institutions reference “**FIN-2020-NTC4**” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice.
- Financial institutions should also select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include the type of fraud and/or name of the scam or product (e.g., vaccine scam or vaccine ransomware) in SAR field 34(z).
- FinCEN requests that filers further detail the reported activity in the narrative portion of the SAR. If the activity is suspected of being a scam, filers should provide known details about how the scammers contacted the victim, how the victim provided or attempted to provide payment related to the scam, and any other available details including data related to the financial transactions or method of contact, such as Internet Protocol (IP) addresses and phone numbers. For guidance on ransomware attacks, see FinCEN Advisory, [FIN-2020-A006](#), “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” (October 1, 2020).
- Please refer to FinCEN’s May 2020 [Notice Related to the Coronavirus Disease 2019 \(COVID-19\)](#), which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations

For Further Information

Additional COVID-19-related information, including advisories and notices, can be found on FinCEN’s website at <https://www.fincen.gov/coronavirus>, which also contains information on how to register for [FinCEN Updates](#).

Questions or comments regarding the contents of this notice should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



FinCEN ADVISORY

FIN-2021-A001

February 2, 2021

Advisory on COVID-19 Health Insurance- and Health Care-Related Fraud

While FinCEN has observed a wide range of COVID-19 related fraud, this advisory primarily focuses on COVID-19-related fraud involving the health care industry.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: “**FIN-2021-A001**” and select SAR field 34g (health care – public or private health insurance). Additional guidance for filing SARs appears near the end of this advisory.

enforcement partners. Additional COVID-19-related information is located on FinCEN’s website at <https://www.fincen.gov/coronavirus>, which also contains information on how to register for [FinCEN Updates](#).

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to health insurance and health care frauds related to the COVID-19 pandemic. These frauds target Medicare, Medicaid/Children’s Health Insurance Program (CHIP), and TRICARE as well as health care programs provided through the Departments of Labor and Veterans Affairs (collectively, “health care benefit programs”) and private health insurance companies. In addition, the United States government has observed frauds in connection with COVID-19 relief funds for health care providers, such as those provided under the Paycheck Protection Program and Health Care Enhancement Act (PPP-HCEA).¹ This advisory contains descriptions of COVID-19-related fraud involving health care benefit programs and health insurance, associated financial red flag indicators, select case studies, and information on reporting suspicious activity.

This advisory is based on FinCEN’s analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, public reporting, and law

1. See Pub. L. No. 116-139.

EXHIBIT 3-A

FINCEN ADVISORY

Financial Red Flag Indicators of COVID-19 Health Insurance- and Health Care-Related Fraud Activity

Law enforcement and financial institutions have detected numerous instances of potential frauds related to health care benefit programs, health insurance, and COVID-19 health care relief funds.² Criminals are adapting known health insurance and health care fraud to take advantage of the pandemic. The following are representative types of this illicit activity:

- *Unnecessary services:* Ordering or submitting claims for expensive tests or services that do not test for COVID-19, oftentimes in conjunction with COVID-19 testing, such as medically unnecessary and expensive respiratory testing, allergy testing, genetic testing, narcotics screening, or whole-body health assessments,³ or providing testing for services not usually rendered by the company.
- *Billing schemes:* Billing for services not provided, or overbilling (e.g., upcoding or unbundling), when administering or processing COVID-19 testing and treatments.⁴
- *Kickbacks:* Paying service providers or purported marketing organizations an illegal kickback or bribe in exchange for ordering, or arranging for the ordering of, services and testing.
- *Health care technology schemes:* False and fraudulent representations about COVID-19 testing, treatments, or cures are used to defraud insurance carriers and to perpetrate fraud on the financial markets by defrauding investors.⁵
- *Telefraud and telehealth schemes:* Collecting beneficiaries' personally identifiable information (PII), including Medicare information. Solicitations will often link their requests for information to COVID-19 treatment and prevention, such as testing or protective equipment. Fraudsters then submit fraudulent claims for payment from health care benefit programs. Fraudsters have also used the stolen PII to submit fraudulent telehealth services claims.⁶

-
2. For information concerning frauds related to the COVID-19 vaccine, see FinCEN Notice, [FIN-2020-NTC4](#), "FinCEN Asks Financial Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks," (December 28, 2020).
 3. See Department of Justice (DOJ) Press Releases, "[United States Attorney's Office Announces Charges in Fraud Cases Related to COVID-19](#)," (May 27, 2020) and "[Georgia Woman Arrested for Role in Scheme to Defraud Health Care Benefit Programs Related to Cancer Genetic Testing and COVID-19 Testing](#)," (May 15, 2020).
 4. See DOJ Press Releases, "[Two Owners of New York Pharmacies Charged in a \\$30 Million COVID-19 Health Care Fraud and Money Laundering Case](#)," (December 21, 2020); and "[United States Attorney's Office Announces Charges in Fraud Cases Related to COVID-19](#)," (May 27, 2020). Upcoding occurs when a provider bills the insurance company for higher and more expensive levels of medical service than were actually performed. Unbundling fraud occurs when a provider bills for multiple codes for a group of procedures that are covered in a single global billing code.
 5. See DOJ Press Release, "[Medical Technology Company President Charged in Scheme to Defraud Investors and Health Care Benefit Programs in Connection with COVID-19 Testing](#)," (June 9, 2020). For additional information, including red flags for fraudulent COVID-19 testing, treatments, and cures, see FinCEN Advisory, [FIN-2020-A002](#), "Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," (May 18, 2020).
 6. See HHS-OIG Fraud Alert, "[COVID-19 Fraud is Rapidly Evolving](#)," (Last update, December 21, 2020) and "[National Telefraud Takedown Scheme](#)" (Current as of September 2020).

EXHIBIT 3-A

FINCEN ADVISORY

- *Fraudulently obtaining COVID-19 health care relief funds:* Filing false claims and applications for Federal relief funds,⁷ such as those provided under the Coronavirus Aid, Relief, and Economic Security (CARES) Act's Provider Relief Fund,⁸ the PPP-HCEA,⁹ or the Economic Impact Disaster Loan (EIDL) program, and the claim or application has a nexus to health care benefit programs.¹⁰
- *Identity theft leading to additional fraud:* Targeting beneficiaries for their PII and then using the stolen PII to commit COVID-19-related fraud against health care benefit programs.¹¹

To discern whether a health insurance fraud is COVID-19-related, financial institutions should assess whether the activity occurred around or after the Secretary of Health and Human Services' public health emergency declaration of January 31, 2020,¹² and whether the underlying purported service relates to COVID-19.

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider all surrounding facts and circumstances before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent activities related to COVID-19. In line with a risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate.

FinCEN identified the financial red flag indicators described below to alert financial institutions to fraud related to health insurance and health care, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such COVID-19-related fraud.

Such financial red flag indicators may include:

Additional, medically unnecessary services or billing schemes

- 1** After the COVID-19 public health emergency declaration, a health care service provider's account receives or continues to receive: (1) health care benefit program or health insurance payments well above the provider's estimated business transactions; or (2) payments at

7. See DOJ Press Releases, "[Florida Man Charged with COVID Relief Fraud, Health Care Fraud and Money Laundering](#)," (July 29, 2020); "[Florida Man Charged with COVID Relief Fraud and Health Care Fraud](#)," (July 10, 2020); and "[Ophthalmologist Previously Charged with Health Care Fraud Indicted For Defrauding SBA Program Intended To Help Small Businesses During COVID-19 Pandemic](#)," (June 24, 2020).

8. See U.S. Department of Health and Human Services (HHS), "[CARES Act Provider Relief Fund](#)," (Last reviewed on January 21, 2021).

9. See Pub. L. No. 116-139. For more information about unemployment insurance fraud, not necessarily connected to the health care industry, see FinCEN Advisory, [FIN-2020-A007](#), "Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic," (October 13, 2020).

10. See Pub. L. No. 116-123 and U.S. Small Business Administration, Information Notice [5000-20037](#), "Guidance Regarding Identification and Reporting of Suspicious Activity in the COVID-19 EIDL Loan Program," (July 22, 2020).



11. See HHS-Office of Inspector General (OIG) Fraud Alert, "[COVID-19 Fraud is Rapidly Evolving](#)," (Last update, December 21, 2020). For more information about identity theft related to COVID-19 relief efforts, including red flags, see FinCEN Advisory, [FIN-2020-A005](#), "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020); and FinCEN Advisory, [FIN-2020-A003](#), "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020).

12. See HHS, "[Determination that a Public Health Emergency Exists](#)," (January 31, 2020).

EXHIBIT 3-A

FINCEN ADVISORY

the same volume despite an expected diminished activity level during the public health emergency (e.g., a non-emergency medical transport company receiving higher than expected payments during stay-at-home orders).

-  A health care service provider's account receives health care benefit program or health insurance payments beyond the expected type or volume of service, based on staffing and other characteristics of the business (e.g., processing COVID-19 tests when the medical facility does not typically offer diagnostic services, or the facility is processing a high volume of tests despite only employing a few medical personnel).
-  A COVID-19-related health care service provider's business account has unusual transaction activities, such as payments for personal or medically irrelevant expenses (e.g., payments to automobile dealers, travel agents, or retailers of luxury goods).

Potential fraudulent businesses







-  Following the COVID-19 public health emergency declaration, personal or business accounts, especially ones that did not previously receive health care-related payments, begin receiving steep increases in health care benefit program or health insurance payments.
-  A purported health care service provider's account receives health care benefit program or health insurance payments related to COVID-19 services, and then individuals immediately withdraw the funds in a manner that is not typical for health care businesses (e.g., cashier's checks, cash withdrawals, certain types of Automated Clearing House (ACH) transfers, or domestic and international wire transfers).
-  After the COVID-19 public health emergency determination, a purported health care provider's account does not receive small-dollar check deposits, payments from merchant fee servicers, or cash payments from patients that would indicate patient copayments. This may indicate the absence of actual business activity.
-  A newly formed health care business account has a volume or type of payment that seems inconsistent with expected levels of activity for such an account.
-  The physical location of a purported medical facility receiving reimbursements for COVID-19-related health care services or relief funds is non-existent, a residential address, a commercial mail receiving agency address (e.g., a UPS Store address), or another non-office building address (e.g., a purported medical facility is listed as a laboratory, but the physical address is a vacant lot, car dealership, restaurant, or retail store).
-  The purported laboratory, health care service provider, or medical service personnel or their counterparties appear to have a minimal web presence, or one that begins around the time of the COVID-19 public health emergency declaration.

EXHIBIT 3-A

FINCEN ADVISORY

- 10** Following the public health emergency declaration, the physical location of a purported medical facility receiving payments for health care services or relief funds is far from the physical location of the majority of its patients or the providers purported to be practicing there, unless the facility is providing appropriate telehealth services (e.g., a purported medical facility located in a western state receives payments related to patients residing on the East Coast).

Kickbacks and money laundering

- 11** After the COVID-19 public health emergency declaration, a health care service provider's or other business account begins having overly complex, medical-related transactions involving multiple counterparties indicative of possible structuring, layering, kickbacks, or fraudulent medical claims.
- 12** A health care service provider's account makes frequent or unusually large payments recorded as advertising or marketing expenses, or makes recurring round-dollar payments to one or multiple individuals in a manner inconsistent with its payroll-related withdrawals. The payments may reference "director fees," "consulting fees," "marketing," or "business process outsourcing."
- 13** A health care service provider starts receiving payments from laboratories and health care services companies, but there is no financial documentation (e.g., operating expense payments) that the provider rendered legitimate services. When questioned, the provider indicates that he or she invested in the company and the payments are dividends or payments for services (e.g., a laboratory pays a physician for services related to a COVID-19 laboratory test). The tests, however, are not related to the physician's specialization or do not normally require a physician's involvement.

Fraudulently obtaining COVID-19-relief funds¹³

- 14** An account with no previous known association with providing health care services, receives an unexpected or excessive COVID-19-related payment that appears to be the CARES Act's Provider Relief Fund or the PPP-HCEA payments. Shortly after the account receives the deposit, an individual(s) withdraws the funds via large cash withdrawals, cashier's checks, wires to an overseas account, transfers to personal accounts, or payments for non-business expenses.
- 15** An account previously associated with providing health care services but that has not been recently active or appears to be defunct, receives an unexpected or excessive COVID-19-related payment that appears to be the CARES Act's Provider Relief Fund or the PPP-HCEA payments.
- 16** An account holder receives a substantial amount of reimbursements from health care benefit programs or health insurance companies for services rendered at the same time that the account holder receives COVID-19-related unemployment insurance payments.¹⁴

13. These red flag indicators pertain only to suspicious activity with a nexus to the health care industry and COVID-19. For non-health care industry suspicious activities related to COVID-19, please review FinCEN's prior COVID-19 related advisories and notices located on FinCEN's website at <https://www.fincen.gov/coronavirus>.

14. For more information about COVID-19-related unemployment insurance fraud, see FinCEN Advisory, [FIN-2020-A007](#), "Advisory on Unemployment Insurance Fraud during the Coronavirus Disease 2019 (COVID-19) Pandemic," (October 13, 2020).

Case Studies

Two Owners of New York Pharmacies Charged in a \$30 Million COVID-19 Health Care Fraud and Money Laundering Case¹⁵

Federal authorities indicted two owners of several New York-area pharmacies for their alleged roles in a \$30 million health care fraud and money laundering scheme. The indictment alleges that the defendants acquired control over dozens of New York pharmacies by paying others to pose as the owners of the pharmacies and hiring pharmacists to pretend to be supervising pharmacists at the pharmacies, for the purpose of obtaining pharmacy licenses and insurance plan credentialing. According to the indictment, the defendants used COVID-19 emergency override billing codes to submit fraudulent claims to Medicare, for which they were allegedly paid over \$30 million for medications that never were purchased by the pharmacies, prescribed by physicians, or dispensed to patients. The defendants frequently filed such claims during periods when pharmacies were non-operational, and used doctors' names on prescriptions without their permission.

The indictment also alleges that, with the proceeds of the fraud, the defendants engaged in a complex, money laundering conspiracy where they created sham pharmacy wholesale companies and fabricated invoices to legitimate pharmaceutical drug purchases. In a first phase, the defendants conspired with an international money launderer who arranged for funds to be wired from the sham pharmacy wholesale companies to companies in China for distribution to individuals in Uzbekistan. The defendants received cash in exchange, provided for by members of the Uzbekistani immigrant community to an unlicensed money transfer business for remittance to their relatives in Uzbekistan, minus a commission that was deducted by the money launderer. In a second phase, when the amount of fraudulent proceeds exceeded the amount of cash available in the Uzbekistani immigrant community, the defendants directed the international money launderer to transfer funds back from the sham wholesale companies to the defendants, their relatives, or their designees, in the form of certified cashier's checks and bags of cash. The defendants used the proceeds of the scheme to purchase real estate and other luxury items.

15. See DOJ Press Release, "[Two Owners of New York Pharmacies Charged in a \\$30 Million COVID-19 Health Care Fraud and Money Laundering Case](#)," (December 21, 2020).

EXHIBIT 3-A

FINCEN ADVISORY

Medical Technology Company President Charged in Scheme to Defraud Investors and Health Care Benefit Programs in Connection with COVID-19 Testing¹⁶

The president of a California-based medical technology company allegedly paid kickbacks and bribes to marketers and doctors to run an allergy screening test for 120 allergens on every patient regardless of medical necessity. As the COVID-19 pandemic progressed and many patients in the United States faced difficulty obtaining access to COVID-19 testing, the company president sought to expand the pre-existing allergy test scheme and capitalize on a national emergency for financial gain by combining the COVID-19 test with the more expensive allergy testing which did not identify or detect COVID-19. In addition, the company president allegedly made false claims to investors concerning the company's ability to provide accurate, fast, reliable, and cheap COVID-19 tests. The Fraud Section of the Criminal Division of the Department of Justice and the U.S. Attorney's Office for the Northern District of California charged the individual in connection with his alleged participation in schemes to mislead investors, to manipulate the company's stock price, and to conspire to commit health care fraud in connection with the submission of over \$69 million in false and fraudulent claims for allergy and COVID-19 testing. HHS-OIG, the U.S. Postal Inspection Service, the Federal Bureau of Investigation, the Veterans Affairs Office of Inspector General, and the Defense Criminal Investigative Service investigated the case.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of BSA compliance requirements by financial institutions, is crucial to identifying and stopping health insurance and health care frauds, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent information in the SAR. Following these filing instructions will make it easier for FinCEN, law enforcement, supervisors, and other relevant government agencies to identify and utilize the information submitted in the SAR.¹⁷

- FinCEN requests that financial institutions reference this advisory by including the key term "FIN-2021-A001" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

16. See DOJ Press Release, "[Medical Technology Company President Charged in Scheme to Defraud Investors and Health Care Benefit Programs in Connection with COVID-19 Testing](#)," (June 9, 2020).

17. FinCEN requests that financial institutions only reference this advisory if the suspicious activity relates to the health care industry and COVID-19. For non-health care industry suspicious activities related to COVID-19, please review FinCEN's prior COVID-19 related advisories and notices located on FinCEN's website at <https://www.fincen.gov/coronavirus>.

EXHIBIT 3-A

FINCEN ADVISORY

- Financial institutions also should select SAR field 34(g) (health care – public or private health insurance) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include additional detail about the type of health care fraud (e.g., Medicare – services not provided) in the narrative.
- FinCEN requests that financial institutions wishing to report potential health care fraud unrelated to COVID-19 should not include this advisory’s key term in SAR field 2 or the SAR’s narrative portion. Instead, please select field 34(g) and detail the activity in the narrative (e.g. addiction treatment – services not provided; or pain clinic – “marketing” fees).
- Please refer to FinCEN’s [May 2020 Notice Related to the Coronavirus Disease 2019 \(COVID-19\)](#) which contain information regarding reporting COVID-19-related crime, and remind financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

To report suspected health care fraud, waste, or abuse within Medicare, Medicaid, CHIP, or the Marketplaces, please go to the following website to determine the best resource to notify:
<https://www.cms.gov/About-CMS/Components/CPI/CPIReportingFraud>.

For the general public to report suspected fraud, waste, or abuse in Medicare or Medicaid call the HHS OIG at 1-800-HHS-TIPS (1-800-447-8477).

The mission of FinCEN is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.



FinCEN ADVISORY

FIN-2021-A002

February 24, 2021

Advisory on Financial Crimes Targeting COVID-19 Economic Impact Payments

Detecting, preventing, and reporting financial crimes related to Economic Impact Payments is vital to the United States' economic recovery, and critical to protecting innocent people from harm.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR filing request

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**FIN-2021-A2002**" and select SAR field 34(z) (Fraud - other). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to fraud and other financial crimes related to the Economic Impact Payments (EIPs),¹ authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act,² and the Coronavirus Response and Relief Supplemental Appropriations Act of 2021.³

This advisory contains descriptions of EIP fraud, associated red flag indicators, and information on reporting suspicious activity. This Advisory is part of a series published by FinCEN on COVID-19-related frauds and criminal activity.⁴

This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, public reporting, and law enforcement partners. Additional COVID-19-related information is located on FinCEN's website at <https://www.fincen.gov/coronavirus>, which also contains information on how to register for [FinCEN Updates](#).

1. For more information about EIPs, see Treasury Press Release, "[Treasury and IRS Begin Delivering the Second Round of Economic Impact Payments to Millions of Americans](#)," (December 29, 2020); and Internal Revenue Service (IRS) [Economic Impact Payment Information Center](#), (Last updated February 17, 2021) and [Coronavirus and Economic Impact Payments: Resources and Guidance](#), (Last updated February 17, 2021). If Congress authorizes any future payments, please monitor these resources for information related to any additional payments.
2. Public Law [116-136](#).
3. Public Law [116-260](#).
4. For a complete listing of FinCEN's COVID-19-related publications, please visit FinCEN's [Coronavirus webpage](#).

FINCEN ADVISORY

EIP-Related Fraud and Theft

U.S. authorities have detected a wide range of EIP-related fraud and theft involving a variety of criminal actors. The following examples are a non-exhaustive list of this type of criminal activity.

- *Fraudulent checks:* Fraudsters send potential victims fraudulent checks, instructing the recipients to call a number or verify information online in order to cash the fraudulent EIP checks. Victims are asked for personal or banking information under the guise that the information is needed to receive or speed up their EIP. Fraudsters then use the information obtained to commit various crimes, such as identity theft and the unauthorized access of bank accounts.⁵
- *Altered checks:* Fraudsters deposit altered EIP checks, often via automated teller machine (ATM) or mobile device. These altered checks may modify the name of the payee, or leave the name blank, and the amount may be altered prior to deposit. There is reporting of checks being chemically altered so the original payee is removed.
- *Counterfeit checks:* Fraudsters deposit counterfeit EIP checks, often via ATM or mobile device. Fraudsters have various methods to create a counterfeit check, including checks reproduced from digital images of checks issued by the U.S. Department of the Treasury. However, such counterfeit checks will often have irregularities involving the check number, paper, coloring, and/or font.
- *Theft of EIP:* Such thefts can include individuals stealing an EIP from the U.S. mail; requesting an EIP disbursement for an ineligible person; seeking another person's EIP without the payee's knowledge and/or approval, or through coercive means; or using stolen Personally Identifiable Information (PII), including providing false bank account information to the IRS to claim an EIP.
- *Phishing schemes using EIP as a lure:* Fraudsters perpetrate phishing schemes using emails, letters, phone calls, and text messages containing keywords such as "Corona Virus," "COVID-19," and "Stimulus," with the purpose of obtaining PII and financial account information, such as account numbers and passwords.⁶
- *Inappropriate seizure of EIP:* A private company that may have control over a person's finances or serves as his or her representative payee seizes a person's EIP, for wage garnishments or debt collection, and does not return the inappropriately seized payments.⁷




5. See IRS News Release, "[IRS Issues Warning about Coronavirus-related Scams; Watch Out for Schemes Tied to Economic Impact Payments](#)," (April 2, 2020).
6. See IRS News Release, "[IRS Warns Against COVID-19 Fraud; Other Financial Schemes](#)," (June 8, 2020). For more information about phishing schemes and identity theft related to COVID-19-relief efforts, including red flags, see FinCEN Advisory, [FIN-2020-A005](#), "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020); and FinCEN Advisory, [FIN-2020-A003](#), "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020).
7. See Social Security Administration, [Second Economic Impact Payment](#) (Last updated January 15, 2021) and [Economic Impact Payments Paid by the CARES Act](#) (Last updated November 23, 2020); and IRS Press Release, "[Economic Impact Payments Belong to Recipient, not Nursing Homes or Care Facilities](#)," (June 16, 2020).

FINCEN ADVISORY

Red Flag Indicators of Financial Crimes Related to EIPs

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider all surrounding facts and circumstances before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent activities related to COVID-19. In line with a risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate. FinCEN has identified the financial red flag indicators described below to alert financial institutions to potential fraud and thefts related to EIPs as well as to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such activities. Such financial red flag indicators may include:



Fraudulent, altered, counterfeit, or stolen EIP checks, Automated Clearing House (ACH) deposits, and prepaid debit cards

-  1 An account holder attempts to deposit one or more checks that appear to be issued by the U.S. Treasury, but are fraudulent or counterfeit checks.⁸ When questioned, the customer may disclose that he or she:
 - (i) was sent a partial payment, and needed to verify his or her PII or financial information before receiving the full EIP; or
 - (ii) received the check purportedly from a current or former employer with instructions that the check was the customer's "stimulus payment" and that he or she was to buy prepaid cards and send them to another individual.
-  2 An existing account receives, or an account holder makes, multiple EIP-related deposits for individuals other than the account holder(s), and the individuals named on the checks reside outside the geographic region of the account holder, or do not have a history at the account holder's purported address. This may be indicative of funnel account activities in which multiple EIPs are deposited or transferred throughout the United States into one account, which may be held by a fraudster or a money mule working for the fraudster.
-  3 An existing account receives an excessive number of EIPs via U.S. Treasury check or deposits related to a prepaid debit card linked to the same address (e.g., an account receiving more checks than expected relative to the customer's profile and financial institution's customer due diligence).







8. The U.S. Secret Service (USSS) and the Department of the Treasury announced several security features in official U.S. Treasury checks. See USSS Press Release, "[U.S. Secret Service in Partnership with the U.S. Department of the Treasury Launch – Know Your U.S. Treasury Check Campaign](#)," (April 20, 2020). For a description of the official U.S. Treasury check, see [U.S. Treasury Check Security Features](#), (April 2020). The status of EIP and other Treasury checks can be determined by using Treasury's Bureau of Fiscal Services' [Treasury Check Verification System \(TCVS\)](#).

EXHIBIT 3-A


FINCEN ADVISORY

-  4 A customer opens a new account with an EIP check or debit card, and the name of the potential account holder is different from that of the depositor or the payee of EIP.
-  5 The EIP check is deposited, or the debit card's funds are transferred, into dormant accounts with little or no prior activity.

Theft of multiple EIPs

-  6 Individual accounts opened after the U.S. government announced the EIP program, receive U.S. Treasury checks or direct deposits from the U.S. Treasury that could indicate multiple EIPs, and for individuals other than the account holder.
-  7 The account holder is a child under age 17 at the end of the taxable year, but the account received numerous EIPs.
-  8 Rapid transfers of multiple EIPs into one account could indicate that bad actors are consolidating the payments. After the funds are consolidated, the funds may be quickly (a) withdrawn via large cash withdrawals or serial ATM withdrawals; (b) used to purchase convertible virtual currencies (CVC); (c) transferred out of the account via a money services business such as cryptocurrency exchangers and peer-to-peer mobile payment systems, or wire transfers to other accounts; (d) used for large purchases at merchants that offer cash back as an option, in amounts not typical of this type of merchant; or (e) transferred onto prepaid debit or gift cards.
-  9 An account receives several EIP-related deposits and almost immediately thereafter (a) disburses funds for large purchases at merchants that offer cash back as an option, in amounts not typical of this type of merchant, or (b) has funds transferred onto prepaid debit or gift cards.
-  10 Deposits of one or more EIP U.S. Treasury checks or electronic deposits made into an account held by (a) a retail business, or (b) a personal account of a business owner or employee and the account holder is not the payee/endorser. This may indicate that the business is using identifiers of its employees or customers to apply for their EIP benefits for the purpose of inappropriately collecting the payments.
-  11 The same Internet Protocol (IP) address is used to transfer funds from several EIP debit cards to a bank account, especially if that IP address is located outside of the United States or associated with a business.

Other frauds and thefts occurring in an account receiving EIPs

-  12 An account receives (a) numerous deposits or electronic funds transfers (EFTs) that indicate the payments are linked to EIPs, and (b) unemployment insurance payments⁹ from one or more states in names that do not match the account holder(s).

9. FinCEN Advisory, [FIN-2020-A007](#), "Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic," (October 13, 2020).

FINCEN ADVISORY

- 13** An account with several EIP deposits also receives numerous tax refunds from federal and state governments for individuals other than the account holder(s). The names indicated on the EIPs and tax returns may be the same but are not those of the account holder(s).
- 14** Deposits of one or more EIP checks or electronic deposits are made into a nursing home or assisted living facility's business account and those payments have not been returned to the resident. This may be an indication that the business is inappropriately withholding residents' EIP funds.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of BSA compliance requirements by financial institutions, is crucial to identifying and stopping EIP-related fraud and theft. Financial institutions should provide all pertinent information in the SAR.

- FinCEN requests that financial institutions reference this advisory by including the key term **"FIN-2021-A002"** SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- FinCEN also requests that filers mention **"economic impact payment"** in the SAR narrative along with any other relevant behavior, such as counterfeit checks, money mule activity, or identity theft, to indicate a connection between those activities and EIP frauds and thefts. Additionally, FinCEN requests that filers use this program-specific term and avoid relying on generalized key terms, such as "stimulus check."
- Financial institutions should also select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include the type of fraud and/or name of the scam or product (e.g., economic impact payment) in SAR field 34(z).
- FinCEN requests filers not report the potential victim of an EIP fraud scheme as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.
- Please refer to FinCEN's May 2020 [Notice Related to the Coronavirus Disease 2019 \(COVID-19\)](#) and February 2021 [Consolidated COVID-19 Suspicious Activity Report Key Terms and Filing Instructions](#), which contain information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.



FinCEN NOTICE

FIN-2021-NTC2

March 9, 2021

FinCEN Informs Financial Institutions of Efforts Related to Trade in Antiquities and Art

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to inform financial institutions about (1) the Anti-Money Laundering Act of 2020 (the AML Act)¹ efforts related to trade in antiquities and art, (2) select sources of information about existing illicit activity related to antiquities and art, and (3) provide specific instructions for filing Suspicious Activity Reports (SARs) related to trade in antiquities and art. FinCEN encourages financial institutions to continue filing SARs regarding these topics.

New AML Act Measures

- *Antiquities Regulations:* Section 6110(a) of the AML Act amends the definition of “financial institution” under the Bank Secrecy Act (BSA) to include persons “engaged in the trade of antiquities” and directs FinCEN to promulgate implementing regulations. The BSA obligations imposed by Section 6110(a) will take effect on the effective date of those final regulations.
- *Art Study:* Section 6110(c) of the AML Act requires the Secretary of the Treasury, in coordination with the Director of the Federal Bureau of Investigation, the Attorney General, and the Secretary of Homeland Security, to perform a study of the facilitation of money laundering and the financing of terrorism through the trade in works of art. The study will include an analysis of, among other things, which markets should be subject to regulations and the degree to which the regulations, if any, should focus on high-value trade in works of art, and on the need to identify the actual purchasers of such works, in addition to other persons engaged in the art trade.

Illicit Activity Associated with Trade in Antiquities and Art

Financial institutions with existing BSA obligations, including the reporting of suspicious activity, should be aware that illicit activity associated with the trade in antiquities and art may involve their institutions. Crimes relating to antiquities and art may include looting or theft, the illicit excavation of archaeological items, smuggling, and the sale of stolen or counterfeit

1. The AML Act was enacted into law as part of the National Defense Authorization Act for Fiscal Year 2021, Public Law 116-283.

EXHIBIT 3-A

FINCEN NOTICE

objects.² Crimes relating to antiquities and art also may include money laundering and sanctions violations, and have been linked to transnational criminal networks, international terrorism, and the persecution of individuals or groups on cultural grounds.³

SAR Filing Instructions

Financial institutions' SAR reporting, in conjunction with effective implementation of their other BSA compliance requirements, is crucial to identifying and stopping money laundering and other crimes related to trade in antiquities and art.

- FinCEN requests that financial institutions reference "FIN-2021-NTC2" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice.
- Financial institutions should also select SAR field 36(z) (Money Laundering - other) as the associated suspicious activity type, and note if the suspicious activity relates to "Antiquities," "Art," or both (in some instances, an object could be considered both an antiquity and a work of art).

SAR Narrative. FinCEN also requests that filers detail the reported activity in the narrative portion of the SAR, explaining how the suspicious activity relates to "Antiquities," "Art," or both. Filers should provide any available details that may assist in the identification of (1) the objects connected to the financial transactions, (2) other transactions or proposed transactions that may involve antiquities or art, and (3) any other relevant information. Filers should provide all available details (such as names, identifiers, and contact information—including Internet Protocol (IP) and email addresses and phone numbers) regarding (1) the actual purchasers or sellers of the property, and their intermediaries or agents, (2) the volume and dollar amount of the transactions involving an entity that is—or may be functioning as—a dealer in antiquities or art, and (3) any beneficial owner(s) of entities (such as shell companies). In the case of *stolen art or antiquities*, filers should provide a detailed and specific description of the stolen item(s) and indicate whether photographs of the items are available. Filers should also provide information about the place(s) where the reported individuals or entities are operating.

-
2. INTERPOL, "[The Issues – Cultural Property](#)," (Last Accessed March 8, 2021).
 3. U.S. Senate, Permanent Subcommittee on Investigations, "[The Art Industry and U.S. Policies that Undermine Sanctions](#)," (July 29, 2020); INTERPOL, "[The Issues – Cultural Property](#)," (Last Accessed March 8, 2021); U.S. Department of State, "[Tackling Illicit Trafficking of Antiquities and its Ties to Terrorist Financing](#)," (June 20, 2018); U.N. Office on Drugs and Crime, "[Links Between Terrorism, Crime and Trafficking in Cultural Property/Antiquities](#)," (March 2019); Financial Action Task Force, "[Emerging Terrorist Financing Risks](#)," (October 2015); U.S. Department of the Treasury, Office of Foreign Assets Control, "[Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork](#)," (October 30, 2020); Congressional Research Service, "[Transnational Crime Issues: Arts and Antiquities Trafficking](#)," (March 1, 2021).

EXHIBIT 3-A

Suspicious Activity Reporting (SAR) Questions

True or False

- _____ 1. Six different SAR forms are in use by the various industry groups filing suspicious activity reports.
- _____ 2. For banks, S&Ls and credit unions, the initial SAR is filed within thirty days of the date of determination, assuming the presence of a subject.
- _____ 3. An updating (continuing) SAR, when needed, is filed every 90 business days.
- _____ 4. The Narrative to the SAR (Part V) is the most important section of the SAR itself?
- _____ 5. \$Zero is the mandatory filing limit of the SAR Form 111 when a suspect is known.
- _____ 6. Documentation of the decision and the decision process when the SAR is not filed is the most important “retained record” of a SAR “event”.
- _____ 7. The safe harbor provision protects financial institutions from civil liability for all reports of suspicious transactions made to appropriate authorities, such as law enforcement officials.
- _____ 8. To safeguard the confidentiality of the SAR process, the minutes of the Board meeting at which the SAR was discussed should not contain any record of such discussion.
- _____ 9. \$25,000 is the mandatory compulsion limit when there is no identified subject on the SAR.
- _____ 10. For banks, S&Ls, and credit unions, the most often reported crime on the SAR has been Elder Financial Exploitation.
- _____ 11. A suspicious currency transaction more than \$10,000 can be reported using either the SAR or the CTR form.
- _____ 12. Banks send the supporting documentation along with the SAR form that is filed.
- _____ 13. A suspicious transaction is anything under the circumstances, which is suspicious.
- _____ 14. The “gag order” which becomes effective with the filing of any SAR prohibits banks from notifying any person involved in the transaction that the transaction has been reported.
- _____ 15. Section 314(a) “matches” are reported to FinCEN using the SAR.
- _____ 16. Blocked or rejected SDN transactions are reported to FinCEN using the SAR.
- _____ 17. Human trafficking exploitations are never reported using the SAR.
- _____ 18. Check kiting is no longer reported on Form 1

EXAMINATION PROCEDURES

I. INTRODUCTION

- A. Overview** – The FFIEC’s *Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual* provides guidance to examiners for carrying out BSA/AML and OFAC examinations. An effective BSA/AML compliance program requires sound risk management, and the examination manual continues to emphasize a financial institution’s responsibility to establish and implement risk-based policies, procedures, and processes to comply with the BSA, and to safeguard its operations from money laundering and terrorist financing. The examination manual provides guidance on identifying and controlling the risks associated with money laundering and terrorist financing and is available at: <https://bsaaml.ffiec.gov/manual>.

First released in its present format in 2005, and last fully updated in late 2014, “pieces” of the manual have been added/updated three times since 2014 and include:

- February 25, 2021 – Four “topics” within the “Assessing Compliance with BSA Regulatory Compliance” section (Introduction, Customer Identification (CIP), Currency Transaction Reporting (CTR), and CTR Exemptions) were updated, and are available at: <https://www.ffiec.gov/press/pr022521.htm>
- April 15, 2020 – Four sections (Scoping and Planning, BSA/AML Risk Assessment, Assessing the BSA/AML Compliance program, and Developing Conclusions and Finalizing the Exam) were updated to provide further transparency into the BSA/AML examination process. The update further emphasized and enhanced the Agencies’ risk-focused approach to BSA/AML supervision. The Agencies made revisions throughout the updated sections to ensure the language clearly distinguishes between mandatory regulatory requirements and supervisory expectations set forth in the guidance. The revised sections are available at: <https://www.ffiec.gov/press/pr041520.htm>
- May 11, 2018 – The new set of Examination procedures covering Beneficial Ownership was added to the examination guide, and the existing section on Customer Due Diligence (CDD) was updated to reflect the examination expectations implemented on the updated CDD implementation date. These procedures are available at: <https://www.ffiec.gov/press/pr051118.htm>

The FFIEC’s Bank Secrecy Act/Anti-Money Laundering InfoBase was developed to provide field examiners at the regulatory agencies with an electronic source for training and distributing needed examination information. Financial institutions have access to this InfoBase and will benefit from this training and examination information. The long-term goal of the InfoBase is to provide just-in-time training for new regulations and for other topics of specific concerns to examiners within the FFIEC’s member agencies – Federal Reserve Bank (FRB), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), Consumer

Financial Protection Bureau (CFPB), Conference of State Bank Supervisors (CSBS), American Council of State Savings Supervisors (ACSSS), and National Association of State Credit Union Supervisors (NCSCUS).

B. Sections – The examination manual is currently comprised of ten sections:

1. Introduction -- This section presents the: structure of the manual; background information on the evolution of the BSA; role of the various government agencies in the BSA; basic money laundering and terrorist financing (ML/TF); and a discussion on criminal and civil penalties for violations of the BSA.
2. Scoping and Planning -- This section discusses how the federal examiner will assess the adequacy of the institution's BSA/AML compliance program relative to its risk profile, and the institution's compliance the BSA regulatory requirements. The scoping and planning process enables the examiners to focus their reviews of the risk management practices and compliance with BSA requirements on areas of greatest ML/TF and other illicit financial activity risks. During the scoping and planning process, the agency will determine the examination staffing needs, including technical expertise, and determine the actual exam plan that will be used to determine whether the financial institution has developed, administered and maintained an effective program for compliance with the BSA, and all of its implementing regulations.
3. BSA/AML Risk Assessment – This section discusses how the examiners will review the institution's risk assessment process to determine if the institution adequately identified the money laundering / terrorist financing and other illicit financial activity risks within its banking operations. This section provides standards for examiners to assess the adequacy of the institution's risk assessment process.
4. Assessing the BSA/AML Compliance Program – This section identifies “how” the examiner will assess whether the institution has designed, implemented, and maintains an adequate BSA/AML compliance program that complies with BSA regulatory requirements – the four “tenets” / “pillars” – System of Internal Controls, Independent Testing, Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance, and Training – along with Customer Identification Program (CIP) and Customer Due Diligence (CDD).
5. Developing Conclusions and Finalizing the Exam – This section describes how the examiner will formulate conclusions about the adequacy of the institution's BSA/AML compliance program relative to its risk profile and the institution's compliance with BSA regulatory requirements. This section also discusses the development of an appropriate supervisory response and communicating the examination findings to the examined institution.

6. Assessing Compliance with BSA Regulatory Requirements - In addition to the five “tenets” / “pillars”, financial institutions must comply with other program reporting and recordkeeping requirements, special information sharing procedures, and special standards of diligence, prohibitions, and special measures set forth in 31 CFR Chapter X Parts 1010 and 1020. This section contains the exam procedures covering: CIP; CDD; Beneficial Ownership; Suspicious Activity Reporting (SAR); CTR; Transactions of Exempt Persons; Information Sharing; Monetary Instrument Sales; Funds Transfer Recordkeeping; Foreign Correspondent Account Recordkeeping and Reporting; Private Banking for Non-U.S. Persons; Special Measures; Foreign Bank and Financial Accounts Reporting (FBAR); and International Transportation of Currency or Monetary Instruments Reporting (CMIR).
7. Office of Foreign Asset Control (OFAC) – This section describes how the examiner will assess the risk-based OFAC compliance program to evaluate whether it is appropriate for the examined institution’s OFAC risk, taking into consideration its products, services, consumers, business entities, transactions, and geographic locations. The examiner will also review the institution’s documented Sanctions Compliance Program (SCP) – the framework for such was published and “encouraged” by OFAC in May 2019.
8. Program Structures – This section discusses how the examiner will assess the structure and management of the organization’s BSA/AML compliance program and if applicable, the organization’s consolidated or partially consolidated approach to BSA/AML compliance. If applicable, the examiner will assess the adequacy of the U.S. institution’s systems to manage the risk associated with foreign branch and offices, and management’s ability to implement effective monitoring and reporting systems. Also, if applicable, the examiner will assess the adequacy of the examined institution’s systems to manage the risks associated with parallel banking relationships – instances when at least one U.S. financial institution and one foreign financial institution are controlled either directly or indirectly by the same person or group of persons who are closely associated in their business dealings.
9. Risks Associated with Money Laundering and Terrorist Financing – This section contains the exam procedures covering: Correspondent Accounts (Domestic); Correspondent Accounts (Foreign); Bulk Shipments of Currency; U.S. Dollar Drafts; Payable Through Accounts; Pouch Activities; Electronic Banking (including Remote Deposit Capture); Funds Transfers; ACH; Prepaid Access; Third-Party Payment Processors (TPPP); Monetary Instrument purchases and sales; Brokered Deposits; Privately Owned ATMs; Non-deposit investment products; Insurance; Concentration Accounts; Lending Activities; Trade Finance Activities; Private Banking; Trust and Asset Management Services; Non-resident Aliens and Foreign Individuals; Politically

Exposed Persons (PEPs); Embassy, Foreign Consulate and Foreign Mission Accounts; Non-Bank Financial Institutions (NBFIs); Professional Service Providers (PSPs); Non-Governmental Organizations (NGOs) and Charities; Business Entities (Domestic and Foreign); and Cash Intensive Businesses.

10. Appendices – The examination manual contains 21 appendices which include: Appendix -1 Beneficial Ownership; A – BSA Laws and Regulations; B – BSA/AML Directives; C – BSA References; D – Statutory Definition of Financial Institution; E – International Organizations; F- Money Laundering and Terrorist Red-Flags; G – Structuring; H – Request Letter Items; I – Risk Assessment Link to the BSA/AML Compliance Program; J – Quantity of Risk Matrix; K – Customer Risk versus Due Diligence and SAR Monitoring; L – SAR Quality Guidance; M – Quantity of Risk Matrix – OFAC; N – Private Banking – Common Structure; O – Examiner Tools for Transaction Testing; P – BSA Record Retention Requirements; Q – Abbreviations; R – Enforcement Guidance; S – Key Suspicious Activity Monitoring Components; and T – BSA E-Filing System.

At the FFIEC's BSA/AML Infobase, the sections, sub-sections, and corresponding exam procedures can either be viewed on-line, and/or downloaded in a .pdf format.

II. COMPLIANCE PROGRAM STRUCTURES

- A. Compliance Program Structures** – Each financial institution must have a comprehensive BSA/AML compliance program that addresses BSA requirements applicable to all operations of the organization. Institutions have much discretion as to how their BSA/AML compliance program is structured and managed: organizing the compliance program or some parts of the program within a specific legal entity; or with some degree of consolidation across entities within an organization; or as part of a comprehensive enterprise-wide risk management framework.

Small financial institutions may choose to combine BSA/AML compliance with other functions and utilize the same personnel in several roles. (In such circumstances, there should still be adequate senior-level attention to BSA/AML compliance, and sufficient dedicated resources). Large, complex, banking organizations will at times aggregate risk of all types on a firm-wide basis in order to maximize efficiencies, and better identify, monitor, and control all types of risks within or across affiliates, subsidiaries, lines of business or jurisdictions. (In such organizations, management of BSA risk is generally the responsibility of a corporate compliance function that supports and oversees the BSA/AML compliance program). Other banking organizations may adopt a structure that is less centralized but still consolidates some or all aspects of BSA/AML compliance. Regardless of how a consolidated BSA/AML compliance program is organized, it should reflect the organization's business structure, size, complexity, and be designed to effectively address risks, exposures, and applicable legal requirements across the organization. (A consolidated approach should also include the establishment of corporate standards for BSA/AML compliance that

reflect the expectations of the organization's board of directors, with senior management working to ensure that the BSA/AML program implements these corporate standards).

Regardless of "how" the organization structures and manages its program, and appropriate level of BSA/AML compliance independence should be maintained by:

1. Providing BSA/AML compliance staff a reporting line to the corporate compliance or other independent function;
2. Ensuring that BSA/AML compliance staff is actively involved in all matters affecting AML risk (e.g., new products, review or termination of customer relationships, filing determinations, et al);
3. Establishing a process for escalating and objectively resolving disputes between BSA/AML compliance staff and business line management; and
4. Establishing internal controls to ensure that compliance objectivity is maintained when BSA/AML compliance staff is assigned additional bank responsibilities.

B. Management and Oversight of the BSA/AML Compliance Program –

The board of directors and senior management have different responsibilities and roles in overseeing, and managing BSA/AML compliance risk. The board is responsible for:

1. Approving the BSA/AML compliance program and for overseeing the structure and management of the institution's BSA/AML compliance function;
2. Setting an appropriate "culture of compliance" (See FinCEN Advisory 2014-A007 on Promoting a Culture of Compliance), establishing clear policies regarding the management of key BSA/AML risks, and ensuring that these policies are adhered to in practice; and
3. The Board should ensure that:
 - a.) Senior management is fully capable, qualified, and properly motivated to manage the BSA/AML compliance risks arising from the institution's business activities in a manner that is consistent with the Board's expectations;
 - b.) BSA/AML compliance function has an appropriately prominent status with the organization;
 - c.) Its views about the importance of BSA/AML compliance are understood and communicated across all levels of the organization; and
 - d.) Senior Management has established appropriate incentives to integrate BSA/AML compliance objectives

into management goals and compensation structures across the organization, and that corrective actions, including disciplinary measures, if appropriate, are taken when serious BSA/AML compliance failures are identified.

Senior Management is responsible for:

1. Communicating and reinforcing the BSA/AML compliance culture established by the board, and implementing and enforcing the board-approved BSA/AML compliance program; and
2. Supporting and overseeing the organization's BSA/AML compliance program. (BSA/AML compliance staff should report to the board or a committee thereof on the effectiveness of the compliance program and significant BSA/AML compliance matters).

Regardless of the organization structure utilized, the federal examiner will form a conclusion about the adequacy of the BSA/AML compliance program structures and management, including if applicable the effectiveness of the consolidated or partially consolidated approach to compliance.

III. AUTOMATED CLEARINGHOUSE (ACH)

- A. Automated Clearinghouse (ACH)** – The ACH system was originally designed to transfer a high-volume of low dollar transactions, thereby not posing significant BSA/AML risks. The use of ACH is growing though, due to increased volume of electronic check conversions and one-time ACH debits, reflecting the lower cost of ACH processing relative to check processing. The FRB's FedACH system is almost exclusively used for domestic ACH payments, but does accommodate cross-border ACH payments to and from Canada, and to Mexico, and to a variety of Western European and South American nations.

The ability to send high-dollar and higher volume transactions through the ACH may expose financial institutions to BSA/AML risks as ACH transactions can be used in both the layering and integration stages of money laundering. Detecting unusual activity in the layering and integration stages can be a difficult task because ACH may be used to legitimize frequent and recurring transactions.

- B.** Areas of focus and concern within the ACH environment include, but are not limited to:
1. Client Due Diligence (CDD) - Given the reliance that ODFIs and RDFIs place on each other for OFAC reviews and other necessary due diligence information, it is essential that all parties have a strong CDD program for "regular" ACH clients. DFIs may wish to restrict or refuse ACH services to potential originators and receivers that engage in questionable or deceptive business practices.
 2. Third Party Service Provider (TPSP) - For DFIs that rely heavily on a TPSP, contracts between such should clearly identify roles, and

responsibilities, and the DFI will want to understand the suspicious activity monitoring ability provided by the third-party, if any.

3. Third-Party Senders (TPS) – ensure due diligence is performed on the companies “originated for”, or at the very least, on the principals of the TPS.
4. ACH ODFI “Direct Access” – Direct Access Debit Participant is extremely risky.
5. IAT – monitor clients and transaction types and volumes, CIP – CDD – EDD standards and practices, SAR monitoring and reporting, appropriate systems and controls, processing procedures, training programs, and legal agreements.
6. “On-Line” account opening without face-to-face contact, and then allowing the client to originate ACH entries over the web.
7. “Other” ACH entries such as those originated through the Internet (WEB) or over the telephone (TEL) may be susceptible to manipulation and fraudulent use.

C. The federal examiner when performing the ACH section of the BSA/AML exam will:

1. Review the policies, procedures, and processes related to ACH given the DFI’s transactions, including IATs, and assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing;
2. Determine whether the institution has effectively identified and is monitoring high-risk clients using ACH transactions, including IATs;
3. Evaluate the DFI’s risks related to ACH transactions, including IATs, by analyzing frequency and dollar volume and types in relation to the DFI’s size, location, and nature of client relationships, and the location of the origin or destination of IATs relative to the DFI’s location.
4. Determine whether the internal control systems for monitoring clients using ACH for suspicious activities includes:
 - a. Identifying clients with frequent and large ACH transactions;
 - b. Monitoring ACH detail activity when the batch-processed transactions are separated for other purposes (E.g. processing errors);
 - c. As appropriate, identifying and applying increased due-diligence to higher risk clients who originate or receive IATs, particularly when a party to the transaction is located in a higher-risk geographic location; and

- d. Using methods to track, review, and investigate customer complaints regarding fraudulent or duplicate ACH transactions.
- 5. Evaluate the financial institution's adherence to the NACHA and Clearinghouse Rules and operating regulations:
 - a. Review results from the DFI's Rules compliance audit and determine the independence and competence of the party performing the audit;
 - b. Examine the ACH risk assessment and determine the adequacy of the program established to minimize and mitigate the identified risks; and
 - c. Assess the adequacy of separation of duties throughout the ACH process.
- D. Annual training of the ACH team members for BSA/AML must include a review of the SAR process, covering SAR (the concept) itself, who coordinates SAR activities within the institution, "how" to refer potentially suspicious transactions to the central coordinator, and the various types of ACH transactions that could be suspicious and should be "watched for".

IV. INITIAL OBSERVATIONS/LESSONS LEARNED

- A. **Initial Observations/Attendee Feedback/Lessons Learned** – Based on multiple years' experience with examination materials, below are initial observations and lessons learned to this point.
 - 1. Risk Assessment is one of two major factors in not only experiencing a successful exam, but in developing and maintaining a successful BSA compliance program. The examiner will evaluate an institution's BSA compliance program based on the institution's risk profile for money laundering, terrorist financing, and other illicit activities. As new products and services come "on-line" and when new categories of clients are "on-boarded", the institution's risk assessment must be updated to reflect such – definite "red-flag" if such are not included in the institution's risk assessment. Products, services, consumers, business entities, and geographic markets must be analyzed and "risk assessed". It is critically important that effective controls be in place to identify and manage the residual risk which management has accepted. Examiners continue to look for more granularity, more detail, more data, and trend-line analysis considering the direction of risk over time when evaluating the institution's risk assessment.
 - 2. Knowledgeable and experienced BSA officer is the other major factor in experiencing a successful exam and in developing and maintaining a successful BSA compliance program. The examiner will meet with the BSA Officer and inquire and ask questions –

can the BSA Officer answer the questions, or do they have to go to someone else to find the answer? Is the BSA Officer's opinions sought and considered when making: SAR File/No-File decisions; when deciding to enter into new product lines and/or markets and/or new lines of business; and when making system decisions impacting BSA compliance. Is the BSA Officer actively involved in new product development? What kind of outside training has the BSA Officer received? Are detailed policies and procedures kept up to date so that when needed, the back-up BSA Officer can step in and successfully continue. (Basic question – what qualifies this person to be the BSA Officer)?

3. Transaction testing with minimal to no exceptions, is a third “key” factor to the success of the exam. The federal examiners will complete transaction testing during every exam, and will expect the independent audit to include reasonable levels of transactional testing and identify any deficiencies. Transactional testing should focus on these areas:
 - a. CIP, CDD, and EDD;
 - b. Currency transaction and suspicious activity reporting;
 - c. Funds transfer monitoring (Wires and ACH);
 - d. Adequacy of deposit account information and trust and asset account information – for selected new accounts, testing the adequacy of the institution's CIP process;
 - e. Testing currency-shipment logs – reviewing selected currency logs to identify significant aberrations or unusual patterns of currency-shipment activity;
 - f. Nonresident aliens and foreign individuals – reviewing account information to identify accounts that have no TINs or ITINs; and
 - g. Funds Flow Report – identifying “high-velocity” clients with large funds flows and unusual activity.

Appendix O in the examination manual provides additional details on the transactional testing efforts. Financial institutions should realize that in most instances, the federal examiner will be “expecting” the report to be provided in a spreadsheet or data base format to accommodate electronic manipulation and review of the data.

4. Expanded “inclusions” within the required “system of internal controls” – the new exam explicitly details many new points within the most important of the four tenets of a successful BSA program;

5. Board, Management, BSA Officer and Individual employee accountability is emphasized;
6. Board and Senior Management commitment to the BSA program are assessed. BSA Officer competency is judged, and the adequacy of staffing levels and resources in the BSA compliance area(s) are evaluated (Critically important to have adequate staff to clear alerts);
7. Lack of risk identification of all, especially high-risk clients, both existing clients and new clients. Failures to document the assessment process, to provide for interim updates to client risk/rating profile, and a lack of formalized risk assessment process;
8. Independent audit rated deficient due to the scope not being risk focused, audit not being performed every 12 months, and/or the scope was too narrow, transaction testing not conducted, MIS reports not validated for accuracy, inadequate or outdated work programs, insufficiently experienced/trained staff performing the audit, audit work papers not available, and/or “quality” of work papers – explicit and complete, and no overall rating or conclusion. Make sure “follow-up” on audit recommendations to track progress on deficiencies. Important to document board’s response to audit report. (If using outside audit firm, consider changing periodically.)
9. Job specific BSA training – New hires, internal transfers, Lenders, CSRs, Trust, et.al Focus on the qualifications of the trainer. Consider testing and documentation of follow-ups. Consider effectiveness of training program. Rationale for current budget changes. Consider multi-day training for BSA Officer. Documentation of training activities (e.g., rosters, materials, et.al.). Beginning to review testing “process.” Starting to look at training “retention.”
10. AML/Risk Management Systems – “Have you thought about?” For those DFIs with a system, understanding the system itself and “How” the system is being used. (Ensure audit verifies “rules process” through testing and “model-validation.” Need to ensure that policies and procedures are in sync with system operations. Need to ensure that systems are evaluated for accuracy during independent audit, and be sure to get copies of workpapers).
11. Board of Directors “involvement” in BSA process – Updates (quality and frequency), status, commitment of necessary resources, and training.
12. ACH Reviews.
13. National Security Letter (NSL) Procedures.
14. Documentation. Documentation. Documentation.

15. Document your “SAR process” – flowchart, decision points, forms and formats, responsibilities, accountabilities, and “narrative reviewers”. SAR “log” suggestion – dates, filings, next “deadlines.” “SAR Committee” utilization.
16. Do not get lazy. Agencies still finding problems with CTRs records and “weakness in investigating suspicious activity”.
17. Focus on funds transfers, especially those related to TPPPs and other cross-border activities. International transfers - looking for connections between the Transmitter and the Recipient, and for the “purpose” of the transfer. Some institutions have applied such questions domestically too. (OFAC scan on wires should search ALL fields including remarks sections). Watch “stripping.”
18. The examiners will continue to test the staff, test the staff, test the staff – Evaluate staff based on deficiencies noted and knowledge demonstrated.
19. Back-Up and succession planning is important for all critical positions, and BSA Officer is a critical position. The Back-Up or Assistant BSA Officer should be anointed and appointed by the Board and should be able to step in and take over in the morning, should the need arise. The examiner will look for proof that the Back-Up BSA Officer can “hit the ground” running, and they may test that ability by having the back-up BSA Officer answer the examination questions. (Resumes and training records on all the personnel in the BSA compliance group should be maintained and updated when necessary).
20. MSB focus, with some agencies expecting formal policy.
21. Remote Deposit Capture Activities – Exam Procedures last updated November 2014.
22. International Trade Finance – Trade-Based Money Laundering (TBML) and Funnel Accounts – FinCEN Advisories 2010-A001 and 2014-A005.
23. CDD/Beneficial Owner – Identifying and Verifying the identity of beneficial owners of legal entity customers – FinCEN Final Rule 05/11/16 – Applicability Date 05/11/18. (Exam Procedures released 05/11/18).
24. Remotely Created Checks (RCCs)/Remotely Created Payment Orders (RCPOs)/ACH Debits.
25. Third-party Payment Processor (TPPP), mobile payments, and P2P. (Make sure TPPP has completed ACH self-audit where applicable.)
26. CTR Exemptions – Be “careful” when exempting “high-risk” clients – make sure reasonable. Ensure that client remains in “good-standing” at the State level (company could be dissolved for failing annual filing requirements, and as such, no longer

qualified for exemption status). For Phase 2 exemptions, critically important to document ongoing qualifications – 50% Test).

27. Management of outsourced Vendor Arrangements – Understand relationship and understand who is responsible for BSA/AML and OFAC compliance. Evaluate the financial institution's program to oversee/manage the outsourced relationship. (OCC 2013-29)
28. OFAC Process – “Sensitivity Settings” - Account opening timing. Cashing checks for “non-clients.”
29. Employees and Insiders – “How” detecting and reporting suspicious activity.
30. Private ATMs – Increased monitoring of ALL machine types (cash, CVC, “gaming”) expected. Contractual review and analysis of sources of funds and flows at a minimum.
31. Identify and manage marijuana-related businesses. FinCEN Guidance 2014-G001.
32. Cross-Channel Collaboration – Internal groups sharing suspicious activity – all groups selling services to same clients – “High-Level.”
33. Regulation GG – At times has been tested within BSA Exam.
34. Renewed Focus on Trust – With exclusion of most trusts from beneficial ownership requirements, examiners will look more closely at due diligence activities.
35. Terrorist Financing – International Transactions – do they make sense for that client – where are they going to and from, and does that pattern make sense. Jurisdiction where funds are going to – on the FATF list – normal for that client?
36. Default loan on documentation loans secured by cash and cash equivalent.
37. What position has the Board taken regarding banking marijuana-related enterprises and hemp-related enterprises, both now and in future.
38. Although interagency, qualitative and subjective.

RISK ASSESSMENT

- I. RISK ASSESSMENT** - Risk assessment is a major key to success in BSA/AML compliance, and in the updated BSA/AML examination. Management has the responsibility to evaluate products, services, clients, entities, and geographic markets to identify circumstances that expose the institution to greater risk for use in money laundering, terrorist financing, or other fraud schemes. A well-developed risk assessment will assist in identifying the institution's BSA/AML risk profile. Understanding the risk profile enables the institution to apply appropriate risk management processes to the BSA/AML compliance program to mitigate risk. The risk assessment provides a comprehensive analysis of the BSA/AML risks in a concise and organized presentation and it should be shared and communicated with, all business lines across the institutions, board of directors, management and appropriate staff. It is a sound practice that the risk assessment be reduced to writing. Although there are many effective methods and formats that can be used in completing a BSA/AML risk assessment, the format chosen should be easily understood by all appropriate parties.

A. Types of Risk Assessments – Under the updated examination format, financial institutions should prepare three risk assessments including:

1. “Institution-Wide” BSA/AML – Looking at products, services, clients, entities, and geographies.
2. Client – Looking at customers/members to identify baselines of normalcy, and most importantly, identifying high-risk clients. CIP assessments included here;
3. OFAC – A fundamental element of a sound OFAC program is the institution's assessment of its specific product lines, client base, and nature of transactions and identification of the high-risk areas for OFAC transactions. An effective OFAC risk assessment should be a composite of multiple factors, as OFAC sanctions can reach into virtually all areas of its operations. Institutions should consider all types of transactions, products, and services when conducting the OFAC risk assessment and while establishing the appropriate policies, procedures, and processes. Ensure OFAC risk assessment is updated as new products and services are added.

NOTE: If the federal examiner finds that the institution has not completed a risk assessment or the risk assessment is inadequate. The examiner must complete a risk assessment based on available information.

B. Users of Risk Assessments – Three “populations” will use the output from the risk assessments, management, independent auditors, and federal examiners.

1. Management - Management should use the risk assessments to better identify and mitigate gaps in the institution's controls, to identify areas of weakness or areas where there is a need for enhancements or stronger controls, and to assist in new product approval by assessing cost versus risk versus profit potential.
2. Independent auditor – Independent auditors will use the risk assessments to evaluate the quality and reasonableness of management's risk assessment efforts given the institution's risk

profile, and evaluate the quality of the control structure implemented to minimize and mitigate such risks.

3. Federal examiner – Federal examiners will use the risk assessments as part of the scoping and planning of the specific institution’s BSA/AML exam. (The examiners will “build” the scope and plan of the exam using off-site monitoring information, previous examination reports and work papers, the results of the independent audit/test (assuming that it is effective), the institution’s risk assessments, output from the BSA E-Filing database (FinCEN Query), and the request letter items completed by management (Appendix H)). If the financial institution has not completed its own risk assessments, the federal examiner will do it for them).

C. Risk Assessment Development – The development of the BSA/AML risk assessment generally involves two steps; first, identify the specific risk categories (E.g. products, services, clients, entities, and geographic locations) unique to the financial institution – “Quantity of Risk”; second, conduct a more detailed analysis of the data identified in step 1 to better assess the risks within each of these categories – “Quality of Risk Controls” in place. (Quantity of Risk minus the Quality of Risk Controls in place leaves “**Residual Risk**”). In reviewing the risk assessment, the examiner will determine whether management has considered all products, services, clients, entities, and geographic locations within the assessment, and whether management’s detailed analysis within these specific risk categories was adequate.

1. The first step of the risk assessment process is to **identify** the specific products, services, clients, entities, and geographic locations unique to the financial institution. Although attempts to launder money, finance terrorism, or conduct other illegal activities through a financial institution can emanate from many different sources, certain sources may be more vulnerable to or have been historically abused by money launderers and criminals. Also, depending on the specific characteristics of the particular product, service, or client, the risks are not always the same and various factors (E.g. number and volume, nature of the client relationship, et al) should be considered as the risk assessment is prepared. The differences in a way the financial institution interacts with its clients (face-to-face versus electronic banking) should also be considered.
2. Certain products and services may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity or involve the handling of high volumes of currency or currency equivalents. Exhibit 8-A offers a listing of the current products and services receiving federal “focus”.
3. Identifying geographic locations that may pose a higher risk is essential to the financial institution’s BSA/AML compliance program. Domestic institutions should understand and evaluate the specific risks associated with doing business in, opening accounts for clients from, or facilitating transactions involving certain geographic locations. Exhibit 8-A offers a listing of the current geographic locations receiving federal “focus”.
4. Although any type of account is potentially vulnerable to money

laundering or terrorist financing by the nature of their business, occupation, or anticipated transaction activity, certain clients and entities may pose specific risks. It is essential that financial institutions exercise judgment and neither define nor treat all members of a specific category of client as posing the same level of risk. Other variables, such as services sought and geographic locations should be considered as well. Chapter 9 provides additional guidance on the current client listings receiving federal “focus”.

5. The second step of the risk assessment process entails a more **detailed analysis** of the data obtained during the first step (the identification stage) in order to more accurately assess the BSA/AML risk of each specific institution. This second step involves evaluating data pertaining to the institution’s activities (E.g. number of domestic and international funds transfers, private banking clients, foreign correspondent accounts, and domestic and international geographic locations of the institution’s business areas) in relation to the CIP and CDD information. The detailed analysis is important because within any type of product or category of client, there will be accountholders and/or products that pose varying level of risk.
6. The level and sophistication of the analysis will vary from financial institution to financial institution, and is critically important as the detailed analysis gives management a better understanding of the institution’s risk profile to ensure the development of appropriate policies, procedures, and processes to minimize and mitigate the risk. The examination guidelines suggest that the detailed analysis could include reviewing:
 - a. Purpose of the account;
 - b. Actual or anticipated activity in the account;
 - c. Nature of the client’s business;
 - d. Client’s location;
 - e. Types of products and services used by the client.
7. Once the detailed analysis is completed, management can utilize the results to structure the institution’s BSA/AML program to adequately address the risk “profile” built through the process. The independent BSA test should review the institution’s risk assessment process for reasonableness. Additionally, management should consider the staffing resources and level of training necessary to promote adherence with the policies, procedures, and processes. Holding companies or lead financial institutions that implement an enterprise-wide BSA/AML compliance program should assess risk both individually within business lines, and on a consolidated basis across all activities and legal entities.
8. An effective risk-assessment should be an ongoing process. Management should update the risk assessment to identify changes in the institution’s risk profile as necessary, such as when new products and services are introduced, or when the institution is involved in a merger or acquisition. (In the absence of such changes, and depending

on the position of the specific federal examiner, it is a sound practice for the institution to periodically reassess their BSA/AML risks at least every 12 months).

D. Risk Assessment Process – In the absence of any specific federal selected output formats displaying the results of the risk assessment efforts, financial institutions have much latitude in approaching the risk assessment process. A commonly used risk assessment process uses a three-tiered approach to assessing risk:

1. Identify reasonably foreseeable internal and external threats that lead to the financial institution being used intentionally or unintentionally by criminal elements;
2. Determine the likelihood and potential damage from each of these threats; and
3. Identify and consider the sufficiency of existing policies, procedures, systems, and other arrangements intended to control the identified risks.

Once the risks are assessed, the appropriate monitoring program/process is designed and implemented, the staff is trained, and independent testing of the process is included in the annual BSA review.

Risk assessment is nothing new. Many internal financial institution programs begin with a risk assessment process including Information Security, Business Continuity, FDICIA analyses, loan pricing models, et al. In addition to the Federal suggestions presented in Exhibit 8-A, financial institutions should add their own loss and/or exposure experiences as well as information from their own specific SAR filings.

E. Conference of State Bank Supervisors – In January 2017 the Conference of State Bank Supervisors published a voluntary tool that could assist banks with the risk assessment process. The tool is available at: www.csbs.org.

F. Examiner Determination of Institution's BSA/AML Aggregate Risk Profile – The federal examiner will assess whether the controls of the BSA/AML compliance program are appropriate to manage and mitigate the institution's BSA/AML risks. Through the process, the examiner will determine an aggregate risk profile for the institution taking into consideration the risk assessment developed by the institution, and determining whether the compliance program is "adequate" to appropriately mitigate the BSA/AML risk faced by such. (In those situations where the institution has not completed a risk assessment, the federal examiner will complete one on their own in order to develop this aggregate risk profile).

Federally Defined Categories High-Risk Products and Services

In identifying those products which present a “heightened risk” from the BSA/AML perspective, financial institutions could begin with the Federally defined categories of high-risk products found in the *SAR Activity Reviews*, the *FFIEC BSA/AML Examination Manual*, and the Treasury Department’s National Money Laundering Strategy documents. “High-risk” products can include:

1. Certain Trust (Asset Management) or Private Banking Accounts (Domestic and International). FinCEN Guidance 2010-G001 reminds DFIs to:
 - ✓ Determine whether the client is acting as an agent for or on behalf of another, and if so, obtain information regarding the capacity on whose behalf the client is acting;
 - ✓ Obtain information about the structure or ownership of an entity that is not publicly traded in the United States (E.g. unincorporated association, trust or foundation, private investment company, et al);
 - ✓ Obtain information about the trust structure where the client is the trustee.
2. Foreign Correspondent Banking Account Activities:
 - “Nested Accounts” – a foreign financial institution gains access to the U.S. banking system by operating through a U.S. correspondent account belonging to another foreign financial institution;
 - U.S. Dollar Drafts – bank draft or check denominated in U.S. Dollars, drawn on a U.S. Bank, and made available at a foreign financial institution;
 - PTAs – Payable Through Accounts – “pass through” accounts used by foreign institutions to provide their clients with access to the U.S. payments system;
 - Pouch activities – transporting currency, monetary instruments, or other documents from outside the U.S. to a bank in the United States.
3. Foreign Branches and Offices of U.S. Banks;
4. Parallel Banking – At least one U.S. Bank and one foreign financial institution are controlled either directly or indirectly by the same person or group of persons who are closely associated in their business dealings or otherwise acting together, but not subject to consolidated supervision by a single home country supervisor.
5. Special use (e.g., IOLTA) or concentration accounts (e.g., Internal use of general ledger to clear client transactions);
6. Brokered Deposits;
7. Electronic Funds Payment Services – Electronic cash (prepaid and payroll cards), funds transfers (domestic and international), PUPID transactions, third-party payment processors, remittance activity, ACH, and ATM.
8. Electronic Banking – Mobile Banking, WEB Banking, P2P;

Federally Defined Categories High-Risk Products and Services, Continued

9. Bulk Currency Shipments

- Bulk shipments of currency entail the use of common, independent, or Postal Service air/land/sea carriers to transport large volumes of bank notes from sources either inside or outside the U.S. to a DFI in the United States. Bulk shipments of currency to DFIs from shippers that are presumed to be reputable may nevertheless originate from illicit activity.
- DFIs that offer services to receive bulk shipments of currency should have policies, procedures, and processes in place that mitigate and manage the BSA/AML risks associated with the receipt of bulk currency shipments. DFIs should also closely monitor bulk currency shipment transactions to detect and report suspicious activity, with particular emphasis on source of funds, and “reasonableness” of transaction volumes from “Currency Originators” and “Intermediaries”.
- FinCEN Form 105 (CMIR) form implications exist under 31 CFR 1023.220(a)-(c) in certain circumstances. Form 104 (CTR) filings could apply to non-exempt “persons”, and SAR processing must be applied to bulk currency shipments where appropriate.
- “Red Flags” for Bulk Shipments of Currency include:
 - An increase in the sale of large denomination U.S. bank notes to foreign DFIs by US DFIs;
 - Large volumes of small denomination U.S. bank notes being sent from foreign non-bank institutions to their own accounts in the U.S. via armored transport, or sold directly to U.S. banks;
 - Multiple wire transfers initiated by foreign NBFIs that direct U.S. DFIs to remit funds to other jurisdictions that bear no apparent business relationship with that NBFI;
 - The exchange of small denomination U.S. bank notes for large denomination U.S. bank notes that may be sent to foreign countries;
 - Deposits by foreign NBFIs to their accounts at U.S. banks that include third-party items, including sequentially numbered monetary instruments; and
 - Deposits of currency and third-party items by foreign NBFIs to their accounts at foreign financial institutions, and thereafter direct wire transfers to the foreign nonbank DFI’s accounts at U.S. DFIs

10. Non-Deposit Investment Products;

11. Insurance Products; - E.g. borrowing against cash surrender value;

Federally Defined Categories High-Risk Products and Services, Continued

12. International Trade Finance (Letters of Credit) – See FinCEN Advisory 2010-A001 for information on “How” to identify and report suspected instances of trade-based money laundering and See FinCEN Advisory 2014-A005 for information on “funnel accounts” and TBML. (A funnel account is defined as an individual or business account in one geographic area, that receives multiple deposits, often in amounts below the CTR reporting threshold, and from which funds are withdrawn in a different geographic area, with little time elapsing between deposits and withdrawals).
13. Certain Lending Activities:
- CD secured loan – CD purchased with illicit funds;
 - Loans secured by marketable securities;
 - Loans made for ambiguous or illegitimate purpose, or that provide the bank with significant fees for assuming little or no risk, or tend to obscure the movement of funds.
 - Loans made for and/or paid by third-parties;
 - Bank or the customer attempts to sever the paper trail between the borrower and the illicit funds;
 - Loans extended to persons located outside the U.S., particularly to those in high-risk jurisdictions and geographic locations.

See FinCEN Advisory 2010-A001 with information on “how” to identify and report suspected instances of “Trade-Based Money Laundering”;

14. Monetary Instrument Sales

Ensure SAR process identifies:

- Sales of sequentially numbered monetary instruments from the same or different purchasers on the same day to the same payee;
- Sales of monetary instruments to the same purchaser or sales of monetary instruments to different purchasers made payable to the same remitter;
- Monetary instruments purchases by non-clients;
- Common purchasers, payees, addresses, sequentially numbered purchases, and unusual symbols;
- Outstandings/Aging;
- Buyer/Purchaser is the payee;
- Rounded Amounts/Structured Amounts;
- Early redemption of CD with no reasonable explanation.
- Common payees among multiple purchasers.

Federally Defined Categories High-Risk Products and Services, Continued

15. Remote Deposit Capture (RDC):

RDC may expose financial institutions to various risks including money laundering, fraud, and compromised transmission of financial data. Inadequate controls could result in the transmission of fraudulent monetary instruments, exposing the institution to both financial and reputational risks. As the RDC equipment is located outside the financial institution's facilities, data and hardware security issues may also increase. Management should develop programs to mitigate the risks presented through RDC including:

- Comprehensively identifying and assessing RDC risk prior to implementation. Senior management should identify BSA/AML, operational, information security, compliance, legal, and reputation risks. Depending on the bank's size and complexity, this comprehensive risk assessment process should include staff from BSA/AML, information technology and security, deposit operations, treasury or cash management sales, business continuity, audit, compliance, accounting and legal.
- Conducting appropriate customer CDD and EDD.
- Creating risk-based parameters that can be used to conduct RDC customer suitability reviews. Parameters may include a list of acceptable industries, standardized underwriting criteria (e.g., credit history, financial statements, and ownership structure of business), and other risk factors (customer's risk management processes, geographic location, and customer base). When the level of risk warrants, bank staff should consider visiting the customer's physical location as part of the suitability review. During these visits, the customer's operational controls and risk management processes should be evaluated.
- Conducting vendor due diligence when banks use a service provider for RDC activities. Management should ensure implementation of sound vendor management processes.
- Obtaining expected account activity from the RDC customer, such as the anticipated RDC transaction volume, dollar volume, and type (e.g., payroll checks, third-party checks, or traveler's checks), comparing it to actual activity, and resolving significant deviations. Comparing expected activity to business type to ensure they are reasonable and consistent.
- Establishing or modifying customer RDC transaction limits.
- Developing well-constructed contracts that clearly identify each party's role, responsibilities, and liabilities, and that detail record retention procedures for RDC data. These procedures should include physical and logical security expectations for access, transmission, storage, and ultimate disposal of original documents. The contract should also address the customer's responsibility for

Federally Defined Categories High-Risk Products and Services, Continued

properly securing RDC equipment and preventing inappropriate use, including establishing effective equipment security controls (e.g., passwords, dual control access). In addition, contracts should detail the RDC customer's obligation to provide original documents to the bank in order to facilitate investigations related to unusual transactions or poor quality transmissions, or to resolve disputes. Contracts should clearly detail the authority of the bank to mandate specific internal controls, conduct audits, or terminate the RDC relationship.

- Implementing additional monitoring or review when significant changes occur in the type or volume of transactions, or when significant changes occur in the underwriting criteria, customer base, customer risk management processes, or geographic location that the bank relied on when establishing RDC services.
- Ensuring that RDC customers receive adequate training. The training should include documentation that addresses issues such as routine operations and procedures, duplicate presentment, and problem resolution.
- Using improved aggregation and monitoring capabilities as facilitated by the digitized data.
- As appropriate, using technology to minimize errors (e.g., the use of franking to stamp or identify a deposit as being processed).

On 01/14/09, the FFIEC released guidance covering the Risk Management of Remote Deposit Capture, which addresses the necessary elements of an RDC risk management process in an electronic environment, with a focus on RDC deployed at the client location. RDC should be viewed as a new delivery system and not simply as a new service. Prior to implementing RDC, senior management should identify and assess the legal, compliance, reputation, and operational risks associated with the new system, in order to ensure that RDC is compatible with the DFI's business strategies and understand the ROI and understand management's ability to manage the risks inherent in RDC.

- Legal and Compliance Risks – The DFI should evaluate potential risks and regulatory requirements under BSA when designing and implementing RDC. (The growing use of RDC by foreign correspondent DFIs and foreign MSBs to replace pouch and certain instrument processing and clearing activities raises money laundering risks the DFI must understand and mitigate). Additional due diligence may be necessary when there is evidence that the RDC capture device is in a foreign location, or when the client has been identified as being High-Risk.
- Operational Risks – A DFI should consider carefully the authentication method(s) appropriate for RDC clients, as the FFIEC agencies consider single-factor authentication to be inadequate for high-risk transactions involving access to client information or the movement of funds to other parties.

Federally Defined Categories High-Risk Products and Services, Continued

- Client Due Diligence and Suitability – Management should establish appropriate risk-based guidelines to qualify clients for the RDC service.
- Vendor Due Diligence and Suitability – DFIs that rely on service providers for RDC activities should ensure implementation of sound vendor management processes as described in the Outsourcing Technology Services Handbook from the FFIEC.
- RDC Training for Clients – Management should ensure that clients receive sufficient training, including training on routine operations and procedures and the risks of duplicate presentment and other problem resolutions.
- Contracts and Agreements – The FFIEC guidance offers twelve inclusion suggestions for the contract. (E.g. “Types” of items that can be transmitted, periodic audits, et al).
- Business Continuity – Senior management should ensure the DFI’s ability to recover and resume RDC operations to meet client service requirements when an unexpected disruption occurs.
- Other Mitigation and Control Considerations – Controls to ensure the security and integrity of the non-public personal information throughout the transmission flow and while in storage. Separation of duties or other compensating controls. Strong change-control processes. Possible insurance where “cost-practical”.
- Risk Management: Measuring and Monitoring – DFIs offering RDC services should develop and implement risk measuring and monitoring systems for effective oversight of RDC activities.

The guidance is available at: www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf.

On April 29, 2016, the FFIEC released the updated Retail Payment Systems booklet which contains the examination procedures on Remote Deposit Capture. (www.ffiec.gov)

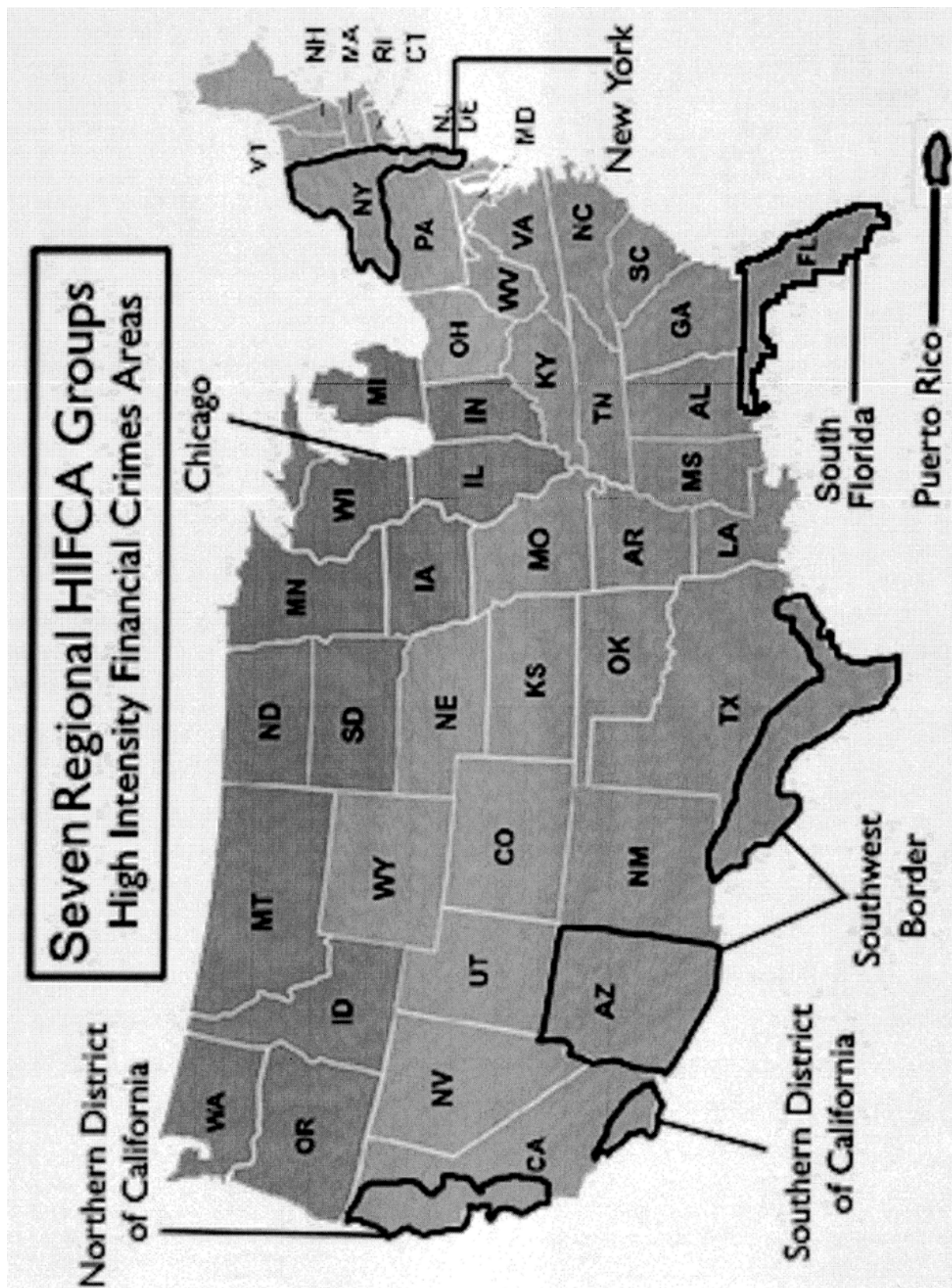
NOTE: Institutions offering RDC services should review deposited images for suspicious transactions and file SARs when appropriate.

Federally Defined Categories

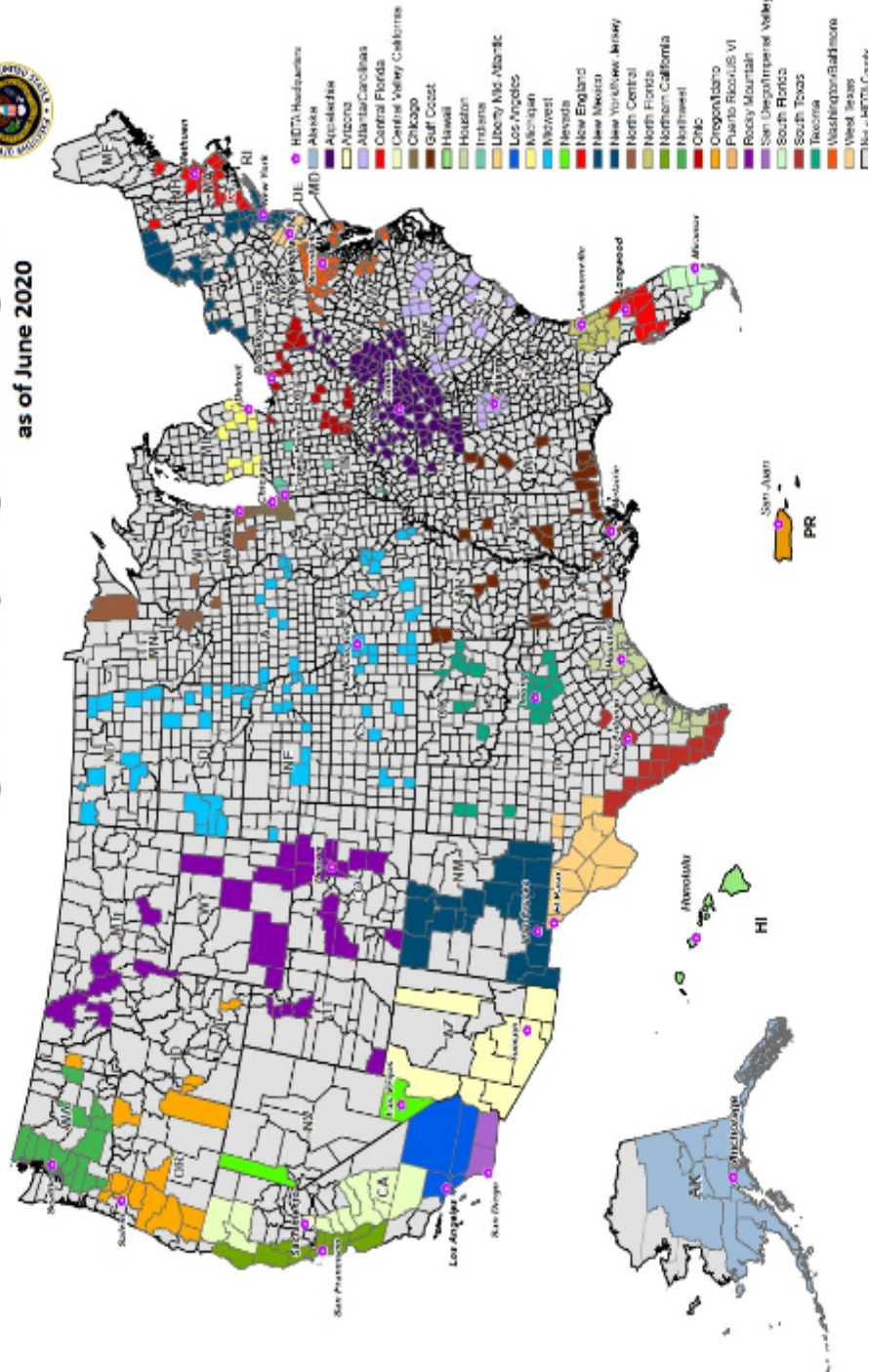
High-Risk Geographies

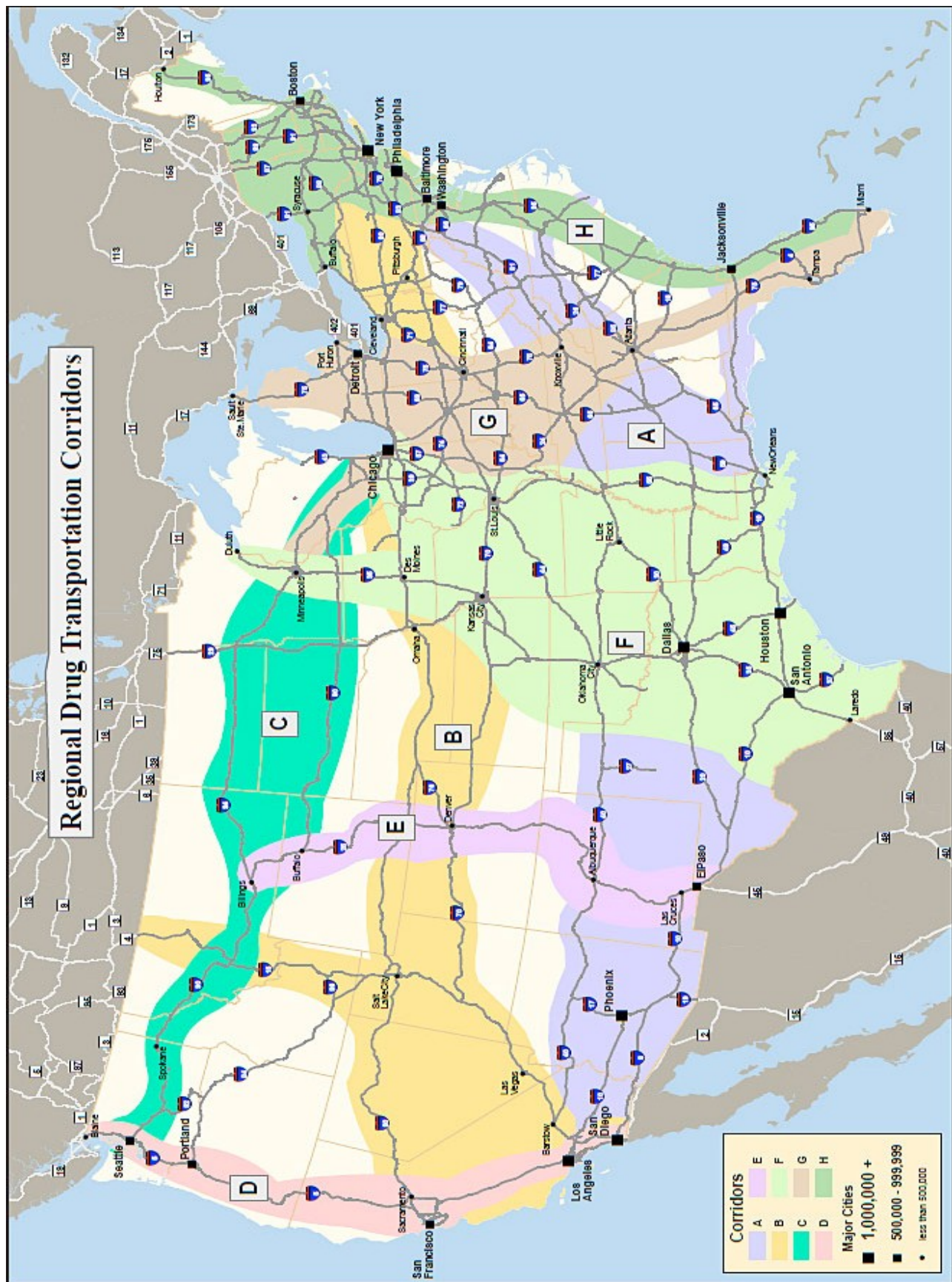
In identifying those geographic locations which present a “heightened risk” from the BSA/AML perspective, financial institutions could begin with the federally defined categories of high-risk geographic locations found in the *SAR Activity Reviews*, the *FFIEC BSA/AML Examination Manual*, and the Treasury Department’s National Money Laundering Strategy documents.

1. High-Risk and Non-Cooperative Jurisdictions (HRNCJ) – The Financial Action Task Force (FATF) publicly identifies countries with remaining AML deficiencies. Two public statements are issued three times a year (latest FATF Statement – 02/25/2021) and identify:
 - Countermeasures – jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply: Iran and Democratic People’s Republic of Korea (DPRK – North Korea). **NOTE:** On 11/04/16, Treasury sent to the federal register a final rule requiring banks to apply special due diligence to its foreign correspondent accounts reasonably designed to guard against their use to process transactions involving North Korean financial institutions;
 - Enhanced Due Diligence (EDD) – None
 - Due Diligence – jurisdictions which have strategic AML/CFT deficiencies for which they have developed an action plan with FATF: Albania; Barbados; Botswana; Burkina Faso; Cambodia; Cayman Islands; Ghana; Jamaica; Mauritius; Morocco; Myanmar; Nicaragua; Pakistan; Panama; Syria; Senegal; Uganda; Yemen; and Zimbabwe.
2. HIFCAs - High Risk Money Laundering and Related Financial Crimes Areas;
3. HIDTAs – High Intensity Drug Trafficking Areas;
4. Narcotics and Bulk Currency Corridors – (FIN-2011-A009);
5. OFAC Sanctioned Countries, including state sponsors of terrorism;
6. Section 311 Countries (Islamic Republic of Iran, Myanmar, DPRK (North Korea));
7. State Department identified countries supporting international terrorism – “Patterns of Global Terrorism” – www.state.gov/s/ct/.
8. Other countries identified by the financial institution as high-risk because of its prior experiences, transaction history, or other factors.



High Intensity Drug Trafficking Areas as of June 2020





Quantity of Risk Matrix – BSA/AML DFI Identified (Appendix J – Modified)

I. Client Base

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Stable, known client base.	Client base increasing due to branching, merger, or acquisition.	A large and growing client base in a wide and diverse geographic area.	(E.g. Low, Moderate, or High)	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Statistics/Volumes, Descriptions, Comments, and (most importantly) the Rationale supporting Management's Acceptance of the Residual Risk Rating – (IR minus CCs = Residual Risk)

The examiners are also now expecting to see "trend-line" analyses – percentage increases along with explanations as to "why" the change.

(Note: Peer group data from the regulatory agency would be most helpful in this analysis.)

(Note: AML/Risk Management System statistical output most helpful here as well).

(This analysis would accompany each of the factors identified in the Risk Matrix – could result in multiple pages of analysis per each factor)

II. Electronic Banking

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
No electronic banking (e-banking), or the depository financial institution's (DFI) web site is informational or non-transactional.	The DFI is beginning e-banking and offers limited products and services at the web site.	The DFI offers a wide array of e-banking products and services (E.g. account transfers, e-bill payment, opening accounts on-line).	(E.g. Low, Moderate, or High)	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – BSA/AML DFI Identified (Appendix J – Modified) (cont.)

III. Currency Processing

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Few, or no large currency or structured currency transactions.	Moderate volume of large currency or structured currency transactions	Significant volume of large currency or structured currency transactions.	(E.g. Low, Moderate, or High)	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

IV. High-Risk Clients

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Identified a "few" high-risk consumer and business clients.	Identified a "moderate" number of high-risk consumer and business clients.	Identified a "large" number of high-risk consumer and business clients.	(E.g. Low, Moderate, or High)	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – BSA/AML

DFI Identified

(Appendix J – Modified) (cont.)

V. Foreign Correspondent Bank Activity

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
No foreign correspondent bank accounts maintained. No pouch, special-use, "payable through accounts" (PTAs), or U.S. dollar draft services.	"Few" foreign financial institution accounts. Foreign DFIs have adequate AML policies and procedures and are from low-risk countries. Minimal pouch, special-use, PTAs, or U. S. dollar drafts.	"Large" number of foreign correspondent bank accounts. Foreign DFIs have inadequate AML policies and procedures, located in high-risk jurisdictions, substantial pouch, special-use, et al.	(E.g. Low, Moderate, or High)	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

VI. Private Banking / Trust

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Limited or no private banking, or trust and asset management products or services.	Limited domestic private banking or trust and asset management products and services over which the DFI has investment discretion. DFI's strategic plan may be to increase trust business.	"Significant" domestic and international private banking and trust services, and volumes are growing. Products offered include investment management services and non-discretionary activities (versus where the DFI has full investment discretion).	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – BSA/AML **DFI Identified** **(Appendix J – Modified) (cont.)**

VII. International Accounts

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
"Few" international accounts, or accounts with very low volumes of currency activity.	"Moderate" level of international accounts with unexplained currency activity.	"Large" number of international accounts with unexplained currency activity.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

VIII. Funds Transfer Activity

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
"Limited" number of funds transfers for clients, non-clients, limited third-party transactions, and no foreign funds transfers.	"Moderate" number of funds transfers. "Few" international funds transfers from personal or business accounts with typically low-risk countries.	"Large" number of non-client funds transfer transactions and payable-upon-proper-identification (PUPID) transactions. Frequent funds transfers from personal or business accounts to or from high-risk jurisdictions, and financial secrecy havens or jurisdictions.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – BSA/AML DFI Identified (Appendix J – Modified) (cont.)

IX. Geographic Presence

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
DFI not physically located in a HIFCA, HIDTA, or narcotics corridor. No funds transfers or account relationships involve HIFCAs or HDTAs.	DFI is located in a HIFCA, HIDTA, or narcotics corridor. "Some" funds transfers or account relationships that involve HIFCAs or HDTAs.	DFI is located in a HIFCA, HIDTA, or narcotics corridor, and a "large" number of funds transfers or account relationships involve HIFCAs/HDTAs.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

X. High-Risk Geographies

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
No transactions with other high-risk geographies.	"Minimal" transactions with other high-risk geographies.	"Significant" volume of transactions with other high-risk geographies.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

XI. Personnel Turn-over

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
"Low" turnover of key personnel or frontline personnel (E.g. customer service representatives, tellers, or other branch staff).	"Low" turnover of key personnel, but frontline personnel in branch network may have changed.	"High" turnover, especially in "key" personnel positions.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – OFAC DFI Identified (Appendix M and Matrix B – Modified)

I. Client Base

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Stable, well-known client base in a localized environment.	Client base changing due to branching, merger, or acquisition in the domestic market.	A large, fluctuating client base in an international environment.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Statistics/Volumes, Descriptions, Comments, and (most importantly) the Rationale supporting Management's Acceptance of the Residual Risk Rating – (IR minus CCs = Residual Risk)

The examiners are also now expecting to see "trend-line" analyses – percentage increases along with explanations as to "why" the change.

(Note: Peer group data from the regulatory agency would be most helpful in this analysis.)

(Note: AML/Risk Management System statistical output most helpful here as well).

(This analysis would accompany each of the factors identified in the Risk Matrix – could result in multiple pages of analysis per each factor)

II. High-Risk Clients

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
"Few" high-risk clients (which may include non-resident aliens (NRAs), foreign individuals (including accounts with U.S. powers of attorney), and foreign commercial clients.	A "moderate" number of high-risk clients.	A "large" number of high-risk consumer and business clients.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – OFAC DFI Identified (Appendix M and Matrix B – Modified) (cont.)

III. Overseas “Presence”

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
No overseas branches and no correspondent accounts with foreign banks.	Overseas branches or correspondent accounts with foreign banks.	Overseas branches or multiple correspondent accounts with foreign banks.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

IV. Electronic Banking

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
No electronic banking (e-banking), or the products offered are purely informational or non-transactional.	The DFI offers limited e-banking products and services.	The DFI offers a wide array of e-banking products and services (E.g. account transfers, e-bill payment, opening accounts on-line).	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

V. Funds Transfer Activity

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
“Limited” number of funds transfers for clients, non-clients, limited third-party transactions, and no international funds transfers.	“Moderate” number of funds transfer, mostly for existing clients. Possibly, a “few” international funds transfers from personal or business accounts.	“High” number of client and non-client funds transfer transactions, including international funds transfers.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – OFAC DFI Identified (Appendix M and Matrix B – Modified) (cont.)

VI. “Other” International Transactions

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
No other types of international transactions (E.g. trade finance, ACH - IATs, and management of sovereign debt.	“Limited” other types of international transactions.	“High” number of other types of international transactions.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

VII. OFAC “Errors”

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation.	“Small” number of recent actions (E.g. actions within the last five years) by OFAC, including notice letters, or CMPs, with evidence that the DFI addressed the issues and is not in risk of similar violations in the future.	“Multiple” recent actions by OFAC, where the DFI has not addressed the issues, thus leading to an increased risk of the DFI undertaking similar violations in the future.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – OFAC DFI Identified (Appendix M and Matrix B – Modified) (cont.)

VIII. Risk- Assessment

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Management has fully assessed the DFI's level of risk based on its client base and product lines. This understanding of risk and strong commitment to OFAC compliance is satisfactorily communicated throughout the organization.	Management exhibits a reasonable understanding of the key aspects of OFAC compliance and its commitment is generally clean and satisfactorily communicated throughout the organization, but it may lack a compliance program appropriately tailored to risk.	Management does not understand, or has chosen to ignore, key aspects of OFAC compliance risk. The importance of OFAC compliance is not emphasized or communicated throughout the organization.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

IX. OFAC Policy

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Board has approved an OFAC compliance program that includes policies, procedures, controls, and information systems that are adequate and consistent with the DFIs risk profile.	Board has approved an OFAC compliance program that includes most of the appropriate policies, procedures, controls and information systems necessary to ensure compliance, but some weaknesses are noted.	Board has not approved an OFAC compliance program, or policies, procedures, controls, and information systems are significantly deficient.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – OFAC DFI Identified (Appendix M and Matrix B – Modified) (cont.)

X. Staffing Levels

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Staffing levels appear “adequate” to properly execute the OFAC compliance program.	Staffing levels appear generally adequate, but some deficiencies are noted.	Management has failed to provide appropriate staffing levels to handle workload.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

XI. OFAC Officer (Board Approved)

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Authority and accountability for OFAC compliance are clearly defined and enforced, including the designation of a qualified OFAC compliance officer.	Authority and accountability are defined, but some refinements are needed. A qualified OFAC officer has been designated.	Authority and accountability for compliance have not been clearly established. No OFAC compliance officer, or an unqualified one, has been appointed. The role of the OFAC officer is unclear.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

Quantity of Risk Matrix – OFAC DFI Identified (Appendix M and Matrix B – Modified) (cont.)

XII. Training

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
Training is appropriate and effective based on the DFI's risk profile, covers applicable personnel, and provides necessary up-to-date information and resources to ensure compliance.	Training is conducted and management provides adequate resources given the risk profile of the organization; however, "some" areas are not covered within the training program.	Training is sporadic and does not cover important regulatory and risk areas.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

XIII. Quality Controls

Low	Moderate	High	Inherent Risk	Compensating Controls	Residual Risk Rating
DFI employs strong quality control methods.	DFI employs "limited" quality control methods.	DFI does not employ quality control methods.	E.g. Low, Moderate, or High	Listing the controls that take you from Inherent Risk to Residual Risk	(E.g. Low, Moderate, or High)

(Blank Page)

Developing an Institutional Risk Assessment Program

Program Steps There are a number of methodologies available to guide financial institutions as they develop an appropriate BSA/AML Risk Assessment. One approach includes five steps:

1. Assemble;
 2. Inventory;
 3. Develop;
 4. Implement; and
 5. Support and Ongoing Evaluation.
-

Assemble The first step is to assemble the appropriate team/task force. Representatives from appropriate areas throughout the financial institution should be formally assigned to the project, including:

- Compliance;
- Data Processing and Data Security;
- Audit;
- Security;
- Marketing/Product Management;
- Corporate Banking/Relationship Managers;
- Retail Banking/Relationship Managers;
- Human Resources/Training;
- Finance;
- Operations;
- Legal; and
- Senior Management.

Senior management representation assures the proper focus of the team and emphasizes the importance of the project.

Continued on next page

Developing an Institutional Risk Assessment Program,

Continued

Inventory

The second step is to identify/quantify the current level of risk present within the institution, and to identify/qualify how such risks are currently monitored and controlled. The team should:

1. Identify/Quantify the current risk levels:
 - Federal Guidance
 - Financial Institution Specific Factors
 - Decide on weightings and categorizations (e.g., high-medium-low)
2. Identify/Quantify (if/any) the current geographic risks:
 - Federal Guidance?
 - Where - Where are they located?
 - When - When did we start doing business there?
 - Why - Why are we doing business there?
3. Identify/Qualify how the risks are currently monitored and controlled:
 - Systems/reports utilized
 - Manual activities
 - Responsibilities/accountabilities
 - Review methods/audit
4. Determine “residual” risk level for each function and geography.
5. Determine if the "high-risk" functions/geographies should continue and the rationale for such decision (e.g., "good customer base", "High Profit Margins, et.al.).
6. Review where available similar information from industry peers, such as financial institutions with similar asset ranges, or in the same geographic locale.
7. Review current personnel levels to ascertain if staffing needs are covered adequately.

A comprehensive inventory phase results in an overall rating of residual risk and will identify any areas of weakness that need to be addressed.

Continued on next page

Developing an Institutional Risk Assessment Program,

Continued

-
- | | |
|--------------------|--|
| Development | <p>The third step is to develop any required enhancements to the program to allow for successful implementation. In this step the team:</p> <ul style="list-style-type: none">• Determines additional needs;• Identifies various alternatives to satisfy those needs;• Selects the most appropriate alternative after completing the business analysis of the alternatives;• Creates the internal, or acquires the necessary external, solutions;• Tests the solutions to ensure accuracy;• Prepares implementation plans and the conversion methodology, as well as assigns various accountabilities. Critical success factors will also be established during this phase;• Finalizes the internal audit and compliance process;• Completes any required changes to the ethics and personnel policies;• Determines appropriate training approach; and• Documents the changes in the written BSA/AML policy and procedures. |
|--------------------|--|
-

- | | |
|-----------------------|---|
| Implementation | <p>The fourth step is to formally implement the program solutions. In this step:</p> <ul style="list-style-type: none">• Initial team member training is completed;• Software and hardware solutions are moved into final production;• Operational routines are enabled;• Critical success factors are measured and reported; and• Board approval of the risk assessment and results. |
|-----------------------|---|
-

Continued on next page

Developing an Institutional Risk Assessment Program,

Continued

Support and Ongoing Evaluation

Risk assessment within financial institutions is not a journey to merely complete and then move on to the next totally unrelated task assignment. Risk assessment is an evolutionary mind-set that continues to grow and build within the institution and is the future of BSA/AML compliance. The worst mistake that a financial institution can make is not following the policy that it created and communicated. Continual evaluation of the overall program as well as ongoing training helps foster the mind-set of risk assessment, and assures compliance with the BSA/AML policy. Included in this fifth step are:

- Internal operating unit quality reviews;
 - Formal internal audits, the independent tests;
 - Ongoing training, communication of new risk developments, and the training of new team members;
 - Unit feedback and program modifications;
 - Federal compliance examinations; and
 - Periodic report to the Board – include as part of the periodic BSA review..
-



U.S. Department of the Treasury

Financial Crimes Enforcement Network

FIN-2014-A005

May 28, 2014

Advisory

Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML

Restrictions on USD cash transactions in Mexico may have led criminal actors to use additional schemes, such as using “funnel accounts” in conjunction with trade-based money laundering, to launder illicit proceeds.

The Financial Crimes Enforcement Network (FinCEN) is issuing this update to advise financial institutions on the increased use of funnel accounts as part of trade-based money laundering conducted by criminal actors

following the restrictions on U.S. currency transactions in Mexico. This Advisory provides “red flags” that may assist financial institutions identify and report suspicious funnel account activity.

Funnel Account: *An individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.*

Background

In June 2010, the Mexican government announced regulations limiting deposits of U.S. cash in Mexican banks.¹ Several months later, the Mexican government expanded the restrictions to include cash deposits made at exchange houses (casas de cambio) and brokerages (casas de bolsa). In 2011 and 2012, FinCEN issued two advisories that detailed the rise of funnel account use (also known as interstate or out-of-state funnel account activity) as a technique employed by individuals seeking to move illicit proceeds following the currency restrictions.²

Law enforcement information and Suspicious Activity Reports (SARs) now show that Mexico-related criminal organizations: (i) continue to employ funnel accounts to move illicit proceeds and (ii) are using funnel accounts to finance the purchase of goods as part of Trade-Based Money Laundering (TBML) activity. In some instances, multiple funnel accounts have been observed to transfer funds into a single consolidated account from where the funds are subsequently withdrawn. Criminal organizations use wires and checks issued

1. See, FinCEN (June, 2010) Advisory [FIN-2010-A007: “Newly Released Mexican Regulations Imposing Restrictions on Mexican Banks for Transactions in U.S. Currency.”](#)
2. See, FinCEN (April, 2011) Advisory [FIN-2011-A009: “Information on Narcotics and Bulk Currency Corridors”](#) and (July, 2012) Advisory [FIN-2012-A006: “Update on U.S. Currency Restrictions in Mexico.”](#)

from funnel accounts to move illicit narcotics proceeds to the accounts of businesses offering trade goods and services as part of trade-based money laundering as further described below.

Schemes such as the use of funnel accounts and TBML are a money laundering concern for both the U.S. and Mexican governments.

Funnel Accounts and Trade-Based Money Laundering

Typical steps of funnel account activity in conjunction with trade-based money laundering include:

- (I) A U.S. or foreign business owner or other individual, colluding with representatives of a criminal organization, opens an account at banks or credit unions whose accounts can readily receive cash deposits in multiple states through their own branches or through shared branches.³
- (II) Multiple individuals acting on behalf of representatives of the criminal organization deposit the cash proceeds of narcotics sales into this account at different bank or credit union branches, often in multiple states geographically distant from the branch in which the account was opened or domiciled. The deposits are kept below \$10,000 in order for transactors to avoid identification and record keeping requirements.
- (III) After a number of deposits have been credited to the account, an intermediary will initiate wire transfers (or issue checks) from the funnel account to a U.S. or foreign-based business for the purchase of goods that are then shipped to foreign countries for sale.
- (IV) Once the purchased goods arrive at the destination country, they are sold and the sale proceeds, in the destination country's currency, are transferred to the drug trafficking or money laundering organization to provide the criminal actors with funds that have been laundered through TBML.⁴

When the goods in this scheme are sold in Mexico, a drug trafficking organization or its intermediary, often termed a "money broker" or "peso broker,"⁵ will contract with a U.S. or Mexican business owner to open a funnel account at banks or credit unions whose accounts can readily receive cash deposits in multiple states. The peso broker subsequently directs the deposit of narcotics proceeds into the funnel account and makes payments from this account for the purchase of U.S. and foreign goods. These goods are then shipped to Mexican businesses where they are sold for pesos. In essence, the drug trafficking organization has exchanged the U.S. dollar cash proceeds in the United

3. Credit unions that do not have a national presence but participate in shared branching may also be vulnerable to this activity.

4. For additional information on TBML and potential indicators of TBML activity, see FinCEN (February, 2010) Advisory [FIN-2010-A001: "Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering."](#)

5. Money brokers or peso brokers are third parties that seek to purchase drug proceeds located in the United States from Mexican cartels at a discounted rate. Once purchased, money brokers take possession of the drug proceeds that are, in turn, frequently sold to Mexican based businesses seeking U.S. dollars to buy goods from businesses in the United States and in other countries.

States for Mexican pesos in Mexico through the use of a funnel account and TBML. The criminal actors can both repatriate and give a plausible source to the proceeds of illicit activity obtained in the United States through apparently legitimate business transactions.

Funnel Accounts and Trade-Based Money Laundering Red Flags

A funnel account associated with TBML might manifest one or more of the following red flags:

- An account opened in one state (typically along the Southwest border) receives multiple cash deposits of less than \$10,000 by unidentified persons at branches outside of the geographic region where the account is domiciled. The accounts receiving the out-of-state deposits can be either individual or business accounts.
- In the case of a business account, the deposits take place in a different geographic region from where the business operates.⁶ For example, the account of a produce company operating locally in Southern California receives small cash deposits, below the currency reporting threshold, at bank branches in Chicago, Indianapolis, and Minneapolis.
- If questioned, the individuals opening or making deposits to funnel accounts may have no detailed knowledge about the stated business activity of the account, the account holder (in the case of a depositor), or the source of the cash. This is because criminal organizations sometimes pay individuals outside their organization, such as students, itinerant workers, or the un/under-employed to open or carry out funnel account transactions.
- In the case of a business account receiving out-of-state deposits, the debits do not appear to be related to the stated business activity of the account holder. For example, checks drawn on the account of a produce company are made payable to a leather goods business, or funds are wired from the produce company's account to a textile manufacturer in China.⁷
- Checks issued from an account that receives out-of-state cash deposits appear to have different handwriting on the payee and amount lines than the signature line. This may indicate that (i) the checks, originally issued to the account holder, have been pre-signed but the payee and amount lines have been left blank, then (ii) the checks were handed over to a criminal organization, which then (iii) used the checks to pay U.S. or foreign parties by populating the payee and amount fields.
- Wire transfers or checks issued from a funnel account are deposited into, or cleared through, the U.S. correspondent account of a Mexican bank. In addition to exhibiting funnel account activity, in some cases, checks issued from the U.S. account name a Mexican bank as payee and the checks are either deposited into the Mexican bank's U.S. correspondent account or are cleared through said correspondent account by cash letter.

6. Often termed "operating outside the geographic footprint."

7. This differs from traditional funnel account activity where cash would otherwise be withdrawn from the account and be provided to the drug trafficking or money laundering organization.

FinCEN Guidance to U.S. Financial Institutions

Because some red flags of funnel accounts and TBML are, in appropriate circumstances, legitimate financial activities, financial institutions should evaluate indicators of potential TBML activity in combination with other red flags and the expected transaction activity for the customer implicated before making determinations of suspiciousness. No one activity by itself is a clear indication of trade-based money laundering. Financial institutions are encouraged to use previous FinCEN advisories as a reference when evaluating potential red flags; FinCEN has published advisories expanding on TBML,⁸ high intensity drug trafficking areas⁹ and the impact of U.S. currency restrictions in Mexico.¹⁰

As a result of the U.S. currency restrictions in Mexico, illicit actors may utilize one or more different methodologies, including funnel accounts, TBML, or movement through other jurisdictions to repatriate illicit proceeds. Additionally, financial institutions should consider and manage the risk associated with receiving deposits from non-customers or unidentified parties. FinCEN continues to evaluate information on money laundering activities involving transnational criminal organizations operating in Mexico and the United States and will report, as appropriate, on emerging methods and schemes used to launder criminal proceeds.

If a financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, attempts to disguise funds derived from illegal activity, is designed to evade regulations promulgated under the Bank Secrecy Act, or lacks a business or apparent lawful purpose, the financial institution may be required to file a SAR.¹¹ While the transactional activity that U.S. financial institutions may experience as a result of the Mexican restrictions may not be indicative of criminal activity, U.S. financial institutions should consider this activity in conjunction with other information, including transaction volumes and source(s) of funds, when determining whether to file a SAR.

Financial institutions should continue to be alert to the variety of methods that may be used to move funds linked to the laundering of criminal proceeds and to report that information as appropriate. FinCEN requests financial institutions to include "MX Restriction" in both the Narrative and the Suspicious Activity Information¹² sections of SARs to indicate a possible connection between the suspicious activity being reported and the enacted U.S. currency restrictions on Mexican financial institutions.

8. See, FinCEN (February, 2010) Advisory [FIN-2010-A001: "Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering."](#)

9. See, FinCEN (April, 2011) Advisory [FIN-2011-A009: "Information on Narcotics and Bulk Currency Corridors."](#)

10. See, FinCEN Advisories [FIN-2010-A007](#) and [FIN-2012-A006](#).

11. See, e.g., 31 CFR § 1020.320.

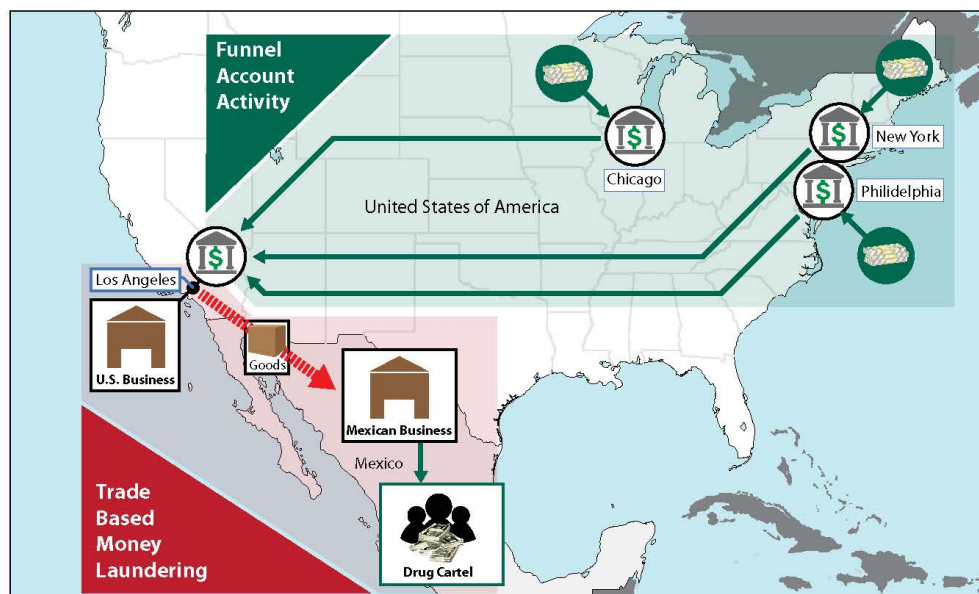
12. Financial institutions may include any relevant key terms in the "Other" fields of items 29 through 38, as applicable, of Part II (Suspicious Activity Information) of the SAR.

In addition, where the use of funnel accounts and or TBML is suspected in the laundering of criminal proceeds, including specific reference to the terms “Funnel Account” and or “TBML” in the Narrative and Suspicious Activity Information sections of SARs is also requested. Financial institutions may include in SARs any or all terms, “MX Restriction,” “Funnel Account” and or “TBML,” as applicable.

Questions or comments regarding the contents of this or any other advisories should be addressed to the FinCEN Resource Center at (800) 767-2825 or (703) 905-3591. ***Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

APPENDIX I

Funnel Account Activity and Trade Based Money Laundering



The above graph illustrates how illicit proceeds, through funnel accounts (highlighted in green), may fuel the purchase of goods as part of a Trade Based Money Laundering (TBML) scheme (highlighted in red).

In this example, proceeds from the sale of drugs are deposited (in the form of currency) into the bank account of a business (controlled by a Mexican cartel) that operates exclusively in Los Angeles, CA. Deposits in the account are conducted through bank branches located in cities where the business does not operate because these localities often represent the areas where the illicit proceeds are derived from. In this example, bank branches used to make deposits into the business' account are located in Chicago, IL; Philadelphia, PA; and New York, NY.

The second part of the example illustrates how the Mexican cartel uses the illicit proceeds, deposited through funnel account activity, to

engage in a TBML scheme. After receiving the funds that have been deposited into the business' account, a peso broker, acting as an intermediary, purchases goods in the United States. The peso broker then coordinates the shipment of the purchased merchandise to Mexico where he/she has partnered with a Mexican business to sell the goods. In exchange for the merchandise purchased by the peso broker (with drug proceeds), the Mexican business provides the cartel with clean pesos. By engaging in this TBML scheme, the Mexican cartel has laundered and repatriated drug proceeds that had been obtained in the United States.

CURRENCY TRANSACTION REPORTING

I. REPORTABLE TRANSACTIONS

- A. Reporting Requirements** – Each financial institution shall file a report of each transaction in currency of more than \$10,000 to the Federal government, except as otherwise provided in the regulations.

NOTE: Treasury has the authority to target specific geographic areas for brief periods of time and reduce the dollar threshold for filing CTRs. For example, if illegal activity was suspected locally, Treasury might notify all banks in a three-county area to file CTRs on all cash transactions above \$3,000 for the next 60 days.

1. To be reportable, there must be a physical transfer of currency from one person to another, in an amount exceeding \$10,000. A transaction which is a transfer of funds by means of bank check, bank draft, wire transfer, or other written order, and which does not include the physical transfer of currency, is not a reportable transaction.
 - a. “Currency” includes coin and paper money which circulates as legal tender and is customarily accepted as a medium of exchange either in the United States or a foreign country.
2. Whenever a single deposit, withdrawal, exchange of currency or other payment or transfer by, through, or to a bank exceeds \$10,000, it must be reported.

EXAMPLE: The sale of a cashier's check for \$12,000 in cash to a retailer and the receipt of an \$11,000 loan payment in cash are both reportable transactions. (Remember, you are not just looking for deposits and withdrawals.)

B. Multiple Transactions

1. Multiple currency transactions taking place on the same business day are treated as a single transaction if the bank has knowledge that they are by or on behalf of the same person.
 - a. In this context, “business day” means that day on which a bank, as normally communicated to its depository customers, routinely posts a particular transaction to its customer's account.

EXAMPLE: Although a local bank remains open until 4 p.m., its business day “cuts off” at 2:30 p.m.; deposits and withdrawals made after 2:30 p.m. are posted on the following business day. If a customer deposited \$6,000 in cash at 10:00 a.m. on July 1 and another \$6,000 in cash at 3:30 p.m. on July 1, no reportable transaction has occurred; the deposits are posted on separate business days and need not be aggregated.

EXAMPLE: A local bank is closed on Saturday and Sunday and a merchant makes night deposits of \$6,000 in cash on each of those days. Since both deposits will be processed or posted to the customer's account on the same business day (Monday), they must be added together for reporting.

2. A reportable transaction occurs when the total of currency received (Cash In) or disbursed (Cash Out) by the bank for the same account or customer on the same business day exceeds \$10,000. Cash In and Cash Out transactions are considered separately and are not offset against one another.

EXAMPLE: If a customer made two \$6,000 cash withdrawals on the same business day it would be reportable as \$12,000. However, if a customer made a \$6,000 cash withdrawal and later makes a \$6,000 cash deposit, no report is necessary.

EXAMPLE: If a customer comes in with \$12,000 in cash and deposits it into two accounts, with neither receiving more than \$10,000, it is reportable.

EXAMPLE: If customer A makes a \$6,000 cash deposit to the XYZ account and later on the same business day customer B makes a second \$6,000 cash deposit to the XYZ account, it is reportable.

3. When an exchange of currency is involved, it is added separately to each of the Cash In and Cash Out totals.

EXAMPLE: A customer deposits \$6,000 in currency to his savings account and withdraws \$4,000 in currency from his checking account. He also presents \$5,000 in cash to be exchanged for the equivalent in Euros. The \$5,000 presented for the currency exchange is added to both the Cash In and Cash Out transactions in determining whether the reporting threshold is met. The result is a reportable Cash In transaction of \$11,000. The total Cash Out amount is \$9,000, which does not meet the reporting threshold.

4. Transactions at all of the bank's branches are considered together.

EXAMPLE: If the bank has knowledge that two \$6,000 deposits are made to the same account on a single business day it must file a report, even if the transactions occur at different branches.

5. Multiple currency transactions taking place on the same business day must be aggregated if the bank has knowledge that they are by or on behalf of the same person.

- a. "Knowledge" that multiple transactions are by or on behalf of the same person means knowledge on the part of a director, officer, or employee.

EXAMPLE: A \$6,000 cash deposit is made into the XYZ account through Teller A. Later in the same business day, a second \$6,000 cash deposit is made to the XYZ account through the same teller. The bank "has knowledge" and must report the transaction.

- b. “Knowledge” also includes knowledge derived from an existing system at the bank which permits it to aggregate transactions.

EXAMPLE: The bank has voluntarily adopted the use of currency transaction logs where cash transactions above an internally established "notice amount" are recorded as they occur. If the same individual conducts multiple transactions which, when aggregated, exceed the reporting amount, proper utilization and review of the currency transaction logs will bring the multiple transfers to the attention of BSA compliance personnel. In this case, the bank "has knowledge" and must report the transaction.

NOTE: Banks have no specific responsibility to adopt or purchase systems or EDP programs to reveal the existence of multiple same day transactions. However, if a bank has a system which provides information on transactions which may require reporting as aggregated transactions, the bank must make use of that system. This is a classic "Catch 22" situation: Although the Treasury would like for banks to adopt systems that allow them to aggregate multiple transactions, banks are not required to do so. However, if they voluntarily adopt such a system they raise the standard of care to which they are subjected in the area of BSA compliance; they are judged on whether the system actually works or is properly used.

C. Structuring – Structuring is the breaking down of currency transactions into amounts under \$10,000 for the purpose of evading reporting requirements. Failing to observe the reporting requirements, or intentionally splitting a transaction into parts in order to fall below reporting thresholds can be a crime and can result in civil enforcement actions, including fines. These consequences can apply even when the funds involved were derived from legitimate, not criminal, activity.

1. Bank personnel should never advise someone to structure deposits or other transactions to avoid currency transaction reporting requirements. Such activity may be subject to criminal prosecution.
2. If structuring is detected or suspected, and the multiple transactions conducted on the same business day exceed \$10,000 when aggregated, a CTR must be filed to report the currency transactions. A Suspicious Activity Report (SAR) should also be filed to report the suspicious activity of structuring.

II. FILING REQUIREMENTS – Reportable currency transactions must be reported on a FinCEN Currency Transaction Report (CTR) – FinCEN Form 112.

Currency Transaction Report

Home

Step 1. Filing Institution
Contact Information

Step 2. Transaction Location(s)
Information

Step 3. Person(s)
Involved Information

Step 4. Amount and Type of
Transaction(s)



Currency Transaction Report

OMB No. 1506-0004, OMB No. 1506-0005, OMB No. 1506-0064

Version Number: 1.3

Steps to Submit

1. Complete the report in its entirety with all requested or required data known to the filer.
2. Click "Validate" to ensure proper formatting and that all required fields are completed.
3. Sign with PIN.
4. Click "Save"; filers may also "Print" a paper copy for their records.
5. Click "Submit".

Filing Name

*1 Type of filing

☐ Initial report

☐ Correct/amend prior report

☐ FinCEN directed Backfiling

Prior report BSA Identifier

Save

Validate

Submit

Print

By providing my PIN, I acknowledge that I am electronically signing the BSA report submitted.

Sign with PIN

Release Date: 04/29/2020

PAPERWORK REDUCTION ACT NOTICE

Public reporting and recordkeeping burden for this collection of information is estimated to average 40 minutes per response. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information to the Department of Treasury, Financial Crimes Enforcement Network, PO Box 39, Vienna, VA 22183.

Page 1 of 5

Currency Transaction Report	
Home	Step 1. Filing Institution Contact Information

Step 2. Transaction Location(s) Information
Step 3. Person(s) Involved Information
Step 4. Amount and Type of Transaction(s)

Part IV Filing Institution Contact Information

*52 Type of financial institution

Other (specify)

*43 Primary federal regulator

53 If 52a - Casino/Card Club is checked, indicate type (check only one)

☐ State licensed casino
☐ Tribal authorized casino
☐ Card club
☐ Other

*44 Legal name of filing institution

45 Alternate name, e.g. trade name, DBA

*46 EIN

*47 Address

*48 City

*49 State

*50 ZIP Code

*51 Country

54 Filing institution ID type

ID number

*55 Contact office

*56 Phone number Ext.

*57 Date filed (Date filed will be auto-populated when the form is signed.)

Currency Transaction Report

Home
Step 1. Filing Institution Contact Information
Step 2. Transaction Location(s) Information
Step 3. Person(s) Involved Information
Step 4. Amount and Type of Transaction(s)

Part III Transaction Location 1 of 1 + -

Would you like to insert all applicable filing institution information into Part III? Yes

*38 Type of financial institution

Other (specify)

*29 Primary federal regulator

39 If 38a - Casino/Card Club is checked, indicate type (check only one)

☐ State licensed casino
 ☐ Tribal authorized casino
 ☐ Card club
 ☐ Other

*30 Legal name of financial institution

31 Alternate name, e.g. trade name, DBA

*32 EIN ☐ Unknown

*33 Address

*34 City

*35 State

*36 ZIP Code

*37 Country

40 Financial institution ID type

ID number

*41 Cash in amount for transaction location

*42 Cash out amount for transaction location

Currency Transaction Report			
Home	Step 1. Filing Institution Contact Information	Step 2. Transaction Location(s) Information	Step 3. Person(s) Involved Information

Part I Person Involved in Transaction(s) 1 of 1 + -			
*2 <input type="checkbox"/> a Person conducting transaction on own behalf 3 <input type="checkbox"/> Multiple transactions	b <input type="checkbox"/> Person conducting transaction for another	c <input type="checkbox"/> Person on whose behalf transaction was conducted	d <input type="checkbox"/> Common carrier

Check <input type="checkbox"/> If entity	
*4 Individual's last name or entity's legal name	<input type="checkbox"/> Unknown <input style="width: 100%;" type="text"/>
*5 First name	<input type="checkbox"/> Unknown <input style="width: 100%;" type="text"/>
6 Middle name	<input style="width: 100%;" type="text"/>
Suffix	<input style="width: 100%;" type="text"/>
7 Gender	<input style="width: 100%;" type="text"/>
8 Alternate name	<input style="width: 100%;" type="text"/>
9 Occupation or type of business	<input style="width: 100%;" type="text"/>
9a NAICS Code	<input style="width: 100%;" type="text"/>
*10 Address	<input type="checkbox"/> Unknown <input style="width: 100%;" type="text"/>
*11 City	<input type="checkbox"/> Unknown <input style="width: 100%;" type="text"/>
*12 State	<input type="checkbox"/> Unknown <input style="width: 100%;" type="text"/>
*14 Country	<input type="checkbox"/> Unknown <input style="width: 100%;" type="text"/>
*15 TIN	<input type="checkbox"/> Unknown <input style="width: 100%;" type="text"/>
*17 Date of birth	<input type="checkbox"/> Unknown <input style="width: 100%;" type="text"/>
18 Contact phone number	<input style="width: 100%;" type="text"/>
19 E-mail address	<input style="width: 100%;" type="text"/>
*20 Form of identification used to verify identity	<input type="checkbox"/> Unknown
<input type="checkbox"/> Driver's license/State ID	<input type="checkbox"/> Passport
<input type="checkbox"/> Alien Registration	<input type="checkbox"/> Other
Number <input style="width: 100%;" type="text"/>	Country <input style="width: 100%;" type="text"/>
21 Cash in amount for individual or entity listed in Item 4	\$ <input style="width: 100%;" type="text"/>
Account number	<input style="width: 100%;" type="text"/>
22 Cash out amount for individual or entity listed in Item 4	\$ <input style="width: 100%;" type="text"/>
Account number	<input style="width: 100%;" type="text"/>

Currency Transaction Report

Home

Step 1. Filing Institution
Contact Information

Step 2. Transaction Location(s)
Information

Step 3. Person(s) Involved
Information

Step 4. Amount and Type of
Transaction(s)

Part II Amount and Type of Transaction(s). Check all boxes that apply.

*23 Date of transaction

24 ☐ Armored car (FI Contract) ☐ ATM ☐ Mail deposit or shipment ☐ Night deposit ☐ Aggregated transactions ☐ Shared branching

*25 CASH IN: (in U.S. dollar equivalent)

a Deposit(s) \$.00

b Payment(s) .00

c Currency received for funds transfer(s) out .00

d Purchase of negotiable instrument (s) .00

e Currency exchange(s) .00

f Currency to prepaid access .00

g Purchases of casinos chips, tokens and other gaming instruments .00

h Currency wager(s) including money plays .00

i Bills inserted into gaming devices .00

z Other (specify): .00

Total cash in \$.00

*27 CASH OUT: (in U.S. dollar equivalent)

a Withdrawal(s) \$.00

b Advance(s) on credit (including markers) .00

c Currency paid from funds transfer(s) in .00

d Negotiable instrument(s) cashed .00

e Currency exchange(s) .00

f Currency from prepaid access .00

g Redemption(s) of casino chips, tokens, TITO tickets and other gaming instruments .00

h Payment(s) on wager(s) (including race and OTB or sports pool) .00

i Travel and complimentary expenses and book gaming incentives .00

j Payment for tournament, contest or other promotions .00

z Other (specify): .00

Total cash out \$.00

26 Foreign cash in

Foreign Country

+ -

28 Foreign cash out

Foreign Country

+ -

A. Timing

1. A CTR must be filed within 15 calendar days after the reportable transaction. The FinCEN CTR must be electronically filed through FinCEN's *BSA E-Filing System*.
2. A bank should never delay the filing of a CTR even though information called for in the CTR cannot be obtained before the filing deadline.

NOTE: If a bank finds that it has failed to file one or more CTRs in a timely fashion it should first verify that the nonfilings are not symptomatic of a larger, widespread problem. If the number of unfiled forms is significant, the bank should contact FinCEN and request a "backfiling" determination. The alternative decision, not to file inadvertently omitted CTRs on the premise that regulatory detection is unlikely, may be a criminal act subject to prosecution.

3. A copy of each CTR filed must be retained for five years from the date it is filed.

B. Content – The CTR is completed according to its accompanying instructions. While most of the information sought is routine description of the transaction and the bank at which the transaction occurred, some items of information require special attention.

1. Identification Requirements - All individuals (except employees of an armored car service operating as an agent of the reporting financial institution) conducting reportable transactions for themselves or for another person, must be identified by means of an official document.
 - a. Acceptable forms of identification include driver's license, military or military/dependent identification card, passport, state issued identification card, foreign cedula card, non-resident alien identification card, or any other identification document which contains name and preferably address and a photograph and is normally acceptable by financial institutions as a means of identification when cashing checks for persons other than established customers.
 - b. Acceptable identification information obtained previously and maintained in the financial institution's records may be used. For example, if documents verifying an individual's identity were examined and recorded on a signature card when an account was opened, the financial institution may rely on that information. In completing the FinCEN CTR, the financial institution must indicate on the form the method, type, and number of the identification. Statements such as "known customer" or "signature card on file" are prohibited and are not sufficient for form completion. The actual identifying information must be provided.
 - c. On Form 112 – Line 20 (Form of Identification used to verify Identity) – Assume that when filing a Part 1 page on a business or non-human entity, Box 20 – "Other" will be checked and the business materials utilized during the verification process for CIP

(E.g. state Certificate of Good Standing, et al) are to be inserted into the block.

2. Recording Information - Complete each FinCEN CTR by providing as much information as possible. Although all items should be completed fully and accurately, items marked with an asterisk (*) must be completed. Filers must follow the instructions for these items by providing the required data *OR, IF THE INSTRUCTIONS PERMIT*, by checking the box labeled, “Unknown” to indicate that the required data was unknown or not applicable. Items that do not begin with an asterisk must be completed if the data are known and will be left blank if the data are unknown. If an item’s instructions differ from this general instruction, the item instructions must be followed. This instruction supersedes all prior instructions or guidelines issued by FinCEN on use of special responses in BSA forms when information is unknown or not available. Therefore, the use in a FinCEN CTR of special responses such as “UNKNOWN,” “NONE,” “NOT APPLICABLE,” or “XX” and their variants is now prohibited. Instructions for any previous version of the Currency Transaction Report do not apply to the FinCEN CTR. (Assume for Line 9 – Occupation or type of business – that although no “*” appears, for financial institutions, that has never been a non-critical field and filers will be expected to complete the box being as descriptive as possible).
3. Corrected or Amended Reports – A corrected report must be filed whenever errors are discovered by the DFI in a previously filed FinCEN CTR. Amended reports must be filed whenever additional data about the transactions previously reported are discovered. Both corrected and amended reports must be complete in their entirety, with the necessary corrections or amendments made to the data. In both cases box “1b” must be checked on the FinCEN CTR. Field “1d” must contain the BSA Identifier (BSA ID) assigned to the prior filing. **NOTE:** - If the FinCEN CTR corrects or amends a CTR, fields not present on the prior filing must be completed by the filer if the data are available.

In some cases, FinCEN will find errors on CTRs that must be addressed by the filing institution. There are two main categories of errors identified in batch files: Schema validation errors that result in automatic rejection of the batch; and data errors that represent errors in data entered for individual elements but may not result in rejection. Schema validation errors prevent the batch from being processed and are considered fatal errors. (Filers should immediately correct and resubmit a batch file rejected for fatal format errors. Rejection of a batch does not relieve the filer of the responsibility to file a CTR within 15 days following the day on which the reportable transaction occurred).

Data errors that result in the acceptance of the batch file are classified as either primary errors or warning errors. Primary errors are data errors that violate electronic filing requirements or report instructions and so degrade CTR data quality that they must be corrected. Warning errors are secondary data errors that violate electronic filing requirements or report instructions but have a lesser impact on data quality. CTRs accepted with primary errors must be re-filed as a corrected report, correcting the primary errors. CTRs accepted with both primary and warning errors must be re-filed as a corrected report, correcting all the errors. CTRs accepted

with only warning errors need not be refiled. FinCEN requires that filers prevent ALL reported errors in their future filings.

FinCEN recommends that primary error corrections be made no later than 30 days after receiving error notifications. FinCEN recommends that filers remedy any systemic problems in their electronic submissions within 30 days of receiving error notifications. (See Attachment B in the *FinCEN Currency Transaction Report Electronic Filing Requirements* for additional information on correcting FinCEN reported errors in CTR filings).

4. **Addresses** - For addresses in the U.S., Canada, or Mexico enter the permanent street address, city, two or three letter state/territory/province abbreviation or code, ZIP Code or foreign postal code, and two letter country code. Provide the apartment number or suite number, if known, following the street address. A non-location address such as a post office box or rural route number should be used only if no other street address information is available. ZIP Codes must be five or nine digits. ZIP Codes and foreign postal codes must be entered without formatting or special characters such as spaces or hyphens. For example, the ZIP Code 12354-6120 would be entered as 123546120. The foreign postal code HKW 702 would be entered HKW702. For other foreign addresses enter the street address, city, postal code, and two letter country code or address equivalent. Leave the state item blank, including the "Unknown" box. If a foreign address contains address information that does not conform to the FinCEN CTR address format, record equivalent address information in the FinCEN CTR address items (except state) and ignore non-conforming data. Complete any address item that is known, even if the entire address is unknown. No abbreviations are permitted in city names, which must be completely spelled out. A U.S. city name should match the city name used by the U.S. Postal Service for the associated state and ZIP Code.
5. **Telephone Numbers** - Record all telephone numbers, both foreign and domestic, as a single number string without formatting or special characters such as parentheses, spaces, or hyphens. For example, a number in the format (NNN) NNN-NNNN would be recorded as NNNNNNNNNN. If known, provide the telephone extension number in the associated field. Telephone numbers that are part of the North American Numbering Plan used by the U.S., Canada, many Caribbean countries, and present/former U.S. Pacific island protectorates must consist of an area code and seven-digit telephone number. Other foreign telephone numbers should include the country number code. If only a partial telephone number is known, record that number in the phone number item.
6. **Identifying Numbers** - Enter all identifying numbers as a single text string without formatting or special characters such as hyphens or periods. An identifying number in the format NNN-NN-NNNN would be entered as NNNNNNNNNN. Such numbers may include letter and number characters. Common identifying numbers include account numbers, alien registration numbers, driver's license and state identification numbers, Employer Identification Numbers (EIN), passport numbers, Social Security Numbers, and industry specific identifiers such as National Futures Association (NFA) numbers and Securities and Central Registration Depository (CRD) numbers.

7. Monetary Amounts – Monetary amounts are recorded in U.S. Dollars, rounded up to the next whole dollar. A foreign currency amount is converted to the U.S. Dollar equivalent to determine whether the CTR reporting threshold has been met, using the exchange rate for the date of the transaction, and rounded up to the next whole amount. On Form 112 – Line 21-Cash in amount for the individual or entity listed in Item 4 – filers will complete Line 21 with the amount of cash by or on behalf of the human/entity entered into Line 4, so long as the amount entered is not greater than the cash amount entered into Line 25 – Total Cash In.
8. Prohibited words and phrases: Filers may not use the following words or variations of these words in fields on the FinCEN CTR:
- a. AKA
 - b. COMPUTER GENERATED
 - c. CUSTOMER
 - d. DBA
 - e. NONE
 - f. NOT APPLICABLE
 - g. NON CUSTOMER
 - h. OTHER
 - i. SAME
 - j. SAME AS ABOVE
 - k. SEE ABOVE
 - l. SIGNATURE CARD
 - m. UNKNOWN
 - n. VARIOUS
 - o. XX
9. Name Editing Instructions - Because many names do not consist of a single first name, middle name, and last name, care must be taken to ensure these names are entered properly in the FinCEN CTR. This is especially important when there are separate fields for the last name, first name, and middle name. Some names have multiple surnames (family names) or given names. Others may not be written in [first name] [middle name] [last name] order. Multiple surnames must be entered in the last name field. For example, Hispanic names may be written in the order of given name, father's last name, and mother's last name, e.g., "Juan Vega Santiago." Thus the surname "VEGA SANTIAGO" would be entered in the last name field with "JUAN" entered in the first name field. Some Hispanic surnames consist of three names (e.g., father's last name, mother's last name, and husband's first last name). In that case all three would be entered in a last name field. Hispanic names do not have middle names, so a multiple Hispanic given name such as "Rosa Maria" would be recorded in the first name field.

In some cultures names consist of multiple first names and a single family name, not necessarily in (first name) (last name) order. For example, the Korean name "Kim, Chun Nam" consists of the family name "Kim" and the first name "Chun Nam" separated by a comma and space. There is no middle name. In this case "KIM" would be entered in the last name field and "CHUN NAM" would be entered in the first name field. Nothing is entered in the middle name field. When an individual name is entered in a single name field it should be entered in [first name] [middle name] [last name] order regardless of any foreign naming conventions. Thus, "Kim, Chun Nam" would be entered as "CHUN NAM KIM" in a single field.

Punctuation and special characters should be used in names only when they are part of the name. For example, the period in “Expedia.Com” should be included because it is part of the name. Placing a period after a middle initial is prohibited because the period is not part of the middle name.

Abbreviations in names are prohibited unless an abbreviation is part of a legal name. Entry of middle initials is permitted when a middle name is unknown. A name suffix may be abbreviated, i.e. Junior can be JR, Senior can be SR, the Third can be III, etc.

10. “Thoughts and Musings” – Form 112 – When entering data into CTR Form 112, filers should take into consideration the following:
 - a. On the updated Form 112, the form is completed starting with the Cover Sheet, then Part IV (Reporting Financial Institution – The entity that files the CTR, be it a financial institution or a holding or other parent company filing for its subsidiaries.), then Part III (Transaction Location Information – Each transaction location involved in the currency transactions.), then Part I, and finishing with Part II. In each discrete CTR filed, there will always be 1 – Cover Sheet, 1 - Part II, and 1- Part IV pages. There will be at least one and possibly more Part I and Part III pages.
 - b. For every Box 2C utilized on the 112, filers will have at least one corresponding 2A, 2B, and or 2C page unless a block or blocks in Line 24 are selected. Line 24 explains “why” no conductor information is presented on Form 112. Line 24 “Shared Branching” is used if the transaction was conducted on behalf of another financial institution that is a member of a co-operating network (this option applies only to credit unions that are members of a cooperative).
 - c. Box 2D (Common Carrier) versus Box 24 Armored Car (FI contract) – the respective box is selected depending upon with whom the agency relationship is maintained. If the client hires the armored carrier or the private courier to transport their currency to or from the financial institution, Box 2D is selected and the Part 1 page is completed accordingly. If the financial institution hires the armored carrier to transport the currency to or from the financial institution, Box 24 Armored Car is selected, and no corresponding Part 1 page is completed, as the armored car is the agent of the financial institution.

- d. Line 2 – Persons involved in the Transaction – If multiple Line 2 Options exist FinCEN’s guidance states to complete the CTR as follows:
- (1) If 2d applies – select 2d;
 - (2) If 2a, 2b, and 2c apply – select 2a – (e.g., Reportable deposits to personal joint accounts).
 - (3) If Box 2d is checked to indicate an armored car service under contract with the customer, then Box 4b, “If Entity” must also be checked.
 - (4) If more than one Item 2 option applies to a Part 1 person, a separate Part 1 section will be prepared on that person for each Item 2 option. For example, if the Part 1 person conducted a \$ 5,000 deposit into their personal account, and a separate \$7,000 deposit into the account of another person/entity, there will be one Part 1 on that person reporting option 2a on the personal deposit, with that amount (E.g., \$5,000) and account number in Item 22. There will be a second Part 1 on that same person reporting option 2b on the person/entity account transaction with that amount (E.g. \$7,000) and account number in Item 22. (This does NOT apply to reportable deposits to personal joint accounts).
- e. Line 3 – Multiple Transactions – Check Item 3 if multiple cash transactions of any amount totaling more than \$10,000 as cash in or more than \$10,000 as cash out (cash in and cash out transactions should not be combined) were conducted in a single business day by or on behalf of the same person.
- f. Line 24e – Aggregated Transactions maps to the old box above Line 15 of the legacy CTR (Form 104) labeled “Multiple Transactions”. Line 24 Aggregated Transactions is checked to indicate “why” no conductor was known and presented on Form 112. Line 24e “Aggregated Transactions” is checked when:
- ✓ there were multiple currency transactions involved in the report; and
 - ✓ the filing institution did not identify any of the individuals conducting the reportable transactions; and
 - ✓ all of the transactions involved currency below the reporting requirement threshold; and
 - ✓ at least one of the aggregated transactions was a teller transaction.

NOTE: If even one of the transactors is “known”, a separate Part 1 page is completed on the known transactor, and the filing institution would not check Box 24e, due to the fact that it did identify at least one of the transactors.

(NOTE: By definition, one cannot check Box 24e without also checking Line 3 on the Part 1 page. One can however check Line 3 on the Part 1 page, without checking Box 24e);

Line 24f – Shared Branching is a new option in Line 24 of Form 112 and is checked if the transaction was conducted on behalf of another financial institution that is a member of a co-operative network (this option only applies to Credit Unions that are members of a cooperative).

- g. Line 4 (Above) – “Check if Entity” – Do NOT check the box “if Entity” if the person involved in the report is a sole proprietorship.
- h. Line 8 – Alternate Name – maps to the DBA Box 5 on Form 104. (No acronyms are inserted, just the name);
- i. Line 14 – Country Code – keyed each time on Form 112 – no longer U.S. default;
- j. Line 21 – On the updated CTR (Version 1.3), the instructions for the account number inserted now read “Record the account number or other unique account identifier for each account involved.
- k. Part 3 – Multiple Part 3s on Form 112 could be utilized depending on the number of branch offices involved in the currency transaction being reported;
- l. SAVE – Filers should save a copy of the CTR to their own systems as the BSA E-Filing System is a record retrieval system, but not for the submitting DFI. “A filer should not save a copy of the report on a public computer or a computer that is not regularly accessed by the filer. This will ensure that the file remains appropriately secured”;
- m. 15-Days – The filing deadline for Form 112 is 15 days (the 25-day courtesy filing timeframe for electronic filing was eliminated 04/01/13); and
- n. Addresses and Identifying numbers are keyed as single-strings of data with no hyphens or spaces.
- o. Critical (*) versus Non-Critical Fields – FinCEN expects financial institutions to have the capability to submit information for any of the data fields in the FinCEN CTR or SAR (or any other FinCEN report). In general, if your financial institution’s filing software does not permit the institution to include information in a field without an asterisk where information has been collected and is pertinent to the report, the financial institution should instead complete a discrete filing for those transactions until the software is updated. If a filing has been submitted in which such information was not included because of such a limitation in the filing software, an amended filing should be completed using either the discrete filing method or an amended batch filing, once the software is updated.

Such software updates should be implemented within a reasonable period of time.

- p. Purchase of Monetary Instruments - If a customer purchases a monetary instrument using \$15,000 in currency that the customer first deposits into the customer's account, whether at the requirement of the bank or at the customer's discretion, the financial institution would complete Part I of the FinCEN CTR with the customer's information. In Part II Item 25, the financial institution would indicate \$15,000 as cash in for Item 25d "Purchase of negotiable instrument(s)". Completing the FinCEN CTR in this manner will notify law enforcement that the currency was used to purchase a negotiable instrument.
- q. RSSD Numbers (Items 54 and 40) – When the transaction takes place at a branch location, you should include the RSSD number associated with that branch. If the branch location at which the transaction occurred does not have an RSSD number, however, leave all of Item 40 blank. This may occur if an RSSD number has not yet been issued for a new branch, but FinCEN expects few depository institutions to not have an RSSD for each branch. If the branch has the same RSSD number as the financial institution as a whole, you should use the overall financial institution RSSD number. This will occur with credit unions.

In Box 54, insert the number of the main office described in Part IV.

Please note that it is important to have the information within the filing regarding the branch or other location at which the transaction took place as complete and accurate as possible. This greatly assists law enforcement in understanding where the transactions took place. RSSD numbers are available at: www.ffiec.gov/nicpubweb/content/help/HelpBranchLocatorSearch.htm;

- C. **Relationship to Suspicious Activity Report (SAR)** – If a currency transaction (or a series of transactions) exceeds \$10,000 and is suspicious, both a CTR and a SAR must be filed. If a currency transaction (or a series of transactions) is suspicious but does not exceed \$10,000, only a SAR is filed.
- D. **NOTE:** On 04/03/2020, FinCEN suspended the implementation of FIN – 2020 – R001 for an "indefinite period of time".

FinCEN Ruling 2020-R001 (Reporting of Certain Currency Transactions for Sole Proprietorships and Legal Entities Operating Under a "Doing Business As" (DBA) Name (02/10/2020)), replaced and rescinded two previous rulings: 2016-R003 and 2008-R001, and clarifies the requirements of financial institutions reporting on currency transactions involving sole proprietorships and legal entities operating under a DBA name when filing the current CTR form. A sole proprietorship is a business in which one person, operating in his or her own personal capacity, owns all the business's assets and is responsible for all the business's liabilities. (A sole proprietorship is not a separate legal person from its individual owner). When FinCEN Form 112 is prepared on transactions involving a sole proprietorship, a single Part 1 page will be completed with the individual owner's name, gender, and date of birth. If the individual owner is doing business

in his or her own name, then the rest of the Part 1 page will be completed reflecting the individual owner's information. If the individual owner is operating the business under a different name (E.g. DBA name), then such name should appear in Item 8 (Alternate Name), and the rest of the Part 1 page (other than name, gender and DOB) completed with reference to the DBA name. If the individual owner operates under multiple DBAs, then a separate Part 1 Section should be completed for each different DBA involved in the transactions. The amount and account number(s) will be the amount and account numbers associated with the specific location(s) corresponding to the reported transaction.

When a CTR is prepared on a legal entity, such as an incorporated business, partnership, or limited liability company, a Part 1 section should be prepared containing the home office/headquarters data (address, telephone number, identification number, etc.) of the entity. When multiple entity locations are involved in an aggregated CTR, a separate Part 1 section should be prepared for each location involved. Each additional Part 1 section should include the Entity's legal name (in Item 4) and alternate name, if any, in Item 8. Each additional Part 1 section will include the location's address along with all other location or entity data applicable to that location. The amount and account number(s) will be the amount and account number(s) associated with the specific location. The initial Part 1 section on the entity home office/headquarters will show the total amount and all account numbers involved in Item 21 or 22. When there are multiple DBA names involved in the transaction, Item 8 "Alternate Name" should be left blank in the entity home office Part 1 section. When the entity home office address is the same as the transaction location, only a home office Part 1 section should be prepared.

NOTE: On 04/03/2020, FinCEN suspended the implementation of FIN – 2020 – R001 for an "indefinite period of time".

Until FinCEN implements 2020-R001, for reportable transactions on Sole Proprietors and Legal Entities Operating under a DBA Name, financial institutions should continue to follow the guidance found in 2008-R001 (01/25/2008). That Guidance reads "when filing a CTR on a sole proprietorship, financial institutions are required to complete one Part 1 page, containing the name of the sole proprietorship's owner, the sole proprietorship's DBA name, the sole owner's social security number ("SSN"), the sole owner's home address, the sole owner's date of birth, and the sole owner's occupation. Only one Part 1 page is required, even if the business operations have a different address and/or tax identification number (TIN) than its human owner. 2008-R001 replaced FinCEN Ruling 2006-R003 which had required financial institutions to complete two Part 1 pages containing information on the sole proprietorship, and on the sole proprietor themselves in his or her individual capacity. To accommodate those institutions who wish to continue filing in accordance with 2006-R003, FinCEN will continue to accept CTRs completed with two Part 1 pages when the reported transactions involve a sole proprietorship and/or when filing a CTR on a legal entity operating under a DBA name.

- E. FinCEN Ruling 2006-R-004 (Corporate Credit Unions' Currency Transaction Reporting Requirement)** states that FinCEN views a Corporate Credit Union as a "bank" for BSA definitional purposes. Anytime two "banks" transfer or exchange currency between themselves, and the amount of the transfer exceeds \$10,000, both institutions must file a CTR, unless they have both utilized the exemption process and exempted each other from reporting these currency transfers or exchanges.

- F. CTR Brochure** – On 02/24/09, FinCEN released a new informational/educational brochure titled “*Notice to Customers: A CTR Reference Guide*” that MAY be used by financial institutions as a resource to address CTR questions frequently asked by their clients. The pamphlet explains that large currency transactions are not illegal, and explains that if the client attempts to “structure” their currency transactions, there could be potential civil and criminal consequences. On 11/24/2009, FinCEN issued a Spanish language version of the CTR reference guide. The brochures are available at www.fincen.gov.
- G. FinCEN Ruling 2013 – R001 (Treatment of Armored Car Service Transactions Conducted on Behalf of Financial Institution Customers or Third Parties for Currency Transaction Reporting Purposes) dated July 12, 2013**, supersedes FIN- 2009-R002, and provides an exception in the reporting of currency transactions conducted by an Armored Car Service (ACS) to debit or credit the account of a financial institution’s customer pursuant to instructions received from the customer or from a third-party. To take advantage of this exception, the depository financial institution (DFI) is required to determine whether the ACS is acting pursuant to instructions received from the financial institution, the financial institution’s customer, or from a third party.

If the delivery to or pick-up from the DFI performed by the ACS was pursuant to instructions from the DFI, the DFI’s customer is identified on the Part 1 Page, and Box 24 – Armored Car is checked on the Part 2 Page of FinCEN Form 112. If on the other hand, the delivery to or pick up from the DFI performed by the ACS was pursuant to instructions received from either the business customer or a third party, then the DFI’s customer is identified on the Part 1 Page – Box 2c, and the corporate information of the ACS (corporate name, corporate address, EIN, etc.) is identified on a second Part 1 Page – Box 2d. (The name of the employee of the ACS is not required).

If the DFI has knowledge that the same ACS makes several deliveries or pick-ups below \$10,000 to or from the account of the same customer on any one business day for a total exceeding \$10,000, the transactions will be aggregated for purposes of filing a CTR with respect to that customer. The DFI’s reporting obligation regarding transactions conducted by an ACS pursuant to instructions from the DFI’s customer or third party is satisfied by filing CTRs aggregated by customer only. FIN-2013-R001 does not affect the DFI’s responsibility to file suspicious activity reports when applicable.

- H. FinCEN Guidance 2012-G001 (Currency Transaction Report Aggregation for Businesses with Common Ownership dated 03/16/12)** “clarified” the aggregation of multiple transactions conducted by businesses with common ownership for CTR reporting purposes. Although multiple businesses may share a common owner, the presumption is that separately incorporated entities are independent persons. Therefore, the currency transactions of separately incorporated businesses should not automatically be aggregated as being on behalf of any one person simply because those businesses are owned by the same person. (In FinCEN’s mind however) the presumption that the entities are separate, however, is rebuttable. It is ultimately up to a financial institution to determine, based on information obtained in the ordinary course of business, whether multiple businesses that share a common owner are, in fact, being operated independently, which depends on all the facts and circumstances of each business entity. The results of this determination affect whether the businesses’

currency transactions should be aggregated for purposes of complying with currency transaction reporting obligations

When determining whether to aggregate transactions as being on behalf of the same person, a financial institution must use its knowledge of relevant facts and circumstances. There are no universal rules applicable to any situation. Once a financial institution determines that the businesses are independent, then it should not aggregate the separate transactions of these businesses. Alternatively, once a financial institution determines that the businesses are not independent of each other or their common owner (E.g. the businesses are staffed by the same employees and are located at the same address; the bank accounts of one business are repeatedly used to pay the expenses of another business or the businesses are covering each other's overdrafts or the businesses are guaranteeing each other's loans; or the business accounts are repeatedly used to pay the personal expenses of the owner, et al) then the currency transactions of these businesses should be aggregated going forward for CTR reporting purposes.

The above does not impact the standing requirement that multiple currency transactions conducted by the same person on the same business day which aggregate > \$10,000 must be reported on the CTR, regardless of the common ownership question.

I. Exam Procedures - Contained within the current Interagency BSA/AML Examination Manual are the Core Examination procedures covering an institution's currency transaction reporting program. Highly qualitative and subjective in nature, the Federal examiner will form a conclusion about the ability of policies, procedures, and processes to adequately address the preparation, filing, and retention of CTRs by completing a number of reviews which include, but are not limited to:

1. Reviewing correspondence from FinCEN's BSA E-Filing System relating to incorrect or incomplete CTRs;
2. Reviewing the currency transaction "system" to determine if, and how the financial institution aggregates currency transactions within the institution;
3. Validating that the institution's independent testing confirms the integrity and accuracy of the management information systems used for aggregating currency transactions;
4. Determining if discrepancies exist between the institution's records of CTRs filed and the CTRs reflected in the data download obtained from the BSA reporting database.

III. EXEMPTIONS – Many customers engaged in legitimate business activities may conduct currency transactions exceeding the \$10,000 reporting threshold, e.g., restaurants, grocery stores, and other retail merchants. Reports about these customers' transactions are of little or no use to law enforcement since they reflect legitimate activities. To reduce the burden on banks and the CTR database, Congress enacted an exemption process whereby certain customers may be exempted from currency transaction reporting.

NOTE: Exempting a customer from currency transaction reporting is a voluntary process. If a bank chooses to exempt a customer, it must follow the relevant exemption process

for that type of customer, and follow the relevant operating rules for the customer to remain exempt. Additionally, designating a customer as exempt only eliminates the requirement to file CTRs regarding that customer's currency transactions; it does not alter the obligation to file a Suspicious Activity Report (SAR) with respect to any suspicious transactions conducted by the exempt customer.

A. Banks and Government Entities

1. Banks and government entities are eligible for exemption. This includes:
 - a. Banks (i.e., banks, savings and loan associations, and credit unions), to the extent of the bank's domestic (i.e., United States) operations;

NOTE: Transfers of funds to and from any of the twelve Federal Reserve Banks are automatically exempt.
 - b. A department or agency of the United States, any State, or any political subdivision of any State; and
 - c. Any entity established under the laws of the United States, or any State, or of any political subdivision of any State, or under any interstate compact between two or more States, that exercises governmental authority on behalf of the United States or any such State or political subdivision.
 - (1) An entity generally exercises governmental authority only if its authority includes the power to tax, exercise eminent domain, or exercise police powers. The New Jersey Turnpike Authority and the Port Authority of New York and New Jersey are examples of entities that exercise governmental authority.
 - (2) A bank may treat a person as a governmental department, agency or entity if the name of the person or general community knowledge indicates such status. The term "United States" includes both the District of Columbia as well as the Tribal Lands. Therefore, Tribal Governments are eligible to be exempt persons. (Whether gaming operations conducted on Tribal Lands are exemptible depends on the manner in which such operation is organized and operated.)
2. In order to be exempted, depository institutions no longer have to file an initial FinCEN Form 110 in order to designate banks and government entities as exempt (Effective 01/05/09). However, depository institutions should take the same steps to assure themselves of the customer's initial eligibility for exemption, and document the basis of its conclusions, that a reasonable and prudent bank would take to protect itself from loan or other fraud or loss based on misidentification of a person's exempt status. (If a bank is able to determine a customer's eligibility for an exemption in the course of complying with its other BSA obligations (E.g. CIP), then the bank may make notations within its other BSA documentation, and need not maintain additional, separate documentation for the sole purpose of complying with these exemption requirements.)

3. After a bank or government entity customer has been exempted, that customer's continued eligibility for exemption no longer must be reviewed and documented on an annual basis (Effective 01/05/09). However, depository institutions MUST still comply with their SAR reporting obligations should any of their exempted customers engage in suspicious activity.
4. Once a bank or government entity customer has been designated as exempt, the bank is not required to file a CTR regarding any currency transactions (e.g., deposits, withdrawals, currency exchanges, purchases of cashier's checks or certificates of deposit, etc.) conducted by the exempt bank or government entity.

B. Listed Businesses – Certain businesses (and their subsidiaries) that are listed on certain stock exchanges may be exempted from currency transaction reporting requirements.

1. Any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (except stock or interests listed under the separate "NASDAQ Capital Market Companies" heading), provided that a person that is a financial institution other than a bank is an exempt person only to the extent of its domestic operations.
 - a. To determine whether the entity is a listed business, a bank may rely on any New York, American, or NASDAQ Stock Market listing published in a newspaper of general circulation, on any commonly accepted or published stock symbol guide, on any information contained in the Securities and Exchange Commission "Edgar" System, or on any information contained on an Internet site or sites maintained by the New York Stock Exchange, the American Stock Exchange, or the NASDAQ.
 - b. The status of a listed business as exempt ceases once the entity is no longer listed on the applicable stock exchange.
2. Any U.S. subsidiary of a listed business whose common stock is majority owned (at least 51%) by a listed business.
 - a. To determine whether an entity is a subsidiary of a listed business, a bank may rely on an authenticated corporate officer's certificate, an authenticated copy of IRS Form 851 (Affiliation Schedule), or an Annual Report or Form 10-K as filed with the SEC.
 - b. A subsidiary's status as exempt ceases once the subsidiary is no longer majority owned (at least 51%) by a listed business.

3. In order to be exempted, listed businesses or subsidiaries of listed businesses must be designated as exempt with the Treasury Department, using FinCEN Form 110 – Designation of Exempt Person Form. After the listed business or subsidiary of a listed business has been designated:

- a. The customer's continued eligibility must be reviewed annually. Absent specific knowledge that would be grounds for immediate revocation, a bank is required to verify the status of designated exempt persons only once each year.

EXAMPLE: If you become aware that the business is no longer listed on the relevant stock exchange, you may not continue to treat that customer as exempt. But without such specific knowledge, you need only confirm the business is still listed on an annual basis.

- b. The bank must monitor the customer relationship for suspicious transactions, and report any such transactions through a SAR. (For example, a sharp increase from one year to the next in the gross total currency transactions made by an exempt customer, or similar irregular transaction trends or patterns, may trigger the obligation to file a SAR.)

NOTE: This requirement to monitor the customer relationship for suspicious transactions does not eliminate nor reduce the bank's responsibility to report detected or suspected suspicious activity involving any person, regardless of whether that person or customer has been designated as exempt from currency transaction reporting.

4. Once a listed business/subsidiary customer has been designated as exempt, the bank is not required to file a CTR regarding any currency transactions (e.g., deposits, withdrawals, currency exchanges, purchases of cashier's checks or certificates of deposit, etc.) conducted by the exempt business.

C. Non-Listed Businesses – Commercial enterprises (including nonprofit entities) that are not listed on the major stock exchanges can also be exempted, but only as to currency transactions to or from an exemptible account, and only if certain conditions are met.

1. To be eligible for exemption, a non-listed business must meet all of the following requirements:

- a. Has maintained a transaction account at the bank for at least two months (Effective 01/05/09).

NOTE: A bank may designate a non-listed business as an exempt person before the customer has maintained a transaction account at the bank for at least two months if the bank conducts and documents a risk-based assessment of the customer, and forms a reasonable belief that the customer has a legitimate business purpose for conducting frequent transactions in currency.

- b. Frequently engages in currency transactions greater than \$10,000. In general, the customer should demonstrate a recurring or routine need to engage in at least five (Effective 01/05/09) of these large currency transactions throughout the year.

NOTE: In determining the qualification of a customer as an exempt person, a bank may treat all exemptible accounts (transaction and Money Market Deposit Accounts) of the customer as a single account. If a bank elects to treat all transaction accounts of a customer as a single account, the bank must continue to treat such accounts consistently as a single account for purposes of determining the qualification of the customer as an exempt person.

- c. Be incorporated or organized under the laws of the United States or a State, or be registered as and eligible to do business in the United States or a State.
- d. Not engage primarily in one or more of the following ineligible activities (a business that engages in multiple business activities may be exempted as long as no more than 50% of its gross revenues are derived from the following ineligible activities):

- (1) Serving as a financial institution or agent of a financial institution;

NOTE: Since Money Service Businesses (MSBs), i.e., persons or businesses (other than banks) that cash checks, exchange currency, or who issue, sell or redeem traveler's checks, money orders or stored value cards in amounts greater than \$1000 per person per day, or who transmit currency through a financial institution, qualify as financial institutions, customers who are MSBs may not be exempted, unless they meet the "50% test" referenced above.

- (2) Purchase or sale to customers of motor vehicles, vessels, aircraft, farm equipment or mobile homes;
- (3) The practice of law, accountancy, or medicine;
- (4) Investment advisory or investment banking services;
- (5) Real estate brokerage;
- (6) Pawn brokerage;
- (7) Title insurance and real estate closings;
- (8) Chartering or operation of ships, buses or aircraft;
- (9) Auctioning of goods;
- (10) Gaming of any kind (other than licensed pari-mutual betting at racetracks);

- (11) Trade union activities; or
- (12) Any other activities that may be specified by FinCEN, including, and such as, Marijuana-Related Businesses.

NOTE: FinCEN Guidance 2009-G001 (Guidance on Supporting Information Suitable for Determining the Portion of a Business Customer's Annual Gross Revenues that is Derived from Activities Ineligible for Exemption from Currency Transaction Reporting Requirements – April 27, 2009) assists financial institutions in determining the appropriateness of exempting from currency transaction reporting requirements, those non-listed business clients that derive some portion of their annual gross revenues from ineligible business activities.

- 2. A non-listed business can only be exempted to the extent of its domestic (i.e., United States) operations.
- 3. A sole proprietorship may be exempted as a non-listed business, as long as it otherwise meets the above requirements. Only commercial accounts of sole proprietors are eligible for exemption; personal accounts of the individual cannot be exempted. However, banks are not required to track commingled funds.
- 4. A non-listed business can only be exempted as to deposits to and withdrawals from an exemptible account.
 - a. An “exemptible account” means a transaction account as described in Section 19(b)(1)(C) of the Federal Reserve Act [12 USC 461(b)(1)(C)], i.e., a checking, share draft, or Negotiable Order of Withdrawal (NOW) account.
 - b. An “exemptible account” also includes a Money Market Deposit Account (MMDA), even though it is a type of savings account, that is used in connection with the business, provided the customer also maintains a transaction account with the bank.
- 5. In order to treat a non-listed business as exempt, the bank must:
 - a. Document the conclusion that the customer is eligible for exemption as a non-listed business. This conclusion must be based on proper identification of the customer, taking the steps that a reasonable and prudent bank would take to protect itself from fraud or loss based on misidentification of a person's status. This documentation must be retained for a period of five years.
 - b. Designate the customer as exempt with the Treasury Department by filing FinCEN Form 110.
 - c. Establish and maintain a monitoring system that is reasonably designed to detect suspicious transactions for each account of the exempt customer. (For example, a sharp increase from one year to the next in the gross total currency transactions made by an

exempt customer, or similar irregular transaction trends or patterns, may trigger the obligation to file a SAR.)

NOTE: This requirement to monitor the accounts of the exempt customer for suspicious transactions does not eliminate nor reduce the bank's responsibility to report detected or suspected suspicious activity involving any person, regardless of whether that person or customer has been designated as exempt from currency transaction reporting.

- d. Review and verify the information supporting the customer's exempt status, and the monitoring system designed to detect any suspicious transactions, at least annually.

NOTE: The requirement to renew the customer's designation as exempt with the Treasury Department on a biennial (i.e., once every two years) basis was eliminated effective January 5, 2009.

D. Payroll Customers – Businesses that pay their employees in cash and regularly make cash withdrawals for that purpose may be exempted as payroll customers; however, the exemption relates only to withdrawals from an exemptible account for payroll purposes.

1. Any commercial enterprise (including nonprofit entities), regardless of its primary business activity, may be exempted as a payroll customer, provided it meets all of the following requirements:

- a. Has maintained a transaction account at the bank for at least two months (Effective 01/05/09).

NOTE: A bank may designate a payroll customer as an exempt person before the customer has maintained a transaction account at the bank for at least two months if the bank conducts and documents a risk-based assessment of the customer, and forms a reasonable belief that the customer has a legitimate business purpose for conducting frequent transactions in currency.

- b. Frequently withdraws more than \$ 10,000 in currency in order to pay its United States employees' wages in currency. Frequently is now (Effective 06/07/12) defined as having conducted at least five or more reportable cash transactions within a year.

NOTE: In determining the qualification of a customer as an exempt person, a bank may treat all exemptible accounts (transaction and Money Market Deposit Accounts) of the customer as a single account. If a bank elects to treat all transaction accounts of a customer as a single account, the bank must continue to treat such accounts consistently as a single account for purposes of determining the qualification of the customer as an exempt person.

- c. Is incorporated or organized under the laws of the United States or a State, or is registered as and eligible to do business in the United States or a State.

2. A sole proprietorship may be exempted as a payroll customer, as long as it otherwise meets the above requirements. Only commercial accounts of sole proprietors are eligible for exemption; personal accounts of the individual cannot be exempted. However, banks are not required to track commingled funds.
3. A payroll customer can only be exempted as to withdrawals from an exemptible account for payroll purposes.
 - a. An “exemptible account” means a transaction account as described in Section 19(b)(1)(C) of the Federal Reserve Act [12 USC 461(b)(1)(C)], i.e., a checking, share draft, or Negotiable Order of Withdrawal (NOW) account.
 - b. An “exemptible account” also includes a Money Market Deposit Account (MMDA), even though it is a type of savings account, that is used in connection with the business, provided the customer also maintains a transaction account with the bank.
4. In order to treat a payroll customer as exempt, the bank must:
 - a. Document the conclusion that the customer is eligible for exemption as a payroll customer. This conclusion must be based on proper identification of the customer, taking the steps that a reasonable and prudent bank would take to protect itself from fraud or loss based on misidentification of a person’s status. This documentation must be retained for a period of five years.
 - b. Designate the customer as exempt with the Treasury Department by filing FinCEN Form 110.
 - c. Establish and maintain a monitoring system that is reasonably designed to detect suspicious transactions for each account of the exempt customer. (For example, a sharp increase from one year to the next in the gross total currency transactions made by an exempt customer, or similar irregular transaction trends or patterns, may trigger the obligation to file a SAR.)

NOTE: This requirement to monitor the accounts of the exempt customer for suspicious transactions does not eliminate nor reduce the bank’s responsibility to report detected or suspected suspicious activity involving any person, regardless of whether that person or customer has been designated as exempt from currency transaction reporting.
 - d. Review and verify the information supporting the customer’s exempt status, and the monitoring system designed to detect any suspicious transactions, at least annually.

NOTE: The requirement to renew the customer’s designation as exempt with the Treasury Department on a biennial (i.e., once every two years) basis was eliminated effective January 5, 2009.

E. Designation of Exemption

1. In order to treat a listed business, non-listed business, or payroll customer as exempt, the bank must so designate that customer by filing FinCEN Form 110, *Designation of Exempt Person*, with the Treasury Department. (Banks and government entities are excluded from this designation requirement effective January 5, 2009).
 - a. The designation must be filed with the Treasury Department by the close of the 30-day period beginning after the day of the first reportable transaction sought to be exempted.

EXAMPLE: A customer eligible for exemption conducts a reportable transaction on May 1. As long as a designation form is filed with the Treasury Department by May 31, no CTR is required regarding that transaction nor any subsequent transactions (assuming the customer's exempt status does not change).
 - b. A customer may be designated as exempt by all banks that are part of a bank holding company with a single filing. The initial designation may be made by the parent bank holding company, or by one of its bank subsidiaries, on behalf of all bank subsidiaries of the holding company, so long as the designation lists each bank subsidiary to which the designation will apply.
2. When a bank designates a customer as exempt, it must maintain records documenting its compliance with the exemption process, e.g., documentation of the customer's eligibility for exemption, the initial designation of exemption, and the annual review of continued eligibility, where applicable. These records documenting compliance with the exemption process must be retained for five years.

Designation of Exempt Person

[Home](#)[Filing/Exempt Person
Information](#)[Filer
Information](#)

Designation of Exempt Person

OMB No. 1506-0012

Version Number: 1.0

Steps to Submit

1. Complete the report in its entirety with all requested or required data known to the filer.
2. Click "Validate" to ensure proper formatting and that all required fields are completed.
3. Sign with PIN.
4. Click "Save"; filers may also "Print" a paper copy for their records.
5. Click "Submit".

Filing Name

[Save](#)[Validate](#)[Submit](#)[Print](#)

By providing my PIN, I acknowledge that I am electronically signing the BSA report submitted.

[Sign with PIN](#)

This PDF is intended for testing purpose only. Please do not use it in a production environment.

Designation of Exempt Person

Home

Filing/Exempt Person
Information

Filer
Information

Part I Filing Information

*1 Indicate the type of Filing by checking a,b or c

a ☐ Initial designation

b ☐ Exemption amended

c ☐ Exemption revoked

Document Control Number / BSA Identifier

*2 Effective date of the exemption

Part II Exempt Person Information

Check here ☐ If entity

*3 Individual's last name or entity's
legal name of the exempt person

4 First name

5 Middle name

Suffix

6 Alternate Name

7 Occupation or type of business

7a NAICS Code

*8 Address

*9 City

*10 State

*11 ZIP Code

*12 TIN

*13 TIN type

14 E-mail address

15 Phone number

15a Extension

*16 Type of exempt person, check box a, b, c, or d

a ☐ Listed company

b ☐ Listed company subsidiary

c ☐ Eligible non-listed business

d ☐ Payroll customer

Designation of Exempt Person

[Home](#)[Filing/Exempt Person
Information](#)[Filer
Information](#)

Part III Filer Information

*17 Name of bank	<input type="text"/>		
*18 EIN	<input type="text"/>	19 RSSD	<input type="text"/>
*20 Address	<input type="text"/>		
*21 City	<input type="text"/>		
*22 State	<input type="text"/>	*23 ZIP Code	<input type="text"/>
*24 Bank's primary federal regulator	<input type="text"/>		
25 If this designation is also being made for one or more affiliated banks, check this box <input type="checkbox"/>			

Part IV Signature

I am authorized to sign this form on behalf of the bank granting the exemption and any listed bank subsidiaries. I declare that the information provided is true, correct and complete.

26 Print name	<input type="text"/>		
27 Title	<input type="text"/>		
28 Signature	<input type="text" value="Please return to the Home tab to sign with PIN."/>		<input type="button" value="Back to Home"/>
29 Phone number (include area code)	<input type="text"/>	29a Extension	<input type="text"/>
30 Date of Signature	<input type="text"/> (Date of signature will be auto-populated when the form is signed.)		

F. Limitation of Liability

1. If a bank does not comply with the exemption process for a customer that is eligible for exemption, it must file CTRs regarding reportable transactions involving that customer, and remains subject to all rules regarding the filing of CTRs and the penalties for filing false or incomplete CTRs.
2. If a customer has been properly designated as exempt, and the bank complies with the applicable operating rules regarding that exemption, the bank will not be liable for not filing CTRs involving exempted currency transactions. However, the bank will be liable for currency transaction reporting violations involving an exempted customer if the bank:
 - a. knowingly files false or incomplete information regarding an exempt customer;
 - b. has reason to believe that the customer does not meet the exemption criteria;
 - c. has reason to believe that a currency transaction being treated as exempt is not truly a transaction of the exempt customer; or
 - d. has specific knowledge that an exempted customer no longer meets the exemption criteria, e.g., a non-listed business becomes primarily engaged in an ineligible business activity.

G. Risk-Based Analysis

1. With the exemption program modifications effective 01/05/09, FinCEN is adopting a hybrid approach to the Phase II customers that permits financial institutions to exempt an otherwise eligible Phase II customer after two months of maintaining a transaction account at the bank, or prior to the passing of two months' time, if the institution conducts a risk-based analysis of the customer that allows the institution to form and document a reasonable belief that the customer has a legitimate business purpose for conducting frequent large cash transactions.
2. When the two-month waiting period has not been met, the financial institution has less time to observe the normal pattern of transaction activity that a customer engages in to gain a knowledge of that customer, and as such the financial institution must conduct a risk-based analysis. This analysis will involve a greater level of review of that customer than under the reasonable and prudent standard, depending upon the depository institution's assessment of the risks associated with that customer. Factors that the financial institution might consider in order to form that "reasonable belief" include, but are not limited to:
 - a. Whether the depository institution had a past relationship with the customer;
 - b. Certain specific characteristics of the customer's business model that may be pertinent;
 - c. The types of business in which the customer engages; and

- d. Where the business is operating. (Exempting a returning customer who had previously been exempted by the financial institution under the prior exemption process could be a qualifying candidate for this risk-based analysis.)
3. Nothing in this hybrid approach to Phase II exemptions relieves or reduces the obligations of the SAR requirements.

H. Exam Procedures - Contained within the current Interagency BSA/AML Examination Manual are the Core Examination procedures covering an institution's currency transaction reporting exemption process. Highly qualitative and subjective in nature, the Federal examiner will form a conclusion about the ability of policies, procedures, and processes to adequately address the regulatory requirements associated with currency transaction reporting exemptions by completing a number of reviews which include, but are not limited to:

1. Determining whether the institution files FinCEN Form 110 within 30 days of the first reportable transaction that was exempted for Phase 1 listed businesses and Phase 2 non-listed businesses;
2. Assessing whether ongoing and reasonable due diligence is performed including required annual reviews to determine whether the client remains "exemptible" under the regulatory requirements. (Management should properly document the exemption determinations (E.g. stock quotes from the newspaper, output from the posting system attesting to the five or more currency transactions > \$10,000 during the previous year, et al); and
3. Determining whether the institution maintains documentation to support that the "non-listed businesses" it has designated as exempt from CTR reporting do not receive more than 50 percent of gross revenue from ineligible business activities;

I. FinCEN Guidance – On June 11, 2012 FinCEN issues Guidance 2012-G003 to help DFIs determine whether a client is eligible for exemption from CTR reporting requirements. The Guidance is available at: www.fincen.gov .

	Type of Customer	Transaction Frequency	Waiting Period	Ineligible Activity	File DOEP Report	Annual Review
Phase I	Banks operating in the U.S.	N/A	None	N/A	No	No
	Federal, state, local, or inter-state governmental departments, agencies, or authorities	N/A	None	N/A	No	No
	Entities listed on the major national stock exchanges	N/A	None	N/A	Yes	Yes
	Subsidiaries (at least 51% owned) of entities listed on the major national stock exchanges	N/A	None	N/A	Yes	Yes
Phase II	Non-listed businesses	Five or more transactions per year	Two months; or less after risk-based analysis	No more than 50% of gross revenues derived from ineligible activity	Yes	Yes
	Payroll Customers	Five or more transactions per year	Two months; or less after risk-based analysis	N/A	Yes	Yes

(Blank Page)



Department of the Treasury Financial Crimes Enforcement Network

Guidance

FIN-2012-G001

Issued: March 16, 2012

Subject: Currency Transaction Report Aggregation for Businesses with Common Ownership

The Financial Crimes Enforcement Network ("FinCEN") is issuing this guidance to clarify, for currency transaction reporting purposes, the aggregation of multiple transactions conducted by businesses with common ownership. Subsequent to a ruling on this issue,¹ FinCEN received requests from financial institutions for further guidance. In particular, requestors were interested in guidance that addressed common ownership aggregation beyond the limited set of circumstances discussed in FinCEN Ruling 2001-2. That ruling was specific to an individual who owned three incorporated businesses with separate tax identification numbers and accounts, and who made a practice of using funds from one account to pay for the expenses associated with the other businesses.² FinCEN is supplementing that ruling with the following additional guidance.

Did the Same Person Conduct the Transactions?

FinCEN's regulations implementing the Bank Secrecy Act ("BSA") require financial institutions to aggregate multiple currency transactions "if the financial institution has knowledge that [the multiple transactions] are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 during any one business day."³ Accordingly, the financial institution must file a currency transaction report ("CTR") when it has knowledge that the same person⁴ has conducted multiple transactions that total more than \$10,000 in currency in one business day or when it has knowledge that multiple transactions that total more than \$10,000 in currency in one business day are on behalf of the same person.

¹ FinCEN Ruling 2001-2, *Currency Transaction Reporting: Aggregation* (Aug. 23, 2001).

² *Id.*

³ 31 CFR § 1010.313 (2011).

⁴ A person that gives or receives currency as a function of its agency relationship with a financial institution is not a transactor for the purposes of the CTR requirements. Instead, the transactor is the individual who gives the currency to or receives the currency from the financial institution's agent. An individual conducting a transaction with the agent of a financial institution is considered to be conducting a transaction directly with the financial institution. If the financial institution receives or provides currency through multiple transactions with the same individual through the financial institution's agent, the financial institution will need to consider the aggregation of the amounts of those transactions for the purpose of complying with CTR requirements. See FIN-1988-R005 ("Knowledge by the Bank's agent [...] that the currency was received in multiple transactions, is attributable to the Bank. The Bank must assure that [...] its agent [...] obtains all the information and identification necessary [for the Bank] to complete [and file] the CTR").

For example, a financial institution is considered to have knowledge that the same person deposited \$11,000 in cash transactions in a single business day if it is aware that the same individual made both a \$5,000 cash deposit into his personal account and, later that same business day, a \$6,000 cash deposit into his employer's business account. Accordingly, the financial institution is required to file a CTR. Specifically, the financial institution is expected to complete two sections identifying the persons on whose behalf the transactions were conducted. The remaining parts of the CTR should be filled out according to the form instructions.

On Whose Behalf Were the Transactions Conducted?

Although multiple businesses may share a common owner, the presumption is that separately incorporated entities are independent persons.⁵ Therefore, the currency transactions of separately incorporated businesses should not automatically be aggregated as being on behalf of any one person simply because those businesses are owned by the same person. The presumption that the entities are separate, however, is rebuttable. It is ultimately up to a financial institution to determine, based on information obtained in the ordinary course of business, whether multiple businesses that share a common owner are, in fact, being operated independently depending on all the facts and circumstances. The results of this determination affect whether the businesses' currency transactions should be aggregated for purposes of complying with currency transaction reporting obligations.

If a financial institution determines that these businesses (or one or more of the businesses and the private accounts of the owner) are not operating separately or independently of one another or their common owner – *e.g.*, the businesses are staffed by the same employees and are located at the same address, the bank accounts of one business are repeatedly used to pay the expenses of another business, or the business bank accounts are repeatedly used to pay the personal expenses of the owner – the financial institution may determine that aggregating the businesses' transactions is appropriate because the transactions were made on behalf of a single person.

When determining whether to aggregate transactions as being on behalf of the same person, a financial institution must use its knowledge of relevant facts and circumstances. There are no universal rules applicable to any situation.⁶ Once a financial institution determines that the businesses are independent, then it should not aggregate the separate transactions of these businesses. Alternatively, once a financial institution determines that the businesses are not independent of each other or their common owner, then the transactions of these businesses should be aggregated going forward.

For example, a bank knows that Company A and Company B have the same owner, operate out of the same address, and continually commingle funds between their separate accounts. Because of this information, the bank has determined that Company A and Company B are not independent of each other. One day, an employee of Company A deposits \$6,000 into the

⁵ See 18 Am. Jur. 2d *Corporations* § 2 (“A corporation is a legal entity with an identity or personality separate and distinct from that of its owners or shareholders and must be thought of without reference to the members who compose it”).

⁶ See *e.g.* FinCEN Ruling 2001-2, *Currency Transaction Reporting: Aggregation* (Aug. 23, 2001).

account of Company A. That same business day, an employee of Company B deposits \$5,000 into the account of Company B. Because the bank has determined that the businesses are not independent of each other, the bank should file a CTR listing Company A and Company B in separate sections indentifying the person(s) on whose behalf the transaction is conducted and listing a cash-in deposit of \$11,000. The remaining sections of the CTR should be filled out according to the form instructions.

* * * * *

Financial institutions with questions about this guidance or other matters related to compliance with the Bank Secrecy Act and its implementing regulations may contact FinCEN's regulatory helpline at (800) 949-2732.



Department of the Treasury Financial Crimes Enforcement Network

Guidance

FIN-2012-G003

Issued: June 11, 2012

**Subject: Guidance on Determining Eligibility for Exemption from
Currency Transaction Reporting Requirements**

This document revises the guidance originally published on August 31, 2009, to implement the following changes:

- Relevant citations have been updated to reflect the final rule transferring FinCEN's regulations from 31 CFR § 103 to 31 C.F.R. Chapter X, effective March 1, 2011, and as published at 75 FR 65806;
- The portion of the guidance dealing with exemption eligibility for payroll customers has been amended in accordance with the final rule amending 31 C.F.R. § 1020.315, published at 77 FR 33638 on June 7, 2012.

I. Background:

The Financial Crimes Enforcement Network ("FinCEN") is issuing this guidance to help banks¹ determine whether a customer is eligible for exemption from currency transaction reporting requirements.² This guidance provides examples and answers to commonly asked questions regarding the final rules³ that FinCEN issued in December, 2008 and June, 2012, which amended the currency transaction report ("CTR") exemption requirements ("the final rules").

¹ Pursuant to the Bank Secrecy Act, the term "bank" includes *inter alia* each agent, agency, branch, or office within the United States of any person doing business as a commercial bank, a savings and loan association, a thrift institution, a credit union, or a foreign bank, 31 C.F.R. § 1010.100(d).

² FinCEN consulted with the staffs of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency prior to issuing this guidance.

³ See 73 FR 74010 and 77 FR 33638, respectively.

The Bank Secrecy Act and its implementing regulations require financial institutions to file a CTR on any transaction in currency of more than \$10,000.⁴ The regulations in the Bank Secrecy Act also provide banks with the ability to exempt certain customers from currency transaction reporting.⁵

A. 2008 GAO Report

In 2008, the Government Accountability Office (“GAO”) issued a report⁶ concluding, among other things, that the information provided on CTRs provides unique and reliable information essential to a variety of efforts, including law enforcement investigations, regulatory and counter-terrorism matters. In this same report, the GAO recommended several changes to the exemption requirements, which FinCEN addressed in the final rules. The GAO also concluded that additional web-based guidance was necessary to help banks determine eligibility for exemption, which FinCEN is addressing in this guidance document.

B. The Final Rules – CTR Exemption Changes

Overview of the requirements of the final rules:

The final rules, which went into effect on January 5, 2009 and June 7, 2012, make the following substantive changes to the previous CTR exemption system:

- Elimination of designation and annual review for most Phase I customers.⁷ Banks are no longer required to file a designation of exempt person (“DOEP”) report for, or conduct an annual review of, customers who are other depository institutions operating in the United States, U.S. or State governments, or entities acting with governmental authority. The DOEP filing and annual review are still required for businesses listed on a major national stock exchange (“listed businesses”), non-listed businesses, and payroll customers.
- “Frequently” decreased to five reportable transactions. Banks may designate an otherwise eligible non-listed business customer or payroll customer⁸ for exemption after the customer has within a year conducted five or more reportable transactions in currency (previously, eight or more reportable transactions were required).

⁴ 31 CFR § 1010.310.

⁵ 31 C.F.R. § 1020.315.

⁶ See “Bank Secrecy Act: Increased Use of Exemption Provisions Could Reduce Currency Transaction Reporting While Maintaining Usefulness to Law Enforcement Efforts” GAO-08-355 (GAO: Washington, D.C.: Feb. 21, 2008).

⁷ Entities commonly known as “Phase I” are defined in 31 C.F.R. § 1020.315(b)(1)-(b)(5).

⁸ Entities commonly known as “Phase II” are defined in 31 C.F.R. § 1020.315(b)(6) and (b)(7).

- Waiting time for eligibility decreased. Banks may use a hybrid approach to designate an otherwise eligible customer for a Phase II exemption: The customer may be eligible for exemption after maintaining a transaction account for two months (previously twelve months were required); or, the customer may be eligible for exemption in less than two months if the bank conducts a risk-based analysis to form a reasonable belief that the customer has a legitimate business purpose for conducting frequent or regular large currency transactions.
- Biennial renewals eliminated. Banks are no longer required to file a biennial renewal or record and report a change of control for an exempt Phase II customer.

These final rules, along with the existing requirements established by previous rulemakings, have simplified the exemption process by generally authorizing a bank to treat a customer as exempt from currency transaction reporting under the following circumstances:

	Type of Customer	Transaction Frequency	Waiting Period	Ineligible Activity	File DOEP Report	Annual Review
Phase I	Banks operating in the U.S.	N/A	None	N/A	No	No
	Federal, state, local, or inter-state governmental departments, agencies, or authorities	N/A	None	N/A	No	No
	Entities listed on the major national stock exchanges	N/A	None	N/A	Yes	Yes
	Subsidiaries (at least 51% owned) of entities listed	N/A	None	N/A	Yes	Yes

	on the major national stock exchanges					
Phase II	Non-listed businesses	Five or more transactions per year	Two months; or less after risk-based analysis	No more than 50% of gross revenues derived from ineligible activity	Yes	Yes
	Payroll Customers	Five or more transactions per year	Two months; or less after risk-based analysis	N/A	Yes	Yes

The chart above indicates that for Phase I customers, a bank may immediately treat as exempt any eligible entity without concern for the time it has been a customer of the bank or the number of reportable transactions it has conducted. Additionally, because the “ineligible businesses” provision applies only to non-listed business exemptions, a Phase I customer may be treated as exempt regardless of their involvement in such activities. For all Phase I customers other than listed businesses and their subsidiaries, no DOEP or annual review is required.

Before treating a non-listed business or payroll customer as exempt, a bank must first determine that the customer has conducted five or more transactions within the previous year, has been a customer of the bank for at least two months (or less time on a risk-assessed basis), and, in the case of non-listed businesses, derives no more than 50% of its gross revenues from any ineligible business activity.⁹

Banks must file DOEP reports and conduct annual reviews for all Phase II customers (whether they are non-listed businesses or payroll customers), as well as for listed businesses and their subsidiaries.

⁹ For additional discussion of the “50% rule” relating to ineligible businesses, *see* http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-g001.pdf.

The final CTR exemption rules do not relieve banks of their separate obligation to conduct suspicious activity monitoring and reporting for both Phase I and Phase II exempt customers.¹⁰

II. Frequently asked questions:

Since the publication of the final rules, FinCEN has received questions regarding various provisions. FinCEN is issuing answers to these questions to assist banks in understanding the scope and application of the final rules.

A. Timing

Question: When should a bank make a risk-based determination to exempt an otherwise eligible Phase II customer before they have been a customer for two months?

Answer: The preamble to the 2008 final rule provides some examples of criteria that may be appropriate when making such a risk-based decision. For example, banks could consider the nature of the market the customer serves, the type of services offered, the location of the business, and whether the bank had a past relationship with the customer. In light of such factors, possible examples of customers who may qualify for exemption prior to two months may include the following:

- Returning customers that reopen a previously maintained exempt transaction account with the bank;
- Customers whose exempt status has changed (for example, when a customer that was a publicly listed company privatizes and is otherwise eligible for Phase II exemption).

The above examples are not intended to be exhaustive, but rather representative of the types of customer relationships where a risk-based determination to exempt prior to two months may be appropriate. Readers should note that for each of the examples provided above, there is some factor contributing to a bank's level of knowledge exceeding what is typical for a new customer being considered for exemption. Such knowledge, or other mitigating factors, could assist the bank in forming a reasonable conclusion that the risk of exempting the customer prior to two months was low.

Banks are not required to use the risk-based approach. FinCEN originally proposed¹¹ removing any prescribed amount of time before a bank could consider a Phase II customer for exemption, enabling a bank to make a risk-based determination of when to exempt in all instances. Due to comments submitted in response to that proposal, however, FinCEN implemented a hybrid

¹⁰ See 31 CFR § 1020.320.

¹¹ See 73 FR 22101.

approach that allows banks to choose the flexibility of a risk-based approach or the simplicity of the two-month threshold.

Banks should remember that even if using the two month approach, they are required at least annually to conduct a review of the customer to determine continued eligibility for exemption and to monitor for suspicious activity.

B. Frequency

Question: Using the risk-based approach, can a bank exempt a non-listed business or payroll customer prior to the two month mark even if the customer has conducted fewer than five transactions?

Answer: No. The risk-based approach for determining when to exempt a Phase II customer gives latitude with respect to the timeframe only (i.e., allowing for exemption of customers that have been customers for less than two months). None of the other criteria necessary for Phase II exemption can be adjusted as part of that risk-based approach, including the criteria to for a non-listed business or payroll customer to engage frequently in reportable transactions. Thus, before a bank may exempt a non-listed business or payroll customer, that customer must have conducted at least five reportable transactions. FinCEN believes that without such a frequent large cash transaction volume, a bank could not reasonably expect to have sufficient knowledge of its customer to justify the risk-based approach.

C. Corporate structure and reorganization

Question: What is the status of an exempt customer that previously was a listed public company but has reorganized as a private company?

Answer: If a Phase I customer no longer is a publicly-traded company, the customer is ineligible for a Phase I exemption. However, the bank could evaluate the customer for potential exemption as a non-listed business customer. If the bank's assessment indicates that the private company does not derive more than 50% of its gross revenues from ineligible lines of business,¹² has conducted five or more reportable transactions in the previous year, and otherwise meets all of the exemption criteria, the bank may exempt the company as a non-listed business.

Banks should note that a business's eligibility for exemption under the "listed business" provision may change over time, for example, as it makes an initial public offering or is privatized. This is the primary reason that listed businesses and their subsidiaries are the only

¹² See 31 CFR § 1020.315(e)(8).

Phase I exempt customers under the 2008 final rule for which banks must continue to file DOEP reports and conduct annual reviews. As part of those requirements, banks should have procedures for verifying whether a listed business remains eligible for exemption at least once per year. Annual reports, stock quotes from newspapers, or other information, such as electronic media can be used to document the review.

Question: Does the Phase I exemption available to certain subsidiaries of listed businesses apply to franchises or other affiliated entities when the listed company does not have a 51% or greater ownership stake in the affiliated entity?

Answer: No. To be eligible for exemption, any affiliated entity must meet the definition of “subsidiary” found at 31 C.F.R. § 1020.315(b)(5), which requires that the listed business own at least 51% of the common stock or analogous equity interest of the entity in question. For example, a privately-owned restaurant franchise operating under the corporate name of a listed fast food company would not be eligible for Phase I exemption. A retail business location at least 51% owned by the same listed fast food company and operating under the same corporate name as the franchise, however, would be eligible for Phase I exemption.

Question: What is the exempt status of a Phase II customer who reorganizes his business? For example, what is the recourse for an exempt customer with a doing business as (“DBA”) account who forms a limited liability corporation as his business grows.

Answer: Since the restructuring of a business may cause that business to become ineligible for exemption or otherwise make the original DOEP filing inaccurate or incomplete with respect to the newly restructured business, banks should consider evidence of a business restructuring as part of their annual review or ongoing customer due diligence. Potential evidence of such restructuring could include changes in the customer’s management, business purpose, operations, customers, ownership, or account relationship with the bank. More specifically, changes to a customer’s account relationship with the bank could include the issuance of a new taxpayer identification number,¹³ modifications to the names on the account, changes in account activity, or the addition or removal of signors or controllers of an account.

Banks should use a risk-based approach when determining which factors to consider to ensure that a customer remains eligible for exemption and that the original DOEP filing continues to identify that customer accurately and completely. To the extent that such changes make the original DOEP filing inaccurate or incomplete with respect to the newly restructured business, a

¹³ In some instances, such as the formation of a single member limited liability corporation or certain types of partnerships in some states, a change in corporate structure may not result in the issuance of a new taxpayer identification number.

bank should reevaluate the business for exemption. In such cases, the bank may consider using the risk-based approach for exempting the newly restructured business prior to the two month waiting period. If the restructured business is eligible for exemption and the bank wishes to treat them as such, a new DOEP report must be filed with FinCEN.

In the example used in the question, an unincorporated business that incorporates would likely need reevaluation for the purposes of CTR exemption eligibility.¹⁴ Accordingly, after verifying that the newly restructured business was eligible for exemption, a bank wishing to treat that customer as exempt would need to file a new DOEP report.

D. Ineligible businesses

Question: Does FinCEN consider a hospital or doctors office to be engaged in the practice of medicine and therefore ineligible for exemption as a non-listed business?¹⁵

Answer: FinCEN interprets the term “the practice of medicine” broadly, rather than focusing on the technicalities of individual state laws governing the licensing of medical practitioners. Accordingly, any entity that derives more than 50% of its gross revenues by offering medical services is ineligible for exemption as a non-listed business. This interpretation would likely exclude most privately-owned hospitals, doctors’ offices, or other medical practices from being eligible for exemption as non-listed businesses.

E. Customers no longer eligible for exemption

Question: What should a bank do if, during its annual review of a listed business or Phase II customer, it discovers that the customer no longer meets all the criteria for exemption?

Answer: During the annual review of a Phase II exempt customer, a bank may conclude that a customer is no longer eligible for exemption (for example, if an exempt non-listed business customer conducted only four reportable currency transactions during the year under review). At the time the customer’s ineligibility is discovered, the bank should document its determination of ineligibility and cease to treat the customer as exempt.¹⁶ The bank is not required to back file CTRs with respect to a designated Phase II customer that had met the eligibility requirements in a preceding year, but was subsequently found to be ineligible during the bank’s timely completion of its annual review.

¹⁴ A bank should also consider potential customer identification program obligations under 31 CFR § 1020.220.

¹⁵ The practice of medicine is one of several business activities that make a customer ineligible for exemption as a non-listed business. *See* 31 CFR § 1020.315(e)(8).

¹⁶ In the event the customer meets the eligibility requirements in the future, the bank must file a new DOEP to begin treating the customer as exempt.

F. Suspicious activity of an exempt customer

Question: Is a customer that has been the subject of a Suspicious Activity Report (“SAR”) eligible for initial or continued exemption?

Answer: A Bank is required to file a SAR, where appropriate, regarding the activities of any of its exempt customers.¹⁷ However, if an exempt person is involved in a transaction that has been reported in a SAR, the bank is not required to cease treating the person as exempt. The decision to exempt, or to retain or revoke a customer’s exemption, should be made by the bank in accordance with its risk-based anti-money laundering policies, procedures, and controls.

G. Completing the Designation of Exempt Person report

Question: The DOEP report (FinCEN Form 110) and instructions were not updated with the final rules to account for the various changes to the CTR exemption process. How should a bank complete the DOEP when exempting a new customer?

Answer: The preamble to the 2008 final rule clarified that certain elements of the DOEP report should be disregarded by filers since they are no longer applicable under the new exemption requirements. Because the final rule removed several existing requirements but did not add any new requirements, the DOEP report now contains a limited number of extraneous fields but remains fully sufficient to designate any eligible customer as an exempt person. Accordingly, filers should disregard references on the report as well as in the instructions to biennial renewals and to types of Phase I customers that no longer require a DOEP filing.¹⁸ FinCEN has disabled the unnecessary fields in the E-filing system as well as in the version of FinCEN Form 110 available on its website.

H. Exemptible transaction accounts

Question: The definition of a Phase II “exempt person” in 31 C.F.R. § 1020.315(b)(6) and (7) includes the phrase “only with respect to transactions conducted through its exemptible accounts.” Does this mean that certain transactions of Phase II exempt customers require the filing of a CTR?

Answer: Yes. The scope of the exemption for non-listed businesses and payroll customers is limited by several criteria. While the final rules reduced those criteria with respect to the number

¹⁷ 31 CFR § 1020.320.

¹⁸ See 73 FR 74015, Section V.

of transactions and the waiting period before a bank could treat those customers as exempt, they did not alter the remaining criteria for Phase II customers, including the provision that a Phase II customer is exempt “to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts.”¹⁹ For transactions conducted by the customer outside of the criteria for Phase II customers, the customers would not meet the definition of “exempt person” and could not be treated as exempt by the bank.

For example, a bank may have a convenience store as an exempt non-listed business customer. This customer might regularly make deposits into its transaction account exceeding \$10,000 in currency, none of which would require the bank to file a CTR. However, if the convenience store presents more than \$10,000 in currency in exchange for a cashier’s check, whether the bank is required to file a CTR will depend on whether the transaction was processed “through [the] exemptible account.” Specifically, the bank would not be required to file a CTR if the bank credited the customer’s transaction account as a deposit and then debited the account to fund the cashier’s check, or otherwise processed the transaction in such a way that it resulted in a line item entry into the customer’s transaction account statement. The bank would be required to file a CTR, however, if the currency was deposited into and the cashier’s check was drawn upon the bank’s general ledger account(s), or otherwise did not result in a line item entry into the customer’s transaction account statement.

Banks may generally use the test of whether a transaction results in a line item entry into a Phase II exempt customer’s transaction account statement to determine whether a transaction was “conducted through [the] exemptible account.” For any reportable transaction not conducted through the exemptible account, the customer would not meet the definition of “exempt person” only with respect to that transaction and a CTR must be filed.

I. Revoking an exemption

Question: If a bank ceases to treat a customer as exempt, and begins or intends to begin filing CTRs on that customer for the next reportable transaction, must the bank formally revoke the exemption by filing the DOEP report and selecting the “exemption revoked” box?

Answer: Banks have never been required to formally revoke an exemption using the DOEP report. Generally, examiners or other users of BSA data would be able to rely on a pattern of reporting to know that a customer is no longer being treated as exempt. For purposes of clarity or creating internal documentation, however, many banks voluntarily revoke exemptions using the DOEP report. For example, if during its annual review of an exempt non-listed business customer a bank discovers that the customer conducted no reportable transactions in the previous

¹⁹ See 73 FR 74015, Section V.

year, the bank could no longer treat that customer as exempt. If the exemption is not formally revoked using the DOEP report and the customer continues the pattern of not conducting reportable transactions, a law enforcement agent investigating the company would likely conclude incorrectly from the lack of CTR filings that the customer is still being treated as exempt. While revoking an exemption in such instances may benefit both the filing bank and users of BSA data, banks may choose to do so entirely on a voluntary basis.

* * * * *

Questions or comments regarding the contents of this guidance should be addressed to the FinCEN Regulatory Helpline at 1-800-949-2732.



Department of the Treasury Financial Crimes Enforcement Network

Guidance

FIN-2009-G001

Issued: April 27, 2009

**Subject: Guidance on Supporting Information Suitable
for Determining the Portion of a Business Customer's
Annual Gross Revenues that is Derived from Activities
Ineligible for Exemption from Currency Transaction
Reporting Requirements**

Background

The Financial Crimes Enforcement Network (FinCEN) is issuing this guidance to assist banks¹ in determining the appropriateness of exempting from currency transaction reporting requirements non-listed business customers that derive some portion of their annual gross revenues from ineligible business activities.²

Pursuant to the Bank Secrecy Act, a bank is required to file a Currency Transaction Report for each transaction in currency of more than \$10,000 by, through, or to that bank.³ Additionally, multiple currency transactions totaling more than \$10,000 during any one business day must be treated as a single transaction if the bank has knowledge that they are by or on behalf of the same person.⁴

Nonetheless, a bank may exempt certain customers from currency transaction reporting requirements providing that those customers meet criteria specified in the governing regulation.⁵ For example, a bank may exempt a customer (to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts) that qualifies as a "non-listed business"⁶ – that is, a customer that: (1) has

¹ Pursuant to the Bank Secrecy Act, the term "bank" includes *inter alia* each agent, agency, branch, or office within the United States of any person doing business as a commercial bank, a savings and loan association, a thrift institution, a credit union, or a foreign bank. 31 C.F.R. § 103.11(c).

² FinCEN consulted with the staffs of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision prior to issuing this guidance.

³ 31 C.F.R. § 103.22(b).

⁴ 31 C.F.R. § 103.22(c).

⁵ See 31 C.F.R. § 103.22(d)(2)(i)-(v) ["Phase I" exemption from currency transaction reporting requirements]; 31 C.F.R. § 103.22(d)(2)(vi)-(vii) ["Phase II" exemption].

⁶ 31 C.F.R. § 103(d)(2)(vi).

maintained a transaction account at the bank for at least two months⁷ or upon which the bank has conducted an appropriate risk-based analysis of the legitimacy of the customer's transactions prior to the customer having maintained such a transaction account for two months;⁸ (2) frequently engages in transactions in currency in excess of \$10,000 with the bank;⁹ and (3) is incorporated or organized under the laws of the United States or a State, or is registered as and eligible to do business within the United States or a State.¹⁰

Various businesses (e.g., a business engaged primarily in: serving as a financial institution or as an agent for a financial institution of any type; chartering or operation of ships, aircraft, or buses; operating a real estate brokerage; etc.)¹¹ are ineligible for treatment as exempt non-listed businesses. However, a customer that engages in multiple business activities may qualify for an exemption as a non-listed business provided that no more than 50 percent of its annual gross revenues are derived from one or more ineligible business activities.¹²

Reasonable Determination

Although there is no expectation that a bank will be able to establish the *exact* percentage of a non-listed business customer's annual gross revenues that is derived from ineligible business activities, a bank must consider and maintain materials and other supporting information that allow it to substantiate that the decision to exempt the customer from currency transaction reporting was based upon a *reasonable determination* that the customer derives no more than 50 percent of its annual gross revenues from ineligible business activities.¹³ Such a reasonable determination should be based upon its understanding of the nature of the customer's business, the purpose of the customer's accounts, and the actual or anticipated activity in those accounts.

In instances where it is apparent – through a bank's implementation and application of due diligence policies, procedures, and processes to all customers – that a non-listed

⁷ 31 C.F.R. § 103.22(d)(2)(vi)(A).

⁸ Pursuant to 31 C.F.R. § 103.22(d)(3)(ii)(B), an exempting bank may exempt an otherwise eligible non-listed business customer prior to the passing of two months' time if it conducts and documents a risk-based assessment of the customer that allows it to form a reasonable belief that the customer has a legitimate business purpose for conducting frequent large currency transactions.

⁹ 31 C.F.R. § 103.22(d)(2)(vi)(B). As indicated in the December 5, 2008 final rule amending currency transaction reporting exemption requirements, when interpreting the term "frequently": "[D]epository institutions may designate an otherwise eligible customer for Phase II exemption after the customer has within a year conducted five or more reportable cash transactions." 73 FR 74010, 74014 (Dec. 5, 2008).

¹⁰ 31 C.F.R. § 103.22(d)(2)(vi)(C).

¹¹ 31 C.F.R. § 103.22(d)(5)(viii).

¹² 31 C.F.R. § 103.22(d)(5)(viii); see also FinCEN Advisory, Issue 10 – Reformed CTR Exemption Process: Questions & Answers (Oct. 1998), Question & Answer No. 9: "A business that engages in multiple business activities may be treated as a non-listed business so long as no more than 50% of its gross revenues per year is derived from one or more . . . ineligible business activities . . ."

¹³ 31 C.F.R. § 103.22(d)(5)(i): "[A] bank must take such steps to assure itself that a person is an exempt person . . . to document the basis for its conclusions, and document its compliance, with the terms of [currency transaction reporting exemption requirements], that a reasonable and prudent bank would take and document to protect itself from loan or other fraud or loss based on misidentification of a person's status . . ." See also 31 C.F.R. § 103.22(d)(5)(x).

business customer derives a clear minority of its annual gross revenues from ineligible business activities, the bank could reasonably and appropriately exempt that customer from currency transaction reporting based solely upon materials and information collected and considered in the ordinary course of conducting customer due diligence.

However, in those instances where it is less clear whether a non-listed business customer derives no more than 50 percent of its annual gross revenues from ineligible activities, a bank should obtain such additional supporting materials and information that would allow it to make a reasonable determination that it may appropriately exempt that customer from currency transaction reporting.

In particular, in such cases a bank could reasonably make such a determination based upon customer completion of a bank checklist/form or receipt of a self-certification statement/letter signed by the customer containing credible information regarding its annual gross revenues, which checklist/form or statement/letter would be substantiated by corroborating information.

If available, a bank is encouraged to request and review a business customer's audited financial statements; however, other information may be similarly relied upon providing that it allows the bank to make a reasonable determination regarding the portion of the customer's annual gross revenues that is derived from ineligible business activities.

For example, in many cases a bank could – again, based upon its understanding of the nature of the customer's business, the purpose of the customer's accounts, and the actual or anticipated activity in those accounts – also come to such a reasonable determination based upon reviewing other reliable information, such as: the customer's most recent tax returns that have been filed with the applicable federal and state authorities; the customer's unaudited financial statements; or documents relating to a bank's lending relationship with the customer.

In certain exceptional instances – although there is no requirement to do so – a bank might consider, when deciding to exempt certain business customers, visiting a customer's place of business to develop a greater understanding of the nature of the customer's business activities and then recording relevant information in the customer's file.

The information supporting each designation of an exempt non-listed business customer must be reviewed and verified by a bank at least once per year.¹⁴

¹⁴ 31 C.F.R. § 103.22(d)(4). Additionally, a bank must review and verify at least once each year that management monitors exempt non-listed business customer accounts for suspicious transactions. 31 C.F.R. §§ 103.22(d)(4), (d)(8).

No Effect on Other Regulatory Requirements

Banks are reminded that exempting a customer from currency transaction reporting requirements has no effect on compliance with other Bank Secrecy Act/anti-money laundering programmatic, recordkeeping, and reporting requirements. In particular, banks are reminded of the requirement to implement appropriate risk-based policies, procedures, and processes, including conducting customer due diligence on a risk-assessed basis to aid in the identification of potentially suspicious transactions – and that, if a bank knows, suspects, or has reason to suspect that a transaction involves funds derived from illegal activity or that a customer has otherwise engaged in activities indicative of money laundering, terrorist financing, or other violation of law or regulation, it should file a Suspicious Activity Report.

Attachment B – Error Correction Instructions

This attachment identifies the requirements and procedures for correcting FinCEN CTR errors reported to batch filers during the FinCEN CTR acknowledgement process.

Error Categories:

There are two main categories of errors identified in batch files: Schema validation errors that result in automatic rejection of the batch file and data errors that represent errors in data entered for individual elements but may not result in a rejection. Schema validation errors prevent the batch file from being processed and are considered fatal errors. An example of a schema validation error is a missing required element or an element sequence that does not match the schema. An example of a data error is a required element that contains no value (e.g. a last name element is recorded for the person involved but no last name value is provided for the element and the last name unknown element is not indicated).

Errors that result in the acceptance of the batch file are classified as either primary errors or warning errors. Primary errors are data errors that violate electronic filing requirements or report instructions and so degrade FinCEN CTR data quality that they must be corrected. Primary errors make it difficult for regulators, analysts, and law enforcement investigators to locate the FinCEN CTRs in the database or identify the nature and circumstances of the currency transactions. Examples of such errors include blank last names or legal names, missing financial institution Employer Identification Numbers, or invalid entries in the transaction date field. Refer to Attachment A for a list of elements associated with primary errors.

Warning errors are secondary data errors that violate electronic filing requirements or report instructions but have a lesser impact on FinCEN CTR data quality. Examples of secondary errors are ZIP Codes that end in four zeros (e.g. 123450000), blank or invalid financial institution address information, or invalid telephone numbers.

Correction Requirements:

Filers should immediately correct and resubmit a batch file rejected for fatal format errors. Rejection of a batch file does not relieve the filer of the responsibility to file a FinCEN CTR within 15 days following the day on which the reportable transaction occurred.

When an accepted batch file contains FinCEN CTRs with primary errors, those FinCEN CTRs must be re-filed as corrected reports with the primary errors corrected.

If the accepted batch file contains FinCEN CTRs with both primary and warning errors, they must be re-filed as corrected reports with all errors corrected.

FinCEN CTRs that contain only warning errors need not be re-filed.

FinCEN requires that filers prevent all reported errors in their future filings.

FinCEN recommends that primary error corrections be made no later than 30 days after receiving error notifications. Furthermore, FinCEN recommends that filers remedy any systemic problems in their electronic submissions within 30 days of receiving error notifications. If technical issues prevent filers from implementing corrections within these time frames, filers should notify FinCEN by writing to:

Financial Crimes Enforcement Network
Office of Domestic Liaison
Data Quality Assessments
P.O. Box 39
Vienna, VA 22183

This correspondence should explain the technical issues involved that prevent meeting the time frame, provide an estimate of when the issues will be resolved, and include a contact name and telephone number.

Correction Procedures:

FinCEN CTR batch files are rejected when they contain fatal format errors or when the number of file errors exceeds limits set by the BSA E-Filing Program. In either case, filers must correct all errors identified in the batch file and resubmit the batch file to BSA E-Filing. Because they were not accepted by FinCEN, initial report FinCEN CTRs in the re-submitted batch file are still initial reports. Do not identify FinCEN CTRs from a rejected batch file as corrected reports unless they originally were filed as corrected reports.

If errors in an accepted file involve primary file errors, filers must file corrected reports on all FinCEN CTRs containing primary file errors using the following procedures:

- Make the corrections to both the primary and warning errors in all FinCEN CTRs that contains primary errors.
- Indicate that the FinCEN CTR corrects/amends a prior report under the <ActivityAssociation> element.
- Record the prior report's BSA Identifier from the FinCEN CTR acknowledgement in the <EFilingPriorDocumentNumber> element.
- Ensure that the <FilingDateText> element contains a new date.
- Complete all other data in the FinCEN CTRs in their entirety.
- Retransmit the corrected FinCEN CTR in a new batch file. Do not re-transmit the original batch file because this will cause duplicate database entries on any FinCEN CTRs that were not corrected.

FinCEN monitors FinCEN CTR filings to identify financial institutions that fail to correct primary errors in prior filings or to prevent previously-reported errors of any type in future filings. FinCEN may report such failures to a financial institution's primary federal/state regulator or BSA examiner.



Department of the Treasury Financial Crimes Enforcement Network

Ruling

FIN-2020-R001

Issued: February 10, 2020

Subject: FinCEN CTR (Form 112) Reporting of Certain Currency Transactions for Sole Proprietorships and Legal Entities Operating Under a “Doing Business As” (“DBA”) Name

Effective April 6, 2020,¹ this ruling replaces and rescinds two rulings: FIN-2006-R003 and FIN-2008-R001.² The rescinded rulings were based on the now obsolete FinCEN Form 104. The Financial Crimes Enforcement Network (“FinCEN”) is issuing this administrative ruling to clarify the Currency Transaction Report (“CTR”), FinCEN Form 112 filing obligations when reporting transactions involving sole proprietorships.

In an effort to both enhance regulatory efficiency and provide complete and accurate CTR data to law enforcement, we are clarifying the requirements of financial institutions reporting on currency transactions involving sole proprietorships and legal entities operating under a “doing business as” (“DBA”) name when filing the current CTR FinCEN Form 112.³

Sole Proprietorship

A sole proprietorship is a business in which one person, operating in his or her own personal capacity, owns all of the business’s assets and is responsible for all of the business’s liabilities.⁴ Consistent with the definition of “person” in the Bank Secrecy Act’s implementing regulations,⁵ a sole proprietorship is not a separate legal person from its individual owner. Thus, when a CTR FinCEN Form 112 is prepared on transactions involving a sole proprietorship, a financial institution should complete a single Part I “Person Involved in Transaction” section with the individual owner’s name in Items 4 through 6, gender in Item 7, and date of birth in Item 17.⁶ If

1. The effective date for BSA E-Filing batch filers is September 1, 2020.
2. FIN-2006-R003, Currency Transaction Reports on Sole Proprietorships, Feb. 10, 2006, and FIN-2008-R001, Reporting of Certain Currency Transactions for Sole Proprietorships and Legal Entities Operating Under a “Doing Business As” (“DBA”) Name, Jan. 25, 2008.
3. See 31 CFR § 1010.716(a)(3).
4. Black’s Law Dictionary (11th ed. 2019). The owner of a business who acts alone and has no partners. This definition excludes a single member limited liability company (“LLC”), even one operating under the same tax identification number as its member, because the member operates the LLC in its capacity as a separate legal entity and the LLC, not the member, is responsible for its liabilities.
5. 31 CFR § 1010.100(mm).
6. In states with community property laws that allow a husband and wife to operate an unincorporated business as a sole proprietorship, the sole proprietorship’s proprietor, for purposes of CTR reporting, will be the spouse whose social security number is attached to the sole proprietorship.

the individual owner is doing business in his or her own name, then the rest of Part I should be completed reflecting the individual owner's information. If the individual owner is operating the business under a different name (a "doing business as" or "DBA" name), then such name should appear in Item 8 "Alternate name," and the rest of Part I (other than Items 4-6, 7, and 17 identifying the individual owner) be completed with reference to the DBA name.⁷ If the individual owner operates under multiple DBAs, then a separate Part I section should be completed for each different DBA involved in the transactions. The amount and account number(s) entered in Item 21 "Cash in amount..." or Item 22 "Cash out amount..." will be the amount and account number(s) associated with the specific location corresponding to the reported transaction.

Legal Entity

When a CTR is prepared on a legal entity such as a partnership, incorporated business, or limited liability company, a Part I section should be prepared containing the home office/headquarters data (address, telephone number, identification number, etc.) of the entity. When multiple entity locations are involved in an aggregated CTR, a separate Part I section should be prepared for each location involved. Each additional Part I section should include the entity's legal name in Item 4 and alternate name, if any, in Item 8. Each additional Part I section will include the location's address along with all other location or entity data applicable to that location. The amount and account number(s) entered in Item 21 "Cash in amount..." or Item 22 "Cash out amount..." will be the amount and account number(s) associated with the specific location. The initial Part I section on the entity home office/headquarters will show the total amount and all account numbers involved in Item 21 or 22. When there are multiple DBA names involved in the transaction, Item 8 "Alternate name" should be left blank in the entity home office Part I section. When the entity home office address is the same as the transaction location, only a home office Part I section should be prepared.

7. Enter only one "Alternate name" for item 8. If there are multiple alternate names involved in the transactions, additional Part I's are required to record the additional alternate names.

CURRENCY TRANSACTION REPORTING QUESTIONS

In each of the examples below the first issue is whether a CTR should be filed by the bank and if so, the content of the A and B Sections of Part 1. Other matters which may affect how the CTR is completed should also be addressed if appropriate.

1. A customer deposits \$12,000 in cash to his daughter's accounts: Eleanor receives \$6,000 and Margaret receives \$6,000.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

2. Two employees make \$6,000 cash deposits into the PBS, Inc. account during the same business day.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

3. A customer cashes an official check drawn on another bank in the amount of \$18,000. The transaction was processed as follows: \$10,500 was deposited to a savings account; and \$7,500 in cash was returned to the customer.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

4. \$15,000 is wired to a bank for deposit into a savings account.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

5. Jane Doe, the trustee of the John Smith Trust, makes an \$11,000 cash deposit to the trust account. (What if the transaction is conducted for Jane Doe, the trustee, by her secretary?)

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

6. Husband deposits \$11,000 in cash into joint husband and wife account.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

7. Next day wife withdraws \$11,000 in cash from joint husband and wife account.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

8. Multiple employees of one of bank's business customers come in on payday to cash multiple payroll checks. More than \$10,000 in cash is withdrawn but no single employee receives over \$10,000.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

9. Same facts except one employee brings in several paychecks of co-workers and receives over \$10,000 in cash.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

10. Same employer distributes bonus checks to employees totaling \$50,000 during annual meeting in Las Vegas. Employer also cashes those checks for employees who want to take advantage of the location.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

11. Non-customer cashes a check for \$10,050 and receives \$9,990 after a service fee is deducted.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

12. A customer purchases a cashiers check for \$9,990 and pays a service fee of \$20 for a total of \$10,010 in cash.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

13. Ben Stillman is the owner of Stillman's Liquor, Inc., which has been exempted from CTR reporting as a "non-listed business." On one day he deposits \$11,000 in cash into the business account and \$6,000 in cash into the personal account he owns jointly with his wife Mary.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

14. Same facts as in Question #13, except Mr. Stillman also purchases a cashier's check for \$8,000 in cash made payable to Bluefin Wholesale Liquors for inventory.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

15. Anytown Bank drills open customer's safe deposit box for non-payment of rent. Among other items, the box contains \$11,000 in cash. Anytown mails ex-customer a cashier's check for the balance less the overdue rent.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

16. A minor traffic arrest results in police seizing \$75,000 in cash found within the suspects vehicle. The next day police bring the cash to Anytown Bank to purchase a cashier's check made payable to the Anytown Police Department.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

17. A business customer of Anytown Bank (ABC, Inc.) hires an armored car service to pick up deposits at its three restaurants for delivering to Anytown Bank. The receipts total \$15,000 in cash and are deposited to the ABC, Inc. account.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

18. Mr. Jones owns 100% of three corporations operating liquor stores under separate EINs. The stores make daily cash deposits at Anytown Bank. The managers typically make the deposits and on one day the deposits to Anytown Branch(es) 1, 2, and 3 respectively were \$9,000, \$8,500, and \$8,000 in cash.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

19. Same facts except Mr. Jones picks up deposits at two locations totaling \$18,000 and brings them to Anytown Bank. On the same day, the manager of the remaining store brings in \$8,000 for deposit at the same branch.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages _____ Part 3 Pages _____

Other Considerations: _____

20. David Jones, a customer of Anytown Bank, operates “Dave’s Crispy Fried Chicken,” a sole proprietorship. An employee of the restaurant makes a deposit to the business account of \$11,000 in cash.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

21. Dorothy Green, a partner at a law firm, makes a \$50,000 cash deposit into the firm’s escrow account. The \$50,000 represents cash received from three clients.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

22. Wayne Uberboss owns four separate corporations. These corporations each have their own separate account, and their own separate EIN, and the bank account statements for all four accounts are mailed to the same office at the same address. Either Wayne or his administrative assistant Vicky Portensky make cash deposits for each of the corporations, using four separate branch offices, always on the same business day. The cash deposits today for each of the respective corporations totaled \$2,750, \$2,850, \$ 2,950, and \$ 3,150 respectively.

CTR Filed: ☐ YES ☐ NO

Part 1 Pages_____ Part 3 Pages_____

Other Considerations:_____

Notice to Customers: A CTR Reference Guide

Why is my financial institution asking me for identification and personal information?

Federal law requires financial institutions to report currency (cash or coin) transactions over \$10,000 conducted by, or on behalf of, one person, as well as multiple currency transactions that aggregate to be over \$10,000 in a single day. These transactions are reported on Currency Transaction Reports (CTRs). The federal law requiring these reports was passed to safeguard the financial industry from threats posed by money laundering and other financial crime. To comply with this law, financial institutions must obtain personal identification information about the individual conducting the transaction such as a Social Security number as well as a driver's license or other government issued document. This requirement applies whether the individual conducting the transaction has an account relationship with the institution or not.

There is no general prohibition against handling large amounts of currency and the filing of a CTR is required regardless of the reasons for the currency transaction. The financial institution collects this information in a manner consistent with a customer's right to financial privacy.

Can I break up my currency transactions into multiple, smaller amounts to avoid being reported to the government?

No. This is called "structuring." Federal law makes it a crime to break up transactions into smaller amounts for the purpose of evading the CTR reporting requirement and this may lead to a required disclosure from the financial institution to the government. Structuring transactions to prevent a CTR from being reported can result in imprisonment for not more than five years and/or a fine of up to \$250,000. If structuring involves more than \$100,000 in a twelve month period or is performed while violating another law of the United States, the penalty is doubled.



www.fincen.gov



The following scenarios are examples of structuring.

Examples of Structured Transactions

1. John has \$15,000 in cash he obtained from selling his truck. John knows that if he deposits \$15,000 in cash, his financial institution will be required to file a CTR. John instead deposits \$7,500 in cash in the morning with one financial institution employee and comes back to the financial institution later in the day to another employee to deposit the remaining \$7,500, hoping to evade the CTR reporting requirement.
2. Jane needs \$18,000 in cash to pay for supplies for her wood-carving business. Jane cashes a \$9,000 personal check at a financial institution on a Monday, then cashes another \$9,000 personal check at the financial institution the following day. Jane cashed the checks separately and structured the transactions in an attempt to evade the CTR reporting requirement.
3. A married couple, John and Jane, sell a vehicle for \$15,000 in cash. To evade the CTR reporting requirement, John and Jane structure their transactions using different accounts. John deposits \$8,000 of that money into his and Jane's joint account in the morning. Later that day, Jane deposits \$1,500 into the joint account, and then \$5,500 into her sister's account, which is later transferred to John and Jane's joint account.
4. Bob wants to place \$24,000 cash he earned from his illegal activities into the financial system by using a wire transfer. Bob knows his financial institution will file a CTR if he purchases a wire with over \$10,000 currency in one day. To evade the CTR reporting requirement, Bob wires the \$24,000 by purchasing wires with currency in \$6,000 increments over a short period of time, occasionally skipping days in an attempt to prevent the financial institution from filing a CTR.



If you have further questions, please contact
FinCEN's Regulatory Helpline at (800) 949-2732

EXEMPTION QUESTIONS

True or False

- _____ 1. Banks may exempt individuals from CTR filing.
- _____ 2. Government entities are automatically exempt from CTR filing and the exempting DFI need not file a written designation of exemption with FinCEN.
- _____ 3. Financial institutions are required to exempt all exemptible commercial entities.
- _____ 4. Once designated as exempt under the exemption rules, a bank must verify the continuing status of each exempt person once every five years.
- _____ 5. Once initially designated as a “non-listed business” or “payroll customer,” no additional exemption filings are required between the bank and the treasury.
- _____ 6. Biennial Renewals begin on the second anniversary of the initial exemption designation.
- _____ 7. Money Market Accounts (MMDAs) cannot be exempted.
- _____ 8. Franchise outlets may be placed on the bank’s exempt list.
- _____ 9. Banks are not obligated to report suspicious transactions on exempt persons.
- _____ 10. Either a bank holding company, or one of the subsidiary affiliates within the group, may make a designation of exempt person.
- _____ 11. Sole Proprietorships cannot be exempted as a “non-listed business.”
- _____ 12. Financial institutions must formally designate their Federal Reserve Bank in order to exempt cash transactions between themselves and the Fed.
- _____ 13. A business that engages in multiple business activities may be treated as a non-listed business so long as no more than 60% of its gross revenues are not derived from ineligible business activities.
- _____ 14. A Money Services Business (MSB) cannot be an exempt person.
- _____ 15. Federal examiners will not expect banks to produce evidence of the existence of a monitoring system designed to detect those transactions in currency that would require a bank to file a SAR on that exempt person.
- _____ 16. A financial institution to whom you provide a “one-time” supply of “emergency” currency does not have to be formally exempted from CTR reporting.
- _____ 17. All legal entity customers eligible for exemption from CTR filing are excluded from the beneficial ownership requirements.

(Blank Page)

OFFICE OF FOREIGN ASSETS CONTROL

I. INTRODUCTION AND OVERVIEW

- A. OFAC** - The Office of Foreign Assets Control (OFAC) is an office within the Treasury Department that administers and enforces economic and trade sanctions based on U.S. Foreign Policy and National Security Goals, enacted against targeted individuals, foreign countries, and organizations that not only sponsor terrorism and international drug trafficking, but also those engaged in activities related to the proliferation of weapons of mass destruction. OFAC imposes controls on transactions and freezes foreign assets under U.S. jurisdiction in an effort to thwart money launderers and others who may use financial institutions to commit or finance crimes.

The laws enforced by OFAC include, among others, the Trading with the Enemy Act, the International Emergency Economic Powers Act, the Antiterrorism and Effective Death Penalty Act, the Foreign Narcotics Kingpin Designations Act, the National Emergencies Act and the Countering America's Adversaries Through Sanctions Act. OFAC regulations are located at 31 CFR 500.

- B. OFAC and BSA** - The OFAC regulations are not part of BSA. However, many of the countries, organizations and persons targeted by OFAC have been designated by the U.S. government as involved or associated with the types of activities which BSA regulations attempt to detect and prevent.

C. Coverage and Penalties

1. Coverage - OFAC describes the universe as covered under its jurisdiction. Therefore, all U.S. Citizens and corporations, permanent resident aliens, individuals, and entities located in or organized under U.S. law are subject to OFAC requirements.

OFAC restrictions cover virtually all types of financial transactions including:

- a. Funds transfers;
 - b. Letters of Credit;
 - c. Account openings;
 - d. Bank card issuances;
 - e. Internet banking activities; and
 - f. Philanthropic activities of the bank.
2. Penalties - The U.S. Congress takes compliance with the OFAC-administered laws very seriously. The fines for violations can be substantial. Banks, entities, and individuals found liable for violating these laws can be subject to criminal fines ranging up to \$10,000,000, and imprisonment ranging up to 30 years. OFAC-related civil penalties range from one-half of the transaction's value (for non-egregious, self-disclosed transactions) up to the statutory

maximum (for egregious, non-disclosed transactions) for each violation. (85 FR 19884-19888, 04/09/2020)

D. SDNs, Blocked Persons, and Related Sanctions

1. One of the primary concerns of OFAC is the placement of individuals on the Specially Designated Nationals and Blocked Persons list - "the SDN List." This is an extensive list of individuals and entities which are owned or controlled by, or acting for or on behalf of the governments of targeted countries or are associated with international narcotics trafficking, terrorism, and other sanction programs. This list includes, but is limited to:
 - a. SDN - Specially Designated Nationals
 - b. SDT - Specially Designated Terrorists
 - c. SDGT - Specially Designated Global Terrorists
 - d. FTO - Foreign Terrorist Organizations
 - e. SDNT - Specific Designated Narcotics Traffickers
 - f. SDNTKs - Specially Designated Narcotics Traffickers as designated under the Foreign Narcotics Kingpin Designation Act
 - g. TCOs – Transnational Criminal Organization
 - h. Countering America's Adversaries Through Sanctions (CAATSA)
 - i. Counter Narcotics Trafficking Sanctions
 - j. Counter Terrorism Sanctions
 - k. Cyber-Related Sanctions
 - l. Foreign Interference in a U.S. Election Sanctions
 - m. Non-Proliferation Sanctions
 - n. Rough Diamond Trade Controls

2. OFAC also administers specific sanctions against these following countries:
- a. Balkans (certain entities);
 - b. Belarus;
 - c. Burundi;
 - d. Central African Republic;
 - e. Cuba;
 - f. Democratic Republic of Congo;
 - g. Hong-Kong – Related Sanctions – (07/2020)
 - h. Iran – See documents related to the JCPOA Implementation 01/16/16;
 - i. Iraq –Related Sanctions;
 - j. Lebanon;
 - k. Libya;
 - l. Mali Related Sanctions;
 - m. Myanmar – Related Sanctions (02/2021)
 - n. Nicaragua – Related Sanctions;
 - o. North Korea;
 - p. Somalia;
 - q. South Sudan – Related Sanctions;
 - r. Sudan and Darfur
 - s. Syria and Syria Related Sanctions;
 - t. Ukraine/Russia – Related Sanctions;
 - u. Venezuela – Related Sanctions;
 - v. Yemen – Related Sanctions;
 - w. Zimbabwe (certain persons);

Financial institutions should refer to OFAC for details of each of the specific country sanction programs.

- E. SDN List** - The SDN list is updated on an as needed basis by OFAC. The date of the latest release of the list, as well as copies of the list, may be downloaded from OFAC's web site www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

NOTE: In early February 2019, multiple users of OFAC's data files contacted OFAC's technical support hotline to report difficulty in downloading sanctions list data files hosted at this URL: <https://www.treasury.gov/ofac/downloads/>. After investigating the issue, the Treasury Department discovered that changes had been made regarding HTTP request methods. These changes generally affected users that leverage command line connections to Treasury's website. Users who download OFAC's sanctions list data files manually via browser were not impacted by this change. (Previously users were allowed to request sanctions list data files via HTTP using both POST and GET commands. The change made in February 2019 eliminated the users' ability to use the POST command, and only GET commands are allowed henceforth. This change was made to improve the security for public file repositories and is a permanent change.

Users who continue to have difficulty downloading OFAC's sanctions list data files due to this change are welcome to contact OFAC at O.F.A.C@treasury.gov or contact OFAC's technical support hotline at 1-800-540-6322 – Menu Option 8 for assistance. (OFAC understands that this change may have unexpectedly interrupted users' ability to download and access OFAC data and is working with Treasury's technical team to ensure advance notification of any future changes).

- F. Consolidated Sanctions List Data Files** – In October 2014, OFAC created a consolidated set of data files, the "Consolidated Sanctions List", in order to make it easier to comply with OFAC sanctions regulations by reducing the number of list-related files that must be downloaded in order to maintain an automated sanctions screening program. Currently included in the Consolidated Sanctions List Data Files are the:

- Sectoral Sanctions Identifications (SSI) List – first created in July 2014 – E.O. 13662;
- Foreign Sanctions Evaders (FSE) List – first created in February 2014 – E.O. 13608;
- Non-SDN Iranian Sanctions Act (NS-ISA) List – first created in May 2011 – E.O. 13574;
- List of Foreign Financial Institutions Subject to Part 561 (the Part 561) List – CISADA (2010), NDAA (2012), and IFCA (2012);
- Palestinian Legislative Council (NS-PLC) List – first created in April 2006 – General License 4;
- List of Foreign Financial Institutions Subject to Correspondent Account or Payable Through Account Sanctions (CAPTA List) – first created in March 2019 – E.O. 13846.

- Non-SDN Menu-Based Sanctions (NS-MBS) List – first created in December 2020 – E. O. 13849, CAATSA, and the Ukraine Freedom Support Act.

In the future, as OFAC creates new non-SDN style lists, they will add the new data associated with such to the Consolidated Sanctions List Data Files if appropriate.

- G. Sanctions List Search Tool** – On December 7, 2011, OFAC released an online search application now called “Sanctions List Search” which provides an online interface to search the SDN list across several criteria. The results are viewable on-screen, they are printable, and can be saved as a spreadsheet. On October 10, 2014, the Sanctions List Search tool was upgraded to provide the users the ability to search for a name on the SDN list, on the Consolidated List, or on both lists simultaneously. With this upgrade, users can look for potential name matches on the SDN, SSI, FSE, NS-PLC, NS-ISA and Part 561 Lists. “Sanctions List Search” may be accessed at <https://sanctionssearch.ofac.treas.gov>.

II. A FRAMEWORK FOR OFAC COMPLIANCE COMMITMENTS – On May 02, 2019, OFAC published this framework document. OFAC strongly encourages organizations and persons subject to U.S. jurisdiction to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP). While each risk-based SCP will vary depending on a variety of factors – each program should be predicated on and incorporate at least five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

- A. Management Commitment** – Senior Management’s commitment to, and support of, an organization’s risk-based SCP is one of the most important factors in determining success. This support is essential in ensuring the SCP receives adequate resources and is fully integrated into the organization’s daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.
- B. Risk Assessment** – OFAC recommends that organizations conduct a routine, and if appropriate, ongoing “risk-assessment” for the purposes of identifying potential OFAC issues they are likely to encounter. While there is no “one-size-fits-all” risk assessment, the exercise should generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world. This process allows the organization to identify potential areas in which it may directly or indirectly engage with OFAC-prohibited persons, parties, countries, or regions. An organization’s SCP may assess: (i) customers, supply chain intermediaries, and counter-parties; (ii) products and services it offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and (iii) geographic locations of the organization, as well as its customers and counter-parties.

C. Internal Controls – An effective OFAC compliance program should include internal controls for identifying suspect accounts and reporting to OFAC. Internal controls should include, but are not limited to:

1. **Flagging and Review of suspect transactions and accounts** – Policies and procedures should address how the institution will flag and review transactions and accounts for possible OFAC violations, whether such reviews are conducted manually, systematically, or a combination of both. An institution's procedures should clearly define "how" the names on the OFAC list will be compared with the names in its files or on the transactions, and for flagging transactions or accounts involving the sanctioned countries. In high-risk and high-volume areas, the institution's interdiction filter should be able to flag "close-name" derivations for review. New accounts should be compared with the OFAC list prior to allowing transactions, and established accounts once scanned, should be compared regularly against the OFAC updates.
2. **Updating the Compliance Program** – An institution's OFAC compliance program should also include procedures for maintaining the current lists of blocked countries, entities, and individuals and for disseminating such information throughout the organization, including foreign offices and foreign subsidiaries.
3. **Reporting** – An institution's OFAC compliance program should also include procedures for handling transactions that are validly blocked or rejected under the various sanctions program. These procedures should cover the initial reporting of blocked and rejected items (10 days), and the required annual report when applicable.
4. **Management of Blocked Accounts** – An audit trail should be maintained in order to reconcile all blocked funds. The institution is responsible for tracking the amount of blocked funds, the ownership of those funds, interest paid on those funds, and the release of blocked funds pursuant to license from OFAC.
5. **Maintaining License Information** – An institution should maintain copies of their client's OFAC specific licenses on file. In some cases, it is a sound compliance practice for the financial institution to obtain a statement from the licensee that the transaction is in accordance with the terms of the license, assuming that the financial institution does not know or have reason to know that the statement is false.

D. Testing – Each institution should have a periodic independent test of its OFAC program. The frequency of the independent test should be consistent with the institution's OFAC risk profile, however an in-depth audit of each department within the institution might reasonably be conducted at least once a year. The audit scope should be comprehensive and sufficient to assess OFAC compliance risks across the spectrum of all institutional activities. Should violations be discovered, they should be reported to both OFAC and the institution's federal functional regulator.

- E. Responsible Individuals** – A financial institution should designate a qualified individual or individuals to be responsible for day-to-day compliance of its OFAC compliance program. The individual(s) should be fully knowledgeable about OFAC statutes, regulations, and relevant Executive Orders. (There should also be at least one individual responsible for the oversight of blocked funds, if applicable).
- F. Training** - A financial institution should provide adequate OFAC training for all appropriate employees. The scope of the training should be consistent with the OFAC risk rating and the employee's particular OFAC responsibilities.
- G. ACH Compliance** - In April 2009, the National Automated Clearinghouse Association (NACHA) issued "Rules Supplement # 1-2009" which updated the NACHA Operating Guidelines related to OFAC compliance in ACH processing.

When processing domestic ACH entries, Receiving Depository Financial Institutions (RDFIs) primarily rely on their own institutional customer/account level OFAC compliance program to maintain compliance. In the event that an ODFI inadvertently transmits an unlawful ACH credit, the RDFI should post the credit, ensure the account and funds are frozen, and report the transaction to OFAC. If an ODFI were to inadvertently transmit an unlawful ACH debit, the RDFI should ensure the account is frozen, report the transaction to OFAC, and return the debit item using Return Reason Code R16 (Account Frozen).

When processing domestic ACH entries, Originating Depository Financial Institutions (ODFIs) primarily rely on the Originator/ODFI agreement wherein the Originator is reminded that the Originator themselves is the primary party responsible for the OFAC compliance of the individual transactions contained within the file. (The ODFI must have a process in place to determine whether any of their account holders, including Originators, are identified blocked parties under OFAC. The ODFI may also find it contractually helpful to reference possible delays in processing, settlement, and/or availability of these transactions when enhanced scrutiny or OFAC verification is mandated). If the ODFI encounters a transaction in the normal course of business that would violate OFAC-enforced sanctions, federal law does require the ODFI to comply with OFAC policies. (NOTE: If the ODFI "unbundles" those originated files, greater OFAC scrutiny must be applied by the ODFI to the individual transactions).

On September 18, 2009, NACHA implemented a new Standard Entry Class (SEC) code - IAT (International ACH Transactions) – to identify **ALL** international payments transmitted through the ACH network. RDFIs and Receivers have the obligation to ensure that all aspects of inbound, cross-border transactions are in compliance with OFAC and take the appropriate steps to investigate, suspend, reject, block, and report to OFAC on transactions when necessary. ODFIs and their Originators have the obligation to ensure that all parties to the transactions, as well as the underlying purpose of the transactions are not in violation of OFAC regulations, and must take appropriate steps to investigate, suspend, reject, block, and report on transactions when necessary. When processing international ACH entries, the RDFI when handling inbound entries:

1. If the unlawful inbound IAT credit entry is for a Receiver that is subject to an OFAC sanction, the RDFI is to post the credit entry to the account, ensure that the account and funds are frozen, and report the transaction to OFAC (Fax: 202-622-2426);
2. If the unlawful inbound IAT credit entry is from an Originator subject to an OFAC sanction, the transaction should not be posted, the funds should be suspended, and the transaction reported to OFAC (800-540-6322);
3. If the unlawful inbound IAT is a debit entry, the RDFI should investigate the transaction, and if found to be in violation of an OFAC sanction, the RDFI should contact OFAC for guidance, as OFAC will handle unlawful debit transactions on a case by case basis (800-540-6322).

When processing international ACH entries, the ODFI when handling outbound entries, should screen ALL (IAT) transactions for OFAC compliance prior to being released to the ACH Operator. All parties and all information (including addenda records and remittance information) must be reviewed, and if suspect transactions are discovered, they must be investigated and cleared before release. If the transaction is found to violate an OFAC sanction, the transaction should be frozen or rejected depending on the specifics of the particular sanctions program.

A financial institution acting as an ODFI/Gateway Operator for IAT debit transactions has additional responsibilities under the most recent NACHA guidance, and those institutions should thoroughly review Supplement #1 to the 2009 ACH Rules and ensure proper compliance of such.

All financial institutions must recognize that there is NO time limit for the resolution of suspect IAT transactions.

H. Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments – On October 01, 2020, OFAC issued this Advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the Covid-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions not only encourage future ransomware payment demands but also may risk violating OFAC regulations. OFAC has designated numerous malicious actors under its cyber-related sanctions program, including perpetrators of ransomware attacks and those who facilitate ransomware attacks and those who facilitate ransomware transactions. OFAC strongly suggests that a financial institution's SCP account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction.

I. Exam Procedures - Contained within the current Interagency BSA/AML Examination Manual are the core examination procedures covering an institution's OFAC program. Highly qualitative and subjective in nature, the Federal examiner will evaluate the program to determine whether it is

appropriate for the institution's OFAC risk assessment. The examiner will also form a conclusion about the ability of policies, procedures, and processes to meet the regulatory requirements associated with OFAC by completing a number of reviews which will, or will consider:

1. Determine whether the board and senior management of the institution have developed policies, procedures, and processes based on their risk assessment to ensure compliance with OFAC laws and regulations.
2. The extent of, and method for, conducting OFAC searches of each relevant department/business line.
3. The extent of, and method for, conducting OFAC searches of account parties other than accountholders, which may include beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney.
4. How responsibility for OFAC is assigned.
5. Timeliness of obtaining and updating OFAC lists or filtering criteria.
6. The appropriateness of the filtering criteria used by the institution to reasonably identify OFAC matches (e.g. the extent to which the filtering/search criteria includes misspellings and name derivations).
7. The process used to investigate potential matches.
8. The process used to block and reject transactions.
9. The process used to inform management of blocked or rejected transactions.
10. The adequacy and timeliness of reports to OFAC.
11. The process to manage blocked accounts (such accounts are reported to OFAC and pay a commercially reasonable rate of interest).
12. The record retention requirements (e.g. five years after property is unblocked.)
13. Identify any potential matches not reported to OFAC and advise institution management and OFAC.
14. Determine the origin of deficiencies and conclude on the adequacy of the institution's OFAC compliance program.

On the basis of such risk assessment, prior examination reports, and a review of the institution's own audit findings, the examiner will select a variety of samples and perform transactional testing to test the adequacy of the program.



Sanctions List Search

Specifically Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaded List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program code and the search criteria. Thus, when a user enters a search term in a refined value field, the Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into the Sanctions List Search tool. The Sanctions List Search tool does not perform exact string matching. Sanctions List Search has a side-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return any, or proximate, matches, based on the confidence rating set by the user via the side-bar. The Sanctions List Search tool is not intended to be a substitute for the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists, use of Sanctions List Search is not intended to be a substitute for conducting appropriate due diligence. The use of Sanctions List Search does not imply any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

[Download the SDN List](#)

[Sanctions List Search](#), [Rules for use](#)

Visit The OFAC Website

[Download the Consolidated Non-SDN List](#)

Program Code Key

Lookup

Type:

All

Name:

ID #:

Program:

All

SSI-Related

BALKANS

BEIARIUS

Minimum Name Score:

100

Address:

City:

State/Province*:

Country:

All

List:

All

Search

Reset

Lookup Results:

Name	Address	Type	Program(s)	List	Score
------	---------	------	------------	------	-------

* U.S. states are abbreviated on the SDN and Non-SDN lists. To search for a specific U.S. state, please use the two letter U.S. Postal Service abbreviation.

SDN List last updated on: 12/16/2020 10:01:35 AM
Non-SDN List last updated on: 12/14/2020 12:44:01 PM

REPORT ON BLOCKED PROPERTY – FINANCIAL*

(Use of this form is optional, but the information requested is required by 31 C.F.R. § 501.603)

**UNITED STATES DEPARTMENT OF THE TREASURY
OFFICE OF FOREIGN ASSETS CONTROL****REPORTING INSTITUTION INFORMATION**

INSTITUTION NAME	
ADDRESS	
CITY	
STATE	
POSTAL CODE	
COUNTRY	
CONTACT PERSON NAME	
TITLE	
TELEPHONE NUMBER	
E-MAIL ADDRESS	
DATE PREPARED	

TRANSACTION INFORMATION*

VALUE (USD)	
VALUE DATE	
DATE OF BLOCKING	
TYPE OF TRANSACTION OR PROPERTY (e.g., wire transfer, account, letter of credit, check, securities)	
LEGAL AUTHORITY OR AUTHORITIES FOR BLOCKING (e.g., 31 C.F.R Part 560)	
SANCTIONS TARGET / NEXUS (e.g., name of Specially Designated National or blocked person)	
ORIGINATOR NAME & ADDRESS	
ORIGINATING FINANCIAL INSTITUTION NAME & ADDRESS	
SENDER'S CORRESPONDENT (if applicable)	
RECEIVER'S CORRESPONDENT (if applicable)	
INTERMEDIARY FINANCIAL INSTITUTION NAME & ADDRESS	
BENEFICIARY FINANCIAL INSTITUTION NAME & ADDRESS	
BENEFICIARY NAME & ADDRESS	
SENDER'S REFERENCE	
BANK REFERENCE NUMBER	
ORIGINATOR TO BENEFICIARY AND / OR BANK TO BANK INFORMATION	

* For blocked accounts, checks, letters of credit, securities, and other financial property, some of the above fields may not be applicable. Complete all applicable fields and include all other relevant information (e.g., account number, check number, drawee bank) in the "Additional Relevant Information" field on page 2. To report other types of blocked property, please use the form "Report on Blocked Property – Tangible/Real/Other Non-financial Property" (Form TD-F 93.08).

PLEASE INCLUDE A COPY OF ANY PAYMENT OR TRANSFER INSTRUCTIONS OR OTHER RELEVANT DOCUMENTATION AS A SEPARATE ATTACHMENT

TD-F 93.02

ADDITIONAL RELEVANT INFORMATION

Public reporting burden for this collection of information is estimated to average 30 minutes per response. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information to the Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Freedman's Bank Building, Washington, DC 20220.

REPORT ON REJECTED TRANSACTION*

(Use of this form is optional, but the information requested is required by 31 C.F.R. § 501.604)

**UNITED STATES DEPARTMENT OF THE TREASURY
OFFICE OF FOREIGN ASSETS CONTROL****REPORTING INSTITUTION INFORMATION**

INSTITUTION NAME	
ADDRESS	
CITY	
STATE	
POSTAL CODE	
COUNTRY	
CONTACT PERSON NAME	
TITLE	
TELEPHONE NUMBER	
E-MAIL ADDRESS	
DATE PREPARED	

TRANSACTION INFORMATION

VALUE (USD)	
VALUE DATE	
DATE OF REJECTION	
TYPE OF TRANSACTION (e.g., wire transfer, account, letter of credit, check, securities)	
LEGAL AUTHORITY OR AUTHORITIES FOR REJECTING (e.g., 31 C.F.R Part 560)	
SANCTIONS TARGET / NEXUS (e.g., sectoral sanctions target or commercial activity with Cuba, Iran, Syria, Crimea)	
ORIGINATOR NAME & ADDRESS	
ORIGINATING FINANCIAL INSTITUTION NAME & ADDRESS	
SENDER'S CORRESPONDENT (if applicable)	
RECEIVER'S CORRESPONDENT (if applicable)	
INTERMEDIARY FINANCIAL INSTITUTION NAME & ADDRESS	
BENEFICIARY FINANCIAL INSTITUTION NAME & ADDRESS	
BENEFICIARY NAME & ADDRESS	
SENDER'S REFERENCE	
BANK REFERENCE NUMBER	
ORIGINATOR TO BENEFICIARY AND / OR BANK TO BANK INFORMATION	

* For certain rejected transactions, some of the above fields may not be applicable. Complete all applicable fields and include all other relevant information (e.g., account number, check number, drawee bank) in the "Additional Relevant Information" field on page 2. To report blocked property, please use form "Report on Blocked Property – Tangible/Real/Other Non-financial Property" (Form TD-F 93.08) or "Report on Blocked Property – Financial" (Form TD-F 93.02), whichever is applicable.

PLEASE INCLUDE A COPY OF ANY PAYMENT OR TRANSFER INSTRUCTIONS OR OTHER RELEVANT DOCUMENTATION AS A SEPARATE ATTACHMENT

TD-F 93.07

ADDITIONAL RELEVANT INFORMATION

Public reporting burden for this collection of information is estimated to average 30 minutes per response. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information to the Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Freedman's Bank Building, Washington, DC 20220.

OMB No. 1505-0164

ANNUAL REPORT OF BLOCKED PROPERTY
 UNITED STATES DEPARTMENT OF THE TREASURY
 OFFICE OF FOREIGN ASSETS CONTROL

Part A - U.S. Person Holding Blocked Property

(1) Enter the name and address of the person (e.g., specific financial institution or company) holding the blocked property.

Name:	<Enter Detail Here>
Address:	<Enter Detail Here>
City:	<Enter Detail Here>
State:	<Enter Detail Here>
Postal code:	<Enter Detail Here>
Country:	<Enter Detail Here>

(2) Enter the contact details for the individual from whom additional information may be obtained.

Name:	<Enter Detail Here>
Title:	<Enter Detail Here>
Telephone #:	<Enter Detail Here>
Email:	<Enter Detail Here>
Date prepared:	<Enter Detail Here>

(3) Enter the total quantity of accounts or items reported in the Part B tab:

<Enter Detail Here>

* Please note that the total quantity of accounts or items reported in section (3) must equal the total number of rows containing blocked assets in the Part B tab.

Instructions for the Part B tab

Identify each account or item of blocked property separately in the rows provided in the "Part B" tab. Be sure to indicate the total number of accounts or items reported on Part B in the appropriate space on Part A. Basic details regarding certain information requested in Part B are noted below, however, please refer to 31 C.F.R. 501.603(b)(2)(ii) and the *Guidance on Filing the Annual Report of Blocked Property* on OFAC's Reporting and License Application Forms webpage for further details on the information required to be reported.

Date of Blocking	The date the property was blocked, if available.
Value (USD)	Provide the actual or estimated value of the property in U.S. Dollars as of June 30. If a value date other than June 30 is reported, so indicate.
Legal Authority or Authorities	Legal authority or authorities under which the property is blocked (e.g., 31 C.F.R. Part 515)
Sanctions Target	The associated sanctions target whose property is blocked, or a reference to the relevant communication from OFAC instructing a party to block this property if that target is unknown.
Owner of Property	The person who legally owns the account or other property. In the case of a blocked funds transfer, the party whose account is being debited to effect the transaction.
Owner Type	Please indicate the owner type using the following categories: individual; U.S. bank; non-U.S. bank; U.S. non-bank entity; non-U.S. non-bank entity; or other.
Description	A brief but comprehensive description of the property that is the subject of the blocking, including: • Asset Type (e.g., Bank account, check, wire transfer, stocks, real estate, tangible property) • Account Type (e.g., checking, savings) • Account Number (if applicable for blocked financial assets)
Location (city & country)	List the location or branch where the property is held, if different from the address shown in Part A.
New Item? (Y/N)	"Please indicate "Y" if this is a new item that has not previously been reported. If this property was reported on the prior year's annual report, please indicate "N."

PAPERWORK REDUCTION ACT NOTICE
 Public reporting burden for this collection of information is estimated to average two hours per response. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information to the Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Friedman's Bank Building, Washington, DC 20220.

TD-F 90-22.50

Date of Blocking	Value (USD)	Legal Authority or Authorities	Sanctions Target	Owner of Property	Asset Type	Account Type(s)	Account Number(s)	Additional Description of the Property (if needed)	Location: City	Location: Country	New Item? (Y/N)
------------------	-------------	--------------------------------	------------------	-------------------	------------	-----------------	-------------------	--	----------------	-------------------	-----------------

Office of Foreign Assets Control



This form is specifically designed to facilitate OFAC advice regarding "in process" wire-transfers. Questions or comments received via this form that are not related to in process wire-transfers will not be considered. You will receive a call back as soon as possible.

*=Required Field

Name	*	<input type="text"/>
Institution	*	<input type="text"/>
Work Phone	*	<input type="text"/>
E-mail Address	*	<input type="text"/>
Specific "Hit" or SDN Match (if any)	*	<input type="text"/>
Amount (in US dollars please)	*	<input type="text"/>
Value Date (MM/DD/YYYY format please)		<input type="text"/>
Originator		<input type="text"/>
Originator Bank		<input type="text"/>
Intermediary Financial Institution		<input type="text"/>
Beneficiary Bank		<input type="text"/>
Beneficiary		<input type="text"/>

Originator to Beneficiary Information

Additional Information on the Transaction (Remarks)

NOTE:

OFAC is unable to consider hypothetical or non-specific transactions. Use of this system does not exempt users from filing a formal blocking or reject report.

If you wish to contact the OFE Technical Assistance Center by telephone, please call (202) 622-9372



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

A Framework for OFAC Compliance Commitments

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces U.S. economic and trade sanctions programs against targeted foreign governments, individuals, groups, and entities in accordance with national security and foreign policy goals and objectives.

OFAC strongly encourages organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP). While each risk-based SCP will vary depending on a variety of factors—including the company's size and sophistication, products and services, customers and counterparties, and geographic locations—each program should be predicated on and incorporate at least five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

If after conducting an investigation and determining that a civil monetary penalty ("CMP") is the appropriate administrative action in response to an apparent violation, the Office of Compliance and Enforcement (OCE) will determine which of the following or other elements should be incorporated into the subject person's SCP as part of any accompanying settlement agreement, as appropriate. As in all enforcement cases, OFAC will evaluate a subject person's SCP in a manner consistent with the Economic Sanctions Enforcement Guidelines (the "Guidelines").

When applying the Guidelines to a given factual situation, OFAC will consider favorably subject persons that had effective SCPs at the time of an apparent violation. For example, under General Factor E (compliance program), OFAC may consider the existence, nature, and adequacy of an SCP, and when appropriate, may mitigate a CMP on that basis. Subject persons that have implemented effective SCPs that are predicated on the five essential components of compliance may also benefit from further mitigation of a CMP pursuant to General Factor F (remedial response) when the SCP results in remedial steps being taken.

Finally, OFAC may, in appropriate cases, consider the existence of an effective SCP at the time of an apparent violation as a factor in its analysis as to whether a case is deemed "egregious."

This document is intended to provide organizations with a framework for the five essential components of a risk-based SCP, and contains an appendix outlining several of the root causes that have led to apparent violations of the sanctions programs that OFAC administers. OFAC recommends all organizations subject to U.S. jurisdiction review the settlements published by OFAC to reassess and enhance their respective SCPs, when and as appropriate.

MANAGEMENT COMMITMENT

Senior Management's commitment to, and support of, an organization's risk-based SCP is one of the most important factors in determining its success. This support is essential in ensuring the SCP receives adequate resources and is fully integrated into the organization's daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.

General Aspects of an SCP: Senior Management Commitment

Senior management commitment to supporting an organization's SCP is a critical factor in determining the success of the SCP. Effective management support includes the provision of adequate resources to the compliance unit(s) and support for compliance personnel's authority within an organization. The term "senior management" may differ among various organizations, but typically the term should include senior leadership, executives, and/or the board of directors.

- I. Senior management has reviewed and approved the organization's SCP.**
- II. Senior management ensures that its compliance unit(s) is/are delegated sufficient authority and autonomy to deploy its policies and procedures in a manner that effectively controls the organization's OFAC risk. As part of this effort, senior management ensures the existence of direct reporting lines between the SCP function and senior management, including routine and periodic meetings between these two elements of the organization.**
- III. Senior management has taken, and will continue to take, steps to ensure that the organization's compliance unit(s) receive adequate resources—including in the form of human capital, expertise, information technology, and other resources, as appropriate—that are relative to the organization's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.**

These efforts could generally be measured by the following criteria:

- A.** The organization has appointed a dedicated OFAC sanctions compliance officer¹;
- B.** The quality and experience of the personnel dedicated to the SCP, including: (i) the technical knowledge and expertise of these personnel with respect to OFAC's regulations, processes, and actions; (ii) the ability of these personnel to understand complex financial and commercial activities, apply their knowledge of OFAC to these items, and identify OFAC-related issues, risks, and prohibited activities; and (iii) the efforts to ensure that personnel dedicated to the SCP have sufficient experience and an appropriate position within the organization, and are an integral component to the organization's success; and

¹ This may be the same person serving in other senior compliance positions, e.g., the Bank Secrecy Act Officer or an Export Control Officer, as many institutions, depending on size and complexity, designate a single person to oversee all areas of financial crimes or export control compliance.

- C. Sufficient control functions exist that support the organization's SCP—including but not limited to information technology software and systems—that adequately address the organization's OFAC-risk assessment and levels.

IV. Senior management promotes a “culture of compliance” throughout the organization.

These efforts could generally be measured by the following criteria:

- A. The ability of personnel to report sanctions related misconduct by the organization or its personnel to senior management without fear of reprisal.
- B. Senior management messages and takes actions that discourage misconduct and prohibited activities, and highlight the potential repercussions of non-compliance with OFAC sanctions; and
- C. The ability of the SCP to have oversight over the actions of the entire organization, including but not limited to senior management, for the purposes of compliance with OFAC sanctions.

V. Senior management demonstrates recognition of the seriousness of apparent violations of the laws and regulations administered by OFAC, or malfunctions, deficiencies, or failures by the organization and its personnel to comply with the SCP's policies and procedures, and implements necessary measures to reduce the occurrence of apparent violations in the future. Such measures should address the root causes of past apparent violations and represent systemic solutions whenever possible.

RISK ASSESSMENT

Risks in sanctions compliance are potential threats or vulnerabilities that, if ignored or not properly handled, can lead to violations of OFAC's regulations and negatively affect an organization's reputation and business. OFAC recommends that organizations take a risk-based approach when designing or updating an SCP. One of the central tenets of this approach is for organizations to conduct a routine, and if appropriate, ongoing “risk assessment” for the purposes of identifying potential OFAC issues they are likely to encounter. As described in detail below, the results of a risk assessment are integral in informing the SCP's policies, procedures, internal controls, and training in order to mitigate such risks.

While there is no “one-size-fits all” risk assessment, the exercise should generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world. This process allows the organization to identify potential areas in which it may, directly or indirectly, engage with OFAC-prohibited persons, parties, countries, or regions. For example, an organization's SCP may conduct an assessment of the following: (i) customers, supply chain, intermediaries, and counter-parties; (ii) the products and services it offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and (iii) the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counter-parties. Risk assessments and sanctions-related due diligence is also

important during mergers and acquisitions, particularly in scenarios involving non-U.S. companies or corporations.

General Aspects of an SCP: Conducting a Sanctions Risk Assessment

A fundamental element of a sound SCP is the assessment of specific clients, products, services, and geographic locations in order to determine potential OFAC sanctions risk. The purpose of a risk assessment is to identify inherent risks in order to inform risk-based decisions and controls. The Annex to Appendix A to 31 C.F.R. Part 501, OFAC's Economic Sanctions Enforcement Guidelines, provides an OFAC Risk Matrix that may be used by financial institutions or other entities to evaluate their compliance programs:

- I. The organization conducts, or will conduct, an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks. Such risks could be posed by its clients and customers, products, services, supply chain, intermediaries, counter-parties, transactions, and geographic locations, depending on the nature of the organization. As appropriate, the risk assessment will be updated to account for the root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business.**
- A. In assessing its OFAC risk, organizations should leverage existing information to inform the process. In turn, the risk assessment will generally inform the extent of the due diligence efforts at various points in a relationship or in a transaction. This may include:
 1. On-boarding: The organization develops a sanctions risk rating for customers, customer groups, or account relationships, as appropriate, by leveraging information provided by the customer (for example, through a Know Your Customer or Customer Due Diligence process) and independent research conducted by the organization at the initiation of the customer relationship. This information will guide the timing and scope of future due diligence efforts. Important elements to consider in determining the sanctions risk rating can be found in OFAC's risk matrices. [\[insert hyperlink\]](#)
 2. Mergers and Acquisitions (M&A): As noted above, proper risk assessments should include and encompass a variety of factors and data points for each organization. One of the multitude of areas organizations should include in their risk assessments—which, in recent years, appears to have presented numerous challenges with respect to OFAC sanctions—are mergers and acquisitions. Compliance functions should also be integrated into the merger, acquisition, and integration process. Whether in an advisory capacity or as a participant, the organization engages in appropriate due diligence to ensure that sanctions-related issues are identified, escalated to the relevant senior levels, addressed prior to the conclusion of any transaction, and incorporated into the organization's risk assessment process. After an M&A transaction is

completed, the organization's Audit and Testing function will be critical to identifying any additional sanctions-related issues.

- II. The organization has developed a methodology to identify, analyze, and address the particular risks it identifies. As appropriate, the risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business, for example, through a testing or audit function.**

INTERNAL CONTROLS

An effective SCP should include internal controls, including policies and procedures, in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that may be prohibited by the regulations and laws administered by OFAC. The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance (including reporting and escalation chains), and minimize the risks identified by the organization's risk assessments. Policies and procedures should be enforced, weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated, and internal and/or external audits and assessments of the program should be conducted on a periodic basis.

Given the dynamic nature of U.S. economic and trade sanctions, a successful and effective SCP should be capable of adjusting rapidly to changes published by OFAC. These include the following: (i) updates to OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"), the Sectoral Sanctions Identification List ("SSI List"), and other sanctions-related lists; (ii) new, amended, or updated sanctions programs or prohibitions imposed on targeted foreign countries, governments, regions, or persons, through the enactment of new legislation, the issuance of new Executive orders, regulations, or published OFAC guidance or other OFAC actions; and (iii) the issuance of general licenses.

General Aspects of an SCP: Internal Controls

Effective OFAC compliance programs generally include internal controls, including policies and procedures, in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that is prohibited by the sanctions programs administered by OFAC. The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance, and minimize the risks identified by an entity's OFAC risk assessments. Policies and procedures should be enforced, and weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated in order to prevent activity that might violate the sanctions programs administered by OFAC.

- I. The organization has designed and implemented written policies and procedures outlining the SCP. These policies and procedures are relevant to the organization, capture the organization's day-to-day operations and procedures, are easy to follow, and designed to prevent employees from engaging in misconduct.**

- II. The organization has implemented internal controls that adequately address the results of its OFAC risk assessment and profile. These internal controls should enable the organization to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the organization transactions and activity that may be prohibited by OFAC. To the extent information technology solutions factor into the organization's internal controls, the organization has selected and calibrated the solutions in a manner that is appropriate to address the organization's risk profile and compliance needs, and the organization routinely tests the solutions to ensure effectiveness.
- III. The organization enforces the policies and procedures it implements as part of its OFAC compliance internal controls through internal and/or external audits.
- IV. The organization ensures that its OFAC-related recordkeeping policies and procedures adequately account for its requirements pursuant to the sanctions programs administered by OFAC.
- V. The organization ensures that, upon learning of a weakness in its internal controls pertaining to OFAC compliance, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.
- VI. The organization has clearly communicated the SCP's policies and procedures to all relevant staff, including personnel within the SCP program, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing SCP responsibilities on behalf of the organization.
- VII. The organization has appointed personnel for integrating the SCP's policies and procedures into the daily operations of the company or corporation. This process includes consultations with relevant business units, and confirms the organization's employees understand the policies and procedures.

TESTING AND AUDITING

Audits assess the effectiveness of current processes and check for inconsistencies between these and day-to-day operations. A comprehensive and objective testing or audit function within an SCP ensures that an organization identifies program weaknesses and deficiencies, and it is the organization's responsibility to enhance its program, including all program-related software, systems, and other technology, to remediate any identified compliance gaps. Such enhancements might include updating, improving, or recalibrating SCP elements to account for a changing risk assessment or sanctions environment. Testing and auditing can be conducted on a specific element of an SCP or at the enterprise-wide level.

General Aspects of an SCP: Testing and Auditing

A comprehensive, independent, and objective testing or audit function within an SCP ensures that entities are aware of where and how their programs are performing and should be updated, enhanced, or recalibrated to account for a changing risk assessment or sanctions environment, as appropriate. Testing or audit, whether conducted on a specific element of a compliance program or at the enterprise-wide level, are important tools to ensure the program is working as designed and identify weaknesses and deficiencies within a compliance program.

- I. The organization commits to ensuring that the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization.**
- II. The organization commits to ensuring that it employs testing or audit procedures appropriate to the level and sophistication of its SCP and that this function, whether deployed internally or by an external party, reflects a comprehensive and objective assessment of the organization's OFAC-related risk assessment and internal controls.**
- III. The organization ensures that, upon learning of a confirmed negative testing result or audit finding pertaining to its SCP, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.**

TRAINING

An effective training program is an integral component of a successful SCP. The training program should be provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually) and generally should accomplish the following: (i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments.

General Aspects of an SCP: Training

An adequate training program, tailored to an entity's risk profile and all appropriate employees and stakeholders, is critical to the success of an SCP.

- I. The organization commits to ensuring that its OFAC-related training program provides adequate information and instruction to employees and, as appropriate, stakeholders (for example, clients, suppliers, business partners, and counterparties) in order to support the organization's OFAC compliance efforts. Such training should be further tailored to high-risk employees within the organization.**

- II. The organization commits to provide OFAC-related training with a scope that is appropriate for the products and services it offers; the customers, clients, and partner relationships it maintains; and the geographic regions in which it operates.
- III. The organization commits to providing OFAC-related training with a frequency that is appropriate based on its OFAC risk assessment and risk profile.
- IV. The organization commits to ensuring that, upon learning of a confirmed negative testing result or audit finding, or other deficiency pertaining to its SCP, it will take immediate and effective action to provide training to or other corrective action with respect to relevant personnel.
- V. The organization's training program includes easily accessible resources and materials that are available to all applicable personnel.

**Root Causes of OFAC Sanctions Compliance Program Breakdowns or Deficiencies Based
on Assessment of Prior OFAC Administrative Actions**

Since its publication of the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, App. A (the “Guidelines”), OFAC has finalized numerous public enforcement actions in which it identified deficiencies or weaknesses within the subject person’s SCP. These items, which are provided in a non-exhaustive list below, are provided to alert persons subject to U.S. jurisdiction, including entities that conduct business in or with the United States, U.S. persons, or U.S.-origin goods or services, about several specific root causes associated with apparent violations of the regulations it administers in order to assist them in designing, updating, and amending their respective SCP.

I. Lack of a Formal OFAC SCP

OFAC regulations do not require a formal SCP; however, OFAC encourages organizations subject to U.S. jurisdiction (including but not limited to those entities that conduct business in, with, or through the United States or involving U.S.-origin goods, services, or technology), and particularly those that engage in international trade or transactions or possess any clients or counter-parties located outside of the United States, to adopt a formal SCP. OFAC has finalized numerous civil monetary penalties since publicizing the Guidelines in which the subject person’s lack of an SCP was one of the root causes of the sanctions violations identified during the course of the investigation. In addition, OFAC frequently identified this element as an aggravating factor in its analysis of the General Factors associated with such administrative actions.

II. Misinterpreting, or Failing to Understand the Applicability of, OFAC’s Regulations

Numerous organizations have committed sanctions violations by misinterpreting OFAC’s regulations, particularly in instances in which the subject person determined the transaction, dealing, or activity at issue was either not prohibited or did not apply to their organization or operations. For example, several organizations have failed to appreciate or consider (or, in some instances, actively disregarded) the fact that OFAC sanctions applied to their organization based on their status as a U.S. person, a U.S.-owned or controlled subsidiary (in the Cuba and Iran programs), or dealings in or with U.S. persons, the U.S. financial system, or U.S.-origin goods and technology.

With respect to this specific root cause, OFAC’s administrative actions have typically identified additional aggravating factors, such as reckless conduct, the presence of numerous warning signs that the activity at issue was likely prohibited, awareness by the organization’s management of the conduct at issue, and the size and sophistication of the subject person.

III. Facilitating Transactions by Non-U.S. Persons (Including Through or By Overseas Subsidiaries or Affiliates)

Multiple organizations subject to U.S. jurisdiction—specifically those with foreign-based operations and subsidiaries located outside of the United States—have engaged in transactions or activity that violated OFAC’s regulations by referring business opportunities to, approving or

signing off on transactions conducted by, or otherwise facilitating dealings between their organization's non-U.S. locations and OFAC-sanctioned countries, regions, or persons. In many instances, the root cause of these violations stems from a misinterpretation or misunderstanding of OFAC's regulations. Companies and corporations with integrated operations, particularly those involving or requiring participation by their U.S.-based headquarters, locations, or personnel, should ensure any activities they engage in (i.e., approvals, contracts, procurement, etc.) are compliant with OFAC's regulations.

IV. Exporting or Re-exporting U.S.-origin Goods, Technology, or Services to OFAC-Sanctioned Persons or Countries

Non-U.S. persons have repeatedly purchased U.S.-origin goods with the specific intent of re-exporting, transferring, or selling the items to a person, country, or region subject to OFAC sanctions. In several instances, this activity occurred despite warning signs that U.S. economic sanctions laws prohibited the activity, including contractual language expressly prohibiting any such dealings. OFAC's public enforcement actions in this area have generally been focused on companies or corporations that are large or sophisticated, engaged in a pattern or practice that lasted multiple years, ignored or failed to respond to numerous warning signs, utilized non-routine business practices, and—in several instances—concealed their activity in a willful or reckless manner.

V. Utilizing the U.S. Financial System, or Processing Payments to or through U.S. Financial Institutions, for Commercial Transactions Involving OFAC-Sanctioned Persons or Countries

Many non-U.S. persons have engaged in violations of OFAC's regulations by processing financial transactions (almost all of which have been denominated in U.S. Dollars) to or through U.S. financial institutions that pertain to commercial activity involving an OFAC-sanctioned country, region, or person. Although no organizations subject to U.S. jurisdiction may be involved in the underlying transaction—such as the shipment of goods from a third-country to an OFAC-sanctioned country—the inclusion of a U.S. financial institution in any payments associated with these transactions often results in a prohibited activity (e.g., the exportation or re-exportation of services from the United States to a comprehensively sanctioned country, or dealing in blocked property in the United States). OFAC has generally focused its enforcement investigations on persons who have engaged in willful or reckless conduct, attempted to conceal their activity (e.g., by stripping or manipulating payment messages, or making false representations to their non-U.S. or U.S. financial institution), engaged in a pattern or practice of conduct for several months or years, ignored or failed to consider numerous warning signs that the conduct was prohibited, involved actual knowledge or involvement by the organization's management, caused significant harm to U.S. sanctions program objectives, and were large or sophisticated organizations.

VI. Sanctions Screening Software or Filter Faults

Many organizations conduct screening of their customers, supply chain, intermediaries, counter-parties, commercial and financial documents, and transactions in order to identify OFAC-prohibited locations, parties, or dealings. At times, organizations have failed to update their sanctions screening software to incorporate updates to the SDN List or SSI List, failed to include pertinent identifiers such as SWIFT Business Identifier Codes for designated, blocked, or sanctioned financial institutions, or did not account for alternative spellings of prohibited countries or parties—particularly in instances in which the organization is domiciled or conducts business in geographies that frequently utilize such alternative spellings (i.e., Habana instead of Havana, Kuba instead of Cuba, Soudan instead of Sudan, etc.),

VII. Improper Due Diligence on Customers/Clients (e.g., Ownership, Business Dealings, etc.)

One of the fundamental components of an effective OFAC risk assessment and SCP is conducting due diligence on an organization's customers, supply chain, intermediaries, and counter-parties. Various administrative actions taken by OFAC involved improper or incomplete due diligence by a company or corporation on its customers, such as their ownership, geographic location(s), counter-parties, and transactions, as well as their knowledge and awareness of OFAC sanctions.

VIII. De-Centralized Compliance Functions and Inconsistent Application of an SCP

While each organization should design, develop, and implement its risk-based SCP based on its own characteristics, several organizations subject to U.S. jurisdiction have committed apparent violations due to a de-centralized SCP, often with personnel and decision-makers scattered in various offices or business units. In particular, violations have resulted from this arrangement due to an improper interpretation and application of OFAC's regulations, the lack of a formal escalation process to review high-risk or potential OFAC customers or transactions, an inefficient or incapable oversight and audit function, or miscommunications regarding the organization's sanctions-related policies and procedures.

IX. Utilizing Non-Standard Payment or Commercial Practices

Organizations subject to U.S. jurisdiction are in the best position to determine whether a particular dealing, transaction, or activity is proposed or processed in a manner that is consistent with industry norms and practices. In many instances, organizations attempting to evade or circumvent OFAC sanctions or conceal their activity will implement non-traditional business methods in order to complete their transactions.

X. Individual Liability

In several instances, individual employees—particularly in supervisory, managerial, or executive-level positions—have played integral roles in causing or facilitating violations of the regulations administered by OFAC. Specifically, OFAC has identified scenarios involving U.S.-owned or controlled entities operating outside of the United States, in which supervisory, managerial or executive employees of the entities conducted or facilitated dealings or transactions with OFAC-sanctioned persons, regions, or countries, notwithstanding the fact that the U.S. entity had a fulsome sanctions compliance program in place. In some of these cases, the employees of the foreign entities also made efforts to obfuscate and conceal their activities from others within the corporate organization, including compliance personnel, as well as from regulators or law enforcement. In such circumstances, OFAC will consider using its enforcement authorities not only against the violating entities, but against the individuals as well.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.²

Background on Ransomware Attacks

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a ransomware payment, usually through digital currency, in exchange for a key to decrypt the files and restore victims' access to systems or data.

In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.³ While ransomware attacks are carried out against large corporations, many ransomware attacks also target small- and medium-sized

¹ This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive or as imposing requirements under U.S. law, or otherwise addressing any particular requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

² This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners' cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Cybersecurity Unit, *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources* (February 2020), available at <https://www.justice.gov/criminal-ccips/page/file/1252341/download>.

³ Compare Federal Bureau of Investigation, Internet Crime Complaint Center, *2018 Internet Crime Report*, at 19, 20, available at https://pdf.ic3.gov/2018_IC3Report.pdf, with Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf.

businesses, local government agencies, hospitals, and school districts, which may be more vulnerable as they may have fewer resources to invest in cyber protection.

OFAC Designations of Malicious Cyber Actors

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. For example, starting in 2013, a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States.⁴ OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016.⁵

Starting in late 2015 and lasting approximately 34 months, SamSam ransomware was used to target mostly U.S. government institutions and companies, including the City of Atlanta, the Colorado Department of Transportation, and a large healthcare company. In November 2018, OFAC designated two Iranians for providing material support to a malicious cyber activity and identified two digital currency addresses used to funnel SamSam ransomware proceeds.⁶

In May 2017, a ransomware known as WannaCry 2.0 infected approximately 300,000 computers in at least 150 countries. This attack was linked to the Lazarus Group, a cybercriminal organization sponsored by North Korea. OFAC designated the Lazarus Group and two sub-groups, Bluenoroff and Andariel, in September 2019.⁷

Beginning in 2015, Evil Corp, a Russia-based cybercriminal organization, used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than \$100 million in theft. In December 2019, OFAC designated Evil Corp and its leader, Maksim Yakubets, for their development and distribution of the Dridex malware.⁸

OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.

⁴ Press Release, U.S. Dept. of Justice, U.S. Leads Multi-National Action Against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator (June 2, 2014), available at <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware>.

⁵ Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities (Dec. 29, 2016), available at <https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx>.

⁶ Press Release, U.S. Dept. of the Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), available at <https://home.treasury.gov/news/press-releases/sm556>.

⁷ Press Release, U.S. Dept. of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), available at <https://home.treasury.gov/news/press-releases/sm774>.

⁸ Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware (Dec. 5, 2019), available at <https://home.treasury.gov/news/press-releases/sm845>.

Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),⁹ U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities (“persons”) on OFAC’s Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations. OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

OFAC’s Economic Sanctions Enforcement Guidelines (Enforcement Guidelines)¹⁰ provide more information regarding OFAC’s enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. Under the Enforcement Guidelines, in the event of an apparent violation of U.S. sanctions laws or regulations, the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response (including the amount of civil monetary penalty, if any).

As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations.¹¹ This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services

⁹ 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.

¹⁰ 31 C.F.R. part 501, appx. A.

¹¹ To assist the public in developing an effective sanctions compliance program, in 2019, OFAC published *A Framework for OFAC Compliance Commitments*, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program. The *Framework* is available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.¹²

Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

OFAC Licensing Policy

Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.

Victims of Ransomware Attacks Should Contact Relevant Government Agencies

OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm's ability to perform critical financial services.

- U.S. Department of the Treasury's Office of Foreign Assets Control
 - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
 - Licensing Division: <https://licensing.ofac.treas.gov/>; (202) 622-2480
- U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
 - OCCIP-Coord@treasury.gov; (202) 622-3000
- Financial Crimes Enforcement Network (FinCEN)
 - FinCEN Regulatory Support Section: frc@fincen.gov

¹² See FinCEN Guidance, FIN-2020-A00X, "[Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments](#)," October 1, 2020, for applicable anti-money laundering obligations related to financial institutions in the ransomware context.

Contact Information for Other Relevant U.S. Government Agencies:

- Federal Bureau of Investigation Cyber Task Force
 - <https://www.ic3.gov/default.aspx>; www.fbi.gov/contact-us/field
- U.S. Secret Service Cyber Fraud Task Force
 - www.secretservice.gov/investigation/#field
- Cybersecurity and Infrastructure Security Agency
 - <https://us-cert.cisa.gov/forms/report>
- Homeland Security Investigations Field Office
 - <https://www.ice.gov/contact/hsi>

If you have any questions regarding the scope of any sanctions requirements described in this advisory, please contact OFAC's Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490.

OFAC QUESTIONS

True or False

- _____ 1. Nationally chartered financial institutions are the only institutions subject to the OFAC regulations.
- _____ 2. The Office of Foreign Asset Control (OFAC) is an agency within the Department of Treasury that administers economic sanctions enacted against hostile targets defined by regulation or statute.
- _____ 3. Funds transfers and currency transactions of \$3,000 or more are the only transactions blocked by OFAC sanctions.
- _____ 4. Blocked transactions are reported to OFAC within 10 calendar days of the transaction.
- _____ 5. Statutorily Denoted Nominees (SDNs) include individuals with whom financial institutions are prohibited from conducting transactions.
- _____ 6. OFAC compliance is examined as part of the financial institution's Bank Secrecy Act Examination.
- _____ 7. The SDN listing is the only federally provided list of terrorists that must be reviewed as part of the CIP (326) process.
- _____ 8. Financial institutions may, but are not required to purchase software products or use third-party vendors to ensure OFAC compliance.
- _____ 9. Community-sized financial institutions are allowed to use/default to their upstream correspondent banks and their installed OFAC software and OFAC filter systems to maintain the proper level of OFAC compliance.
- _____ 10. All assets and property blocked/held under OFAC sanctions are reported to OFAC on an annual basis using form TDF 90-22.50 (Annual Report of Blocked Property – Now in electronic format)
- _____ 11. Any transaction for any SDN must be blocked and prevented.
- _____ 12. OFAC liability can be contractually transferred to an ACH Originator by the ODFI assuming the compromise language is included within the Originator/ODFI agreement.
- _____ 13. OFAC Scrutiny of inbound IAT entries is limited to debit transactions only.
- _____ 14. The latest country removed from the OFAC "Country List" was the country of South Sudan.

(Blank Page)

CUSTOMER IDENTIFICATION PROCEDURES

After the terrorist attacks of September 11, 2001, Congress enacted the USA PATRIOT Act. Among other things, the Act added provisions to the Bank Secrecy Act (BSA) intended to facilitate the prevention, detection, and prosecution of international money laundering and the financing of terrorism. One of these new BSA provisions requires each bank to develop and implement a Customer Identification Program (CIP). In addition, banks must exercise enhanced due diligence regarding certain private banking and correspondent accounts, and respond to law enforcement requests under Section 314(a) of the Act.

CUSTOMER IDENTIFICATION PROGRAM

I. GENERAL REQUIREMENTS

A. CIP Required – Under Section 326 of the Act, each bank must establish a written Customer Identification Program (CIP) designed to ensure that it is able to form a reasonable belief that it knows the true identity of each customer within a reasonable period of time of account opening.

1. The CIP must be incorporated into the bank's anti-money laundering compliance program, which in turn must be approved by the board of directors.

NOTE: Section 352 of the USA PATRIOT Act allows banks to establish and maintain combined Bank Secrecy and Anti-Money Laundering Programs.

2. The written CIP must have been in place and operational no later than October 1, 2003.

B. Required Procedures – The CIP should be appropriate for the bank's size, location, and business operations. Each bank's CIP must be risk-based, taking into account the various types of accounts maintained, the various methods by which accounts are opened, and the different types of identifying information available from customers. The bank should also take into account its size, location, and type(s) of business or customer base it serves. The CIP must include procedures for:

1. Verifying the identity of any person seeking to open an account, to the extent reasonable and practicable.
2. Maintaining records of the information used to verify the person's identity.
3. Determining whether the person appears on any federal government-provided terrorist list.

C. CIP Required Components – Each bank's CIP must be risk-based and, at a minimum, must address:

1. Customer information required;
2. Customer verification (See FinCEN Advisory 2014-A004 for Guidance on St.Kitts and Nevis);

3. Customer notice;
4. Comparison with terrorist lists; and
5. Recordkeeping.

II. DEFINITIONS

A. Account – A formal banking relationship established to provide or engage in services, dealings, or other financial transactions, such as:

1. Deposit accounts;
2. Transaction or asset accounts;
3. Extensions of credit;
4. Safety deposit or other safekeeping services; and
5. Cash management, custodian, and trust services.

The term “account” does not include:

1. Products or services without a formal banking relationship, such as check-cashing, wire transfers, or sales of checks or money orders.
2. Accounts acquired through an acquisition, merger, purchase of assets, or assumption of liabilities.

NOTE: If the bank is extending credit to the borrower using a car dealer or mortgage broker as its agent, then it must ensure that the dealer or broker is performing the bank's CIP.

3. Accounts opened in order to participate in an ERISA-qualifying employee benefit plan.

B. Customer – For CIP purposes, a customer is:

1. A person that opens a new account, including each person named on a joint account.
2. An individual who opens a new account for an individual who lacks legal capacity, such as a minor.
3. An individual who opens a new account for an entity that is not a legal person, such as a civic club.

The term “customer” does not include:

1. Financial institutions regulated by a federal regulator or banks regulated by a state bank regulator.
2. Governmental departments, agencies, or entities that exercise governmental authority.

3. Any business whose common stock is listed on the New York or American Stock Exchanges, or whose common stock or interest has been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (except those listed under the separate heading “NASDAQ Small-Cap Issues”).
 4. A person who has an existing account with the bank, provided that the bank has a reasonable belief that it knows the true identity of the person.
- C. Taxpayer Identification Number (TIN)** – An identification number used by the Internal Revenue Service (IRS) in the administration of tax laws. There are four types of TINs:
1. Social Security Number (SSN).
 2. Individual Taxpayer Identification Number (ITIN) issued to foreign individuals who are not eligible for an SSN.
 3. Adoption Identification Number (ATIN).
 4. Employer Identification Number (EIN).
- D. Person** – An individual, corporation, partnership, trust or estate, joint stock company, association, syndicate, joint venture, or other unincorporated organization or group, Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities.

III. PROGRAM REQUIREMENTS

- A. Customer Information** – The CIP must include procedures for opening an account that specify the information that will be obtained from each customer in order to verify that customer’s identity. The identifying information the bank must obtain, at a minimum, is:

1. Name;
2. Date of birth (for individuals);
3. A residential or business street address; and

NOTE: If an individual does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number or the street address of the next of kin or of another contact individual may be used. Also, the number on the roadside mailbox on a rural route is acceptable as an address. For a person other than an individual (such as a corporation, partnership or trust) a principal place of business, local office or other physical location may be used.

NOTE: On January 12, 2010, FinCEN issued Ruling 2009-R003 which stated that a customer who participates in a state- created ACP shall be treated as not having a residential or business street address, and the Secretary of State or other state entity serving as a designated agent of the customer consistent with the terms of the ACP will act as “another contact

individual” for purposes of complying with the CIP rules. (State sponsored Address Confidentiality Programs (ACP) provide a substitute address (a post office box) for victims of domestic violence, sexual assault, and stalking, and help a participant keep his/her physical address confidential).

4. If the customer is a U.S. person (i.e., a U.S. citizen or entity that is established or organized under the laws of a State or the U.S.), a TIN. If the customer is a non-U.S. person, at least one of the following must be obtained:
 - a. a TIN;
 - b. a passport number and country of issuance;
 - c. an alien identification card number and country of issuance; or
 - d. any other government issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
5. When opening an account for a foreign business that does not have an identification number, the bank must request an alternative form of government issued documentation certifying the existence of the business.
6. In those instances where a person has applied for, but not received, a TIN, the CIP must include procedures to confirm the application was filed before the customer opens the account. The bank should obtain the TIN within a reasonable time after the account is opened.
7. In some situations, the bank may need to obtain a TIN for someone other than the customer. For example, if a court appointed guardian of a minor opens an account for the benefit of the minor, for CIP purposes the guardian is the customer and the bank must obtain the guardian’s TIN. However, for IRS reporting requirements, the minor’s TIN would also be needed since the funds are owned by the minor.
8. For a customer who opens a credit card account, the bank may obtain the identifying information about the customer from a third party source prior to extending credit to the customer.

B. Verification – The CIP must contain procedures for verifying the identity of the customer within a reasonable time after the account is opened, using the information obtained at account opening. A bank need not establish the accuracy of every element of identifying information obtained, but must do so for enough information to form a reasonable belief it knows the true identity of the customer. The procedures must describe when the bank will rely on documents, non-documentary methods or a combination thereof in verifying the identity of the customer.

1. When the bank will rely on documents, the CIP must specify the documents that the bank will use. These may include:
 - a. for an individual, unexpired government issued identification such as a driver’s license or passport evidencing nationality or residence and bearing a photograph or similar safeguard.

- b. for a person other than an individual, documents showing the existence of the entity such as certified articles of incorporation, a government issued business license, a partnership agreement or a trust instrument.
- 2. When the bank will rely on non-documentary methods, the CIP must describe the methods the bank will use. These methods may include:
 - a. contacting the customer;
 - b. independently verifying the customer's identity by comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source;
 - c. checking references with other banks; or
 - d. obtaining a financial statement from the customer.
- 3. Non-documentary procedures must also address situations where:
 - a. an individual is unable to present an unexpired government issued identification document bearing a photograph or similar safeguard;
 - b. the bank is not familiar with the documents provided by the customer;
 - c. the account is opened without obtaining documents;
 - d. the customer opens the account without appearing in person; and
 - e. there is an increased risk that the bank will be unable to verify the true identity of the customer through documents.
- 4. When the bank, using these methods, cannot verify the customer's true identity based on the bank's risk assessment of a new account opened by a customer that is not an individual, the bank must obtain information about individuals with authority or control over such account, including signatories, in order to verify the customer's identity. For example, a signatory for a corporation opens a new account for the corporation. The bank may obtain information about the signatory if the bank cannot verify the corporation's true identity using the bank's standard verification methods.
- 5. The CIP must also describe procedures for responding to situations where the bank cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe:
 - a. when the bank should not open an account;
 - b. the terms under which a customer may use an account while the bank attempts to verify the customer's identity;
 - c. when the bank should close an account; and

- d. when the bank should file a Suspicious Activity Report (SAR).

C. Customer Notice

- 1. The bank's CIP must provide customers with adequate notice that the bank is requesting information to verify their identities. Notice is adequate if the bank generally describes the identification requirements and provides notice in a manner reasonably designed to ensure that a customer is given, or is able to view, the notice prior to account opening.

NOTE: Notice must be provided to all owners of a joint account. The agencies agree that a bank may satisfy this requirement by directly providing notice to any one account holder of a joint account for delivery to the other owners of the account.

- 2. Depending upon the manner in which an account is opened, the bank may:
 - a. Post a notice in the lobby.
 - b. Post a notice on its web site.
 - c. Include the notice on its account applications.
 - d. Use any other form of written or oral notice.
- 3. Banks may use the following sample language to provide notice, if appropriate:

**IMPORTANT INFORMATION ABOUT PROCEDURES
FOR OPENING A NEW ACCOUNT**

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all banks to obtain, verify and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

- 4. When a mortgage broker or car dealer is acting as the bank's agent in connection with a loan, the bank may delegate to its agent the obligation to perform the requirements of the bank's CIP, including providing notice.

- D. Comparison with Government Lists** – The CIP must contain steps for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such. The bank must make this determination within a reasonable time after the account is opened, or earlier if required by another federal law.

E. Recordkeeping

1. The CIP must include procedures to make and maintain records of all information obtained under their CIP procedures. At a minimum, records maintained must include:
 - a. The identifying information obtained from a customer at account opening (name, address, TIN, and date of birth for individuals).
 - b. A description of any document relied upon, noting:
 - (1) the type of document;
 - (2) any identification number contained in the document;
 - (3) the place of issuance; and
 - (4) the date of issuance and expiration, if any.
 - c. A description of the methods and results of non-documentary methods of verification.
 - d. A description of the resolution of any discrepancy when verifying the identifying information obtained.
2. The bank must retain the identifying information for five years after the date the account is closed. Other required records must be kept for five years after the date the information is obtained.

NOTE: The CIP rule requires that a bank retain the identifying information obtained about the customer at the time of account opening.

3. With the enactment of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 (EGRRCPA), Section 213 added a “potentially conflicting” requirement pertaining to the destruction of certain images. Section 213 reads “In General, when an individual initiates a request through an online service to open an account with a financial institution or obtain a financial product or service from a financial institution, the financial institution may record personal information from a scan of the driver’s license or personal identification card of the individual, or make a copy or receive an image of the driver’s license or personal identification card of the individual , and store or retain such information in any electronic format”. The financial institution may only use this information to verify the identity of the individual and to comply with a legal requirement to record, retain, or transmit the personal information in connection with opening an account or obtaining a financial product or service. Section 3 introduces the “potential conflict”, as it reads, a financial institution after making a copy or receiving an image “shall after using the image for the purposes above, permanently delete the image and any copy of such, but it does not define “when” the DFI has “finished using the image” for the purposes detailed in the Act. As CIP allows, but does not require DFIs to retain an actual image of any documentary verification tools utilized, the statute is unclear as to whether we have “finished using” once we have recorded the numbers and dates from the government issued document, or if we may retain the image for five years after we have received such, meeting the CIP record retention requirement.

F. Reliance on Other Financial Institutions

1. The CIP may include procedures specifying when the bank will rely upon another financial institution (including an affiliate). The bank may rely on another financial institution to perform any procedures of the bank's CIP, regarding any customer that is opening or has opened an account, or that has established a similar formal relationship with the other financial institution, provided that:
 - a. the reliance is reasonable under the circumstances;
 - b. the other financial institution is subject to regulatory anti-money laundering program requirements; and
 - c. the other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP. In this instance, the bank will not be held responsible for noncompliance should the other financial institution not perform the requirements of the contract.
2. Banks may also contract with third parties or agents to perform their CIP; however, the bank will be responsible for any noncompliance by the third party or agent.

G. Frequently Asked Questions

1. In April 2005, FinCEN and the Federal regulators issued an additional set of "FAQs: Final CIP Rule" to provide interpretive guidance with respect to the CIP rule. Banks should obtain a copy of this guidance from their primary regulator, or directly from FinCEN.

H. CIP Examination Procedures

1. Contained within the current Interagency BSA/AML Examination Manual are the core examination procedures covering an institution's CIP program.
2. Highly qualitative and subjective in nature, the Federal examiner will form a conclusion about the ability of policies, procedures, and processes to meet the regulatory requirements associated with CIP by completing a number of reviews which include, but are not limited to:
 - a. Verify that the institution's policies, procedures, and processes include a comprehensive program for identifying clients who open an account after October 1, 2003;
 - b. Determine whether the institution's CIP considers the types of accounts offered, methods of account opening, and the institution's size, location, and client base;
 - c. Determine whether the institution's policy for opening new accounts appears reasonable;

- d. Review the board minutes to verify that the board of directors approved the CIP either separately or as part of the BSA/AML compliance program;
- e. Evaluate the institution's audit and training programs to ensure that CIP is adequately incorporated therein;
- f. Evaluate the institution's policies, procedures, and processes for verifying that all new accounts are checked against prescribed government lists of suspected terrorists on a timely basis, if such lists are issued;
- g. Select a sample of new accounts and perform transactional testing against the sample to review for compliance with all the facets and ingredients within CIP;
- h. Evaluate the level of CIP exceptions to determine whether the institution is effectively implementing its CIP. (An institution's policy may not allow staff to make or approve CIP exceptions);

I. Authentication in an Internet Banking Environment

- 1. On October 12, 2005, the five regulatory agencies authored the above guidance addressing the need for risk-based assessments, client awareness, and the development and implementation of new security measures to authenticate the identity of client's accessing a financial institution's internet-based services. The effective date of the guidance was 12/31/06.
- 2. On June 28, 2011, the four regulatory agencies issued a Supplement to the 2005 Guidance to reinforce the Guidance's risk management framework and update the Agencies' expectations regarding client authentication, layered security, or other controls in the increasingly hostile online environment. It established minimum control expectations for certain online banking activities, and it identified certain specific minimum elements that should be part of a DFI's client awareness and education program.

The "Effective Date" was 12/31/11 as examiners started to formally assess financial institutions under the enhanced expectations beginning in 01/2012.

- 3. Financial institutions offering internet-based products and services to their clients should use effective methods to authenticate the identity of clients using these products and services. As the agencies consider single-factor authentication to be inadequate for high-risk transactions involving access to client information or the movement of funds to other parties, financial institutions should implement layered security, or other controls reasonably calculated to minimize and mitigate those risks.
- 4. Institution's opening accounts on-line will have to enhance their CIP verification requirements with the new authentication requirements. Authentication/verification methods can include:

- a. Positive Verification – where the prospective “customer” answers a series of client specific client questions, and the answers are compared against the information contained in a trusted database (E.g. reliable credit report).
 - b. Logical Verification – ensuring that the information provided is logically consistent (E.g. telephone area code, zip code, and street addresses “match”).
 - c. Negative Verification – comparing the prospective client’s information against fraud databases.
5. BSA compliance personnel must reassess the CIP risk assessment to account for the changes encountered through the implementation of the new guidance.

J. Federal Banking Agencies and FinCEN Announce Exemption from Customer Identification Program Requirements for Premium Finance Loans. On October 05, 2020, FinCEN and the Federal Banking agencies issued an “Order” granting an exemption from customer identification program requirements implementing section 326 of the USA PATRIOT Act, for loans extended by banks (and their subsidiaries) subject to the jurisdiction of the Federal Banking Agencies to all customers to facilitate the purchases of property and casualty insurance policies, referred to as premium finance loans or premium finance lending. Premium finance loans provide short-term financing to business and non-business borrowers to facilitate their purchases of property and casualty insurance policies. According to FinCEN, these types of loans present a low risk of money laundering because of the purpose for which the loans are extended, and the limitation on the ability of a customer to use such funds for any other purpose, as the bank remits the loan proceeds to the insurance company directly, or through the agent or broker, not through the borrower.

FOREIGN CORRESPONDENT AND PRIVATE BANKING ACCOUNTS

- I. OVERVIEW** – Section 312 of the USA PATRIOT Act requires U.S. financial institutions to perform due diligence and, in some cases, enhanced due diligence, with regard to correspondent accounts established or maintained for foreign financial institutions and private banking accounts established or maintained for non-U.S. persons. These responsibilities are in addition to the Customer Identification Program (CIP) identification requirements and the Office of Foreign Asset Control (OFAC) requirements.

Sections 313 and 319(b) of the USA PATRIOT Act not only prohibit U.S. banks from maintaining account for foreign shell banks, but also require specific certifications and recordkeeping to remain in compliance with these sections.

II. FOREIGN CORRESPONDENT ACCOUNTS

- A. Definition** – Correspondent account is defined as an account established for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of the foreign financial institution, or to handle other financial transactions related to such foreign financial institution, and includes:

1. Demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit;
2. Purchase or sale of securities, and securities loaned and borrowed activity;
3. Contracts for sales of a commodity for future delivery, or options on a commodity; and
4. Contracts to effect transactions in securities issued by a mutual fund, including the purchase or sale of securities.

While this is a relatively broad definition, the definition requires a formal banking or business relationship through which the financial institution provides regular services, dealings or other financial transactions.

B. Regulations and Guidance

1. FinCEN Regulations:
 - a. 31 CFR 1010.100 and 31 CFR 103 1010.605 – Definitions.
 - b. 31 CFR 1010.610 – Due Diligence Foreign Correspondent Bank Accounts.
 - c. 31 CFR 1010.630 – Foreign Shell Bank Prohibition & Records concerning the owners of foreign banks and agents for service of legal process.
 - d. 31 CFR 1010.670 – Termination of correspondent relationships.
2. FinCEN Guidance:
 - a. 2006-G003 (February 3, 2006) – Foreign Bank Recertifications.
3. The above regulations and guidance detail the expectations imposed on domestic financial institutions that maintain an account with a foreign correspondent bank regarding:

- a. Records regarding the owner and agent of foreign banks whose shares are not publically traded;
 - b. The prohibition on establishing, maintaining, administering, or managing a correspondent account for, or on behalf of a foreign shell bank (a bank that has no physical presence in any country);
 - c. The establishment of due diligence policies, procedures, and controls reasonably designed to detect and report money laundering through these foreign correspondent accounts; and
 - d. The enhanced due diligence requirements imposed on domestic DFIs maintaining accounts with “special” foreign banks that took effect on 09/10/2007.
4. Due to the fines (up to \$ 1,000,000/per incident) for failure to comply with sections 313 and 319(b) of the USA PATRIOT Act, domestic DFIs maintaining correspondent accounts for the defined foreign banks should refer to these regulations and guidance to ensure proper compliance.

III. PRIVATE BANKING ACCOUNTS

A. Overview – The final rule requires certain U.S. financial institutions to establish and maintain a due diligence program that is reasonably designed to detect and report any known or suspected money laundering or suspicious activity through private banking accounts established, administered, or maintained for non- U.S. persons. Included in this requirement is the duty to conduct enhanced scrutiny of any private banking account that is maintained for senior foreign political figures, their immediate family members, or persons widely and publicly known to be close associates of such individuals.

B. Definition – A private banking account subject to enhanced due diligence is any account (or any combination of accounts) that meets all of the following criteria:

1. Require a minimum aggregate deposits or other assets of not less than \$1 million;
2. Is established on behalf of or for the benefit of one or more non- U.S. persons who are direct or beneficial owners of the account; and
3. Is assigned to, or administered or managed (at least in part) by, an officer, employee, or agent of the bank acting as liaison between the bank and the nominal or beneficial owner of the account.

Significantly, if an account otherwise satisfies the definition of a private banking account, but the institution does not require a minimum balance of \$1,000,000, then the account does not qualify as a private banking account for purposes of Section 312. However, the account is subject to the internal controls and risk-based due diligence included in the institution’s general anti-money laundering program.

NOTE: Non-U.S. Person is defined as a Natural Person who is neither a United States Citizen nor is accorded the privilege of residing permanently in the United States pursuant to Title 8 of the United States Code.

C. Requirements

1. U.S. financial institutions covered by the final rule are required to establish and maintain a due diligence program that includes policies, procedures, and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving any private banking account that is established, maintained, administered, or managed in the United States.
2. Financial institution covered by the final rule must take reasonable steps to:
 - a. Determine the identity of all nominal and beneficial owners of the private banking account;
 - b. Determine whether any such owner is a senior foreign political official and, thus, is subject to enhanced scrutiny;
 - c. Determine the source(s) of funds deposited into the private banking account and the purpose and expected use of the account; and
 - d. Review the activity of the account to ensure that the activity is consistent with the information obtained about the source of funds, the stated purpose, and expected use of the account as needed to guard against money laundering, and to report any suspicious activity.
3. A “senior foreign political figure” (PEP) is defined as a:
 - a. Current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials;
 - b. Senior executive of a foreign government-owned commercial enterprise. (This definition also includes a corporation, business, or other entity formed by or for the benefit of such an individual. Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources); and
 - c. Immediate family member of a senior foreign political figure, as well as those who are widely and publicly known (or actually known) close associates of a senior foreign political figure.
4. The final rule requires the application of enhanced scrutiny to private banking accounts maintained for senior foreign political figures. Enhanced scrutiny must include procedures reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption. The final rule defines such proceeds as “any asset acquired by, through, or on behalf of a senior foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and include any other property into which any such assets have been transformed or converted.”

D. Implications to the Institution

1. As these types of account relationships pose higher risk, examination procedures look to determine if management has performed due diligence on customers and transactions which include:

- a. Documenting the beneficial owner(s);
 - b. Obtaining information on the client's source of income, line of business and sources of wealth;
 - c. Obtaining references from known third parties;
 - d. Verifying the standing of business customers;
 - e. Contacting/verifying visits to the business ; and
 - f. Monitoring transaction activity and reporting suspicious transactions.
2. If the account is maintained for a non-U.S. person, the institution should:
- a. Identify the beneficial owner(s) of the account, as well as the source of funds deposited;
 - b. Increase scrutiny of accounts maintained by or on behalf of senior foreign political figures, or family members, or associates; and
 - c. Monitor the accounts to detect and report money laundering and the existence of the proceeds of foreign corporation.

IV. BENEFICIAL OWNERSHIP

FinCEN Guidance 2010-G001 (03/05/10) reminded DFIs that heightened risks can arise with respect to beneficial owners of accounts, as nominal account holders can enable individuals and business entities to conceal the identity of the true owner of assets or property derived from or associated with criminal activity. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) could be applied to ALL private banking accounts (not just those defined under Section 312 above), to ALL foreign correspondent accounts, and to ALL accounts for PEPs. DFIs are encouraged to determine whether any client is acting as an agent for or on behalf of another, obtain information about the structure or ownership of an entity that is not publicly traded in the U.S., and obtain information about the trust structure where the client themselves is the trustee. (The final rule issued on 05/11/16 on “Customer Due Diligence for Financial Institutions” imposes mandatory beneficial ownership requirements on DFIs beginning May 11, 2018 – See Chapter 9).

314(a) and 314(b) INFORMATION REQUESTS

- I. OVERVIEW** – Section 314(a) of the USA PATRIOT Act authorizes law enforcement authorities to communicate with banks about suspected money launderers and terrorists. Periodically, FinCEN distributes notifications alerting institutions to the existence of lists of "subjects of interests" which law enforcement has requested information about. Once the notification is received, the institution's "Point-of-Contact" (POC) goes to FinCEN's secure communication system at www.fincen.gov/314a/ to download the list and begin the required search.

NOTE: On February 10 2010, FinCEN published the final rule which amended the 314(a) process to allow certain foreign law enforcement agencies, state and local law enforcement agencies, and FinCEN itself to submit requests for information to financial institutions (75 FR 6560-6570).

II. REQUIREMENTS

- A. Search Requirement** – A bank is required to search its records to determine whether it, at the head office or any U.S. branch, maintains or has maintained accounts for, or has engaged in transactions with, any individual, entity, or organization (named subject) listed in the 314(a) request.

B. Timing

1. The bank must begin searching its records immediately upon retrieving the request. If a notification is received during non-business hours or during the weekend, the bank must commence its search the next business day.
2. If a match is found with a named subject, the match must be reported to FinCEN via the secure communication system. Unless the instructions to a request state otherwise, banks must complete their search on all subjects listed in the request and respond with any matches no later than 14 calendar days after receiving the request.

C. Records Search

1. Using the identifying information contained in the request, the bank must conduct a search of the following records:
 - a. Deposit account records to determine whether a named subject is or was an accountholder.
 - b. Funds transfer records maintained pursuant to BSA regulations to determine whether a named subject was an originator/transmittor of a funds transfer for which the bank was the originator/transmittor's bank, or a beneficiary/recipient of a funds transfer for which the bank was the beneficiary/recipient's bank.
 - c. Records of the sale of monetary instruments maintained pursuant to BSA regulations to determine whether a named subject purchased a monetary instrument.

- d. Loan records to determine whether a named subject is or was a borrower.
 - e. Trust department account records to determine whether a named subject matches the name in which an account is titled.
 - f. Records of accounts to purchase, sell, lend, hold, or maintain custody of securities to determine whether a named subject is or was an accountholder.
 - g. Commodity futures, options, or other derivatives account records to determine whether a named subject is or was an accountholder.
 - h. Safe deposit box records to determine whether a named subject maintains or maintained, or has or had authorized access to, a safe deposit box, but only if such safe deposit box records are searchable electronically.
- 2. All of the above records must be searched whether or not they are maintained electronically, except:
 - a. safe deposit records are only required to be searched if they are searchable electronically; and
 - b. any record that is not maintained in electronic form need only be searched if it is required to be kept under federal law or regulation.
 - 3. The normal search of the records described above must encompass current accounts and accounts maintained by a named subject during the preceding 12 months, and transactions that are not linked to an account that are conducted by a named subject during the preceding six months.

D. Matches

- 1. If a match is found, the search on that subject should be stopped. The records search should continue for an account or transaction matching any of the other named subjects.
- 2. After the search for all of the named subjects listed in the request has been completed, any match must be reported to FinCEN by logging back into the secure communications system, and following the notification procedures.
- 3. The bank is not required to close any account or take any other action with respect to a match. The bank should not maintain the list of named subjects for the purpose of evaluating whether to open an account or to conduct a transaction, unless specific instructions in accompanying the request state otherwise.
- 4. The decision to close or keep open an account due to a match rests with the bank. Should the bank choose to close any account pertaining to a 314(a) request, it is encouraged to first notify the law enforcement contact on the request to determine if closing the account would interfere with an active investigation. (If law enforcement requests that an account remain open, the bank should request written confirmation.)

5. A match does not automatically require the filing of a SAR. The bank should review the transactions relating to the named subject to determine if a SAR should be filed based on the totality of the circumstances and account activity.
6. A positive response to a 314(a) request may result in the bank receiving a grand jury subpoena, a National Security Letter (a request from the FBI or other government authority for a matter relating to terrorism) or an Administrative Summons.
 - a. In the case of an Administrative Summons, the bank must obtain a certification of compliance with the Right to Financial Privacy Act from the federal law enforcement agency that issued the summons.
7. Banks shall maintain adequate procedures to protect the security and confidentiality of these requests from FinCEN. Application of the procedures established to satisfy the customer information security program requirements of the Gramm-Leach-Bliley Act will satisfy the security requirements of Section 314(a).
8. Appropriate documentation of the request and record search should be maintained for a reasonable period of time to provide for an effective and examination trail.

E. Point of Contact Information - Section 314(a)

1. To update, change, add, or delete your financial institution's Point of Contact information on FinCEN's distribution list for receiving Section 314(a) Information Requests, banks should contact their primary Federal Supervisory Agency. Financial Institutions subject to supervision by one of the five Federal "Banking" regulators should also provide information for Section 314(a) Points of Contact on the institution's quarterly call or thrift financial report.
2. For a listing of the current federal agency contacts, see FinCEN Guidance on "Changing Your Point of Contact for 314(a)" located at www.fincen.gov/statutes_regs/patriot/pdf/poc_change_314a.pdf.

F. Examination Procedures

1. Contained within the current Interagency BSA/AML Examination Manual are the core examination procedures covering an institution's 314(a) program.
2. Highly qualitative and subjective in nature, the Federal examiner will form a **conclusion** about the ability of policies, procedures, and processes to meet the regulatory requirements associated with information sharing by completing a number of reviews which include, but are not limited to:
 - a. Verify that the institution has sufficient policies, procedures, and processes to document compliance, maintain sufficient internal controls, provide ongoing training, and independently test its compliance with the Section 314(a) requirements;

- b. Determine whether the search policies, procedures and processes the institution uses to respond to Section 314(a) requests are comprehensive, and cover all records identified to be searched;
 - c. Review the institution's internal controls and determine whether the institution's documentation to evidence compliance with Section 314(a) requests is adequate, and could include the following:
 - i. Copies of the 314(a) requests.
 - ii. A log that records the tracking numbers and includes a sign-off column.
 - iii. Copies of SISS – Generated Search Self-Verification documents.
 - iv. For positive matches, copies of the form returned to FinCEN and the supporting documentation should be retained.
- NOTE:** In November 2007, FinCEN launched a voluntary “Search Self-Verification” Tool at the “Secure Information Sharing System” web-site. This tool allows financial institutions to self-verify that the transmission subject information has been searched against their records. Internal audit should still consider applying transaction testing to the entire 314(a) process to ensure that the proper searches are conducted in a timely manner.
- d. Select a sample of positive matches or recent requests to determine that the institution searches the appropriate records, and that the institution uses information only in the manner and for the purposes allowed and keeps the information secure and confidential;
 - e. If the financial institution uses a third-party vendor to perform or facilitate searches, determine whether an agreement or procedures are in place to ensure confidentiality.

III. SHARING INFORMATION WITH OTHER FINANCIAL INSTITUTIONS – Section 314(b) permits two or more financial institutions, and any association of financial institutions, to share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering activities, or that may involve the proceeds of one or more specified unlawful activities (SUAs). Section 314(b) establishes a safe harbor from liability for a financial institution that chooses to share information with other financial institutions for the purpose of identifying and, where appropriate, reporting possible money laundering or terrorist activity.

A. How to Share

1. Financial institutions must first provide notice to FinCEN of its intent to share information with other financial institutions, even affiliates. Financial institutions may file the notification form electronically on the FinCEN website at www.fincen.gov/314b/314b_notification.php.

B. Duration

1. The notification lasts one year. To continue sharing information after the expiration of the one-year period, an institution must submit a new notification form.

C. Confirmation Regarding Sharing

1. Prior to sharing information with other financial institutions, an institution must take reasonable precautions to confirm that its counterpart has filed notice with FinCEN by:
 - a. verifying that the other institution appears on a list compiled by FinCEN; or
 - b. directly contacting the institution to determine whether the notice has been filed.

D. Use of Information

1. Only information related to suspected money laundering or terrorism will be protected upon disclosure. Financial institutions may use it only in connection with a decision to close or maintain an account or to engage in a transaction or to assist the institution in complying with BSA regulations.

E. Protection of Information

1. Financial institutions are required to maintain adequate procedures to protect the security and confidentiality of information requests from law enforcement and other institutions. Compliance with the Gramm-Leach-Bliley Act requirements regarding the protection of customer's non-public personal information will suffice.

F. Guidance

In December 2020, FinCEN published an updated Section 314b "Fact Sheet" detailing benefits and the procedures to follow to participate in the information sharing between financial institutions program.
(www.fincen.gov)

ANTI-MONEY LAUNDERING PROGRAM FOR INSURANCE COMPANIES AND REQUIREMENT THAT INSURANCE COMPANIES REPORT SUSPICIOUS TRANSACTIONS

I. GENERAL REQUIREMENTS

- A. AML Required** - Each insurance company shall develop and implement a written anti-money laundering program applicable to its covered products that is reasonably designed to prevent the insurance company from being used to facilitate money laundering or the financing of terrorist activities.
1. The program must be approved by senior management, and a copy of the program made available to FinCEN or their designee upon request.
 2. The effective date of the Final Rule was December 5, 2005. The written program had to be in place and operational no later than May 2, 2006.
- B. SAR Required** - Each insurance company shall file a report of any suspicious transaction involving a covered product that is relevant to a possible violation of law or regulation. An insurance company may also file a report of any suspicious transaction that it believes is relevant to the possible violation of any other law or regulation not required by this section.
1. The effective date of the SAR Rule was December 5, 2005. The filing of the SAR was required for appropriate transactions occurring after May 2, 2006.

II. DEFINITIONS

- A. Annuity Contract** - Any agreement between the insurer and the contract owner whereby the insurer promises to pay out a fixed or variable income stream for a period of time.
- B. Covered Product** - The term “covered product” means:
1. A permanent life insurance policy other than a group life insurance policy;
 2. An annuity contract, other than a group annuity contract; and
 3. Any other insurance product with features of cash value or investment.
- C. Insurance Agent** - A sales and/or service representative of an insurance company. The term “insurance agent” encompasses any person that sells, markets, distributes, or services an insurance company’s covered products, including but not limited to, a person who represents more than one insurance company, and a bank or broker-dealer in securities that sells any covered product of an insurance company.
- D. Insurance Broker** - A person who, by acting as the customer’s representative, arranges and/or services covered products on behalf of the customer.

- E. Insurance Company or Insurer** – Any person engaged within the United States as a business in the issuing or underwriting of any covered product. The terms “insurance company” or “insurer” do not include an insurance agent or broker.
- F. Permanent Life Insurance Policy** – An agreement that contains a cash value or investment element and that obligates the insurer to indemnify or to confer a benefit upon the insured or beneficiary to the agreement contingent upon the death of the insured.

III. IMPACTS ON BANKS, SAVINGS AND LOANS, AND CREDIT UNIONS

These AML requirements apply to insurance companies as defined. Insurance companies typically conduct their sales operations through agents. Some elements of the compliance program will best be performed by those agents, in which case it is permissible for an insurance company to make appropriate arrangements with an agent to perform aspects of its AML program. (The insurance company remains responsible for the effectiveness of its program as well as for ensuring that the appropriate examiners have access to information and records relating to the AML program and are able to inspect the agent of the third party for purposes of the program).

Under the terms of the final SAR rule, the obligation to identify and report suspicious transactions applies only to an insurance company, and not its agents or brokers. Nevertheless, because insurance agents and brokers are an integral part of the insurance industry due to their direct contact with customers, the final rule requires an insurance company to establish and implement policies and procedures reasonably designed to obtain customer information necessary to detect suspicious activity from all relevant sources, including from its agents and brokers, and to report suspicious activity based on such information.

Banks, Savings and Loans, and Credit Unions who have “dual” employees who also serve as insurance agents for insurance companies, can expect procedural and operational changes as a result of these AML and SAR reporting requirements.

IV. FINAL RULES

AML Programs for Insurance Companies – 70FR66754 – 66761
SAR Requirements for Insurance Companies – 70FR 66761 - 66901

V. “RED FLAGS” - Below are examples of potentially suspicious insurance transactions.

- A.** Using insurance proceeds from an early policy surrender to purchase other financial assets;
- B.** Purchasing insurance products through unusual methods such as currency or currency equivalents;
- C.** Buying policies that allow the transfer beneficial interests without the knowledge and consent of the issuer (e.g., secondhand endowment and bearer insurance policies);
- D.** Buying products with insurance termination features without concern for the products investment performance;

- E.** Selling units in investment-linked products (such as annuities);
- F.** Borrowing against the cash surrender value of permanent life insurance policies particularly when payments are made to apparently unrelated third-parties;
- G.** Rescission "abuse" where they exercise their rights in order to obtain "clean" money in return;
- H.** Purchasing product(s) that appear outside the client's normal range of financial wealth or estate planning needs; and
- I.** Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.
- J.** A client uses multiple currency equivalents (e.g., cashiers checks and money orders from different banks and money services/businesses) to make insurance policy or annuity payments.

VI. EXAMINATION PROCEDURES

- A.** Contained within the current Interagency BSA/AML Examination Manual are the expanded examination procedures covering an institution's insurance sales program.
- B.** Highly qualitative and subjective in nature, the Federal examiner will form a conclusion about the ability of policies, procedures, and processes to manage the risks associated with the sale of covered insurance products by completing a number of reviews which include, but are not limited to:
 1. Evaluate the adequacy of the policies, procedures, and processes given the institution's insurance sales activities, its role in insurance sales, and the risks the insurance sales present. Assess whether the controls are adequate to reasonably protect the institution from money laundering and terrorist financing;
 2. Depending on the institution's responsibilities as set forth in the contracts and agreements, review MIS reports (E.g. large transaction reports, single premium payments, early policy cancellation records, premium overpayments, and assignments of claims) and internal risk rating factors to determine whether the institution effectively identifies and monitors covered insurance sales;
 3. Depending on the institution's responsibilities as set forth in the contracts and agreements, determine whether the institution's system for monitoring covered insurance products for suspicious activities is adequate, given the institution's size, complexity, location, and types of client relationships;
 4. Where appropriate, select a sample of covered insurance products and perform transactional testing.

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
U.S. Department of the Treasury**

August 30, 2016

**U.S. Department of the Treasury and Federal Banking Agencies
Joint Fact Sheet on Foreign Correspondent Banking:
Approach to BSA/AML and OFAC Sanctions Supervision and Enforcement**

The global financial system, trade flows, and economic development rely on correspondent banking relationships. To protect this system from abuse, U.S. financial institutions must comply with national anti-money laundering (AML) and countering the financing of terrorism requirements set forth in the Bank Secrecy Act (BSA) as well as sanctions programs administered by the Treasury Department's Office of Foreign Assets Control (OFAC). The Financial Crimes Enforcement Network (FinCEN), a bureau of the Treasury Department, is responsible for administering the BSA in furtherance of its mission to safeguard the U.S. financial system from illicit use. The Federal Banking Agencies (FBAs) have the responsibility and authority to conduct examinations of depository institutions for compliance with the BSA and OFAC requirements in order to ensure the safety and soundness of the U.S. financial system. Together, these agencies are responsible for implementing the strong regulatory and supervisory framework that is essential for promoting compliance with these obligations and keeping our U.S. banking system safe and sound.

U.S. depository institutions that maintain correspondent accounts for foreign financial institutions (FFI) are required to establish appropriate, specific, and risk-based due diligence policies, procedures, and processes that are reasonably designed to assess and manage the risks inherent with these relationships. To comply with their legal obligations, U.S. depository institutions must monitor transactions related to these accounts to detect and report suspicious activities. These policies, procedures, and processes will depend on the level of risk posed by the correspondent FFI. Such risks can vary depending on the FFI's strategic profile, including its size and geographic locations, the products and services it offers, and the markets and customer bases it serves.

The Treasury Department and the FBAs communicate expectations regarding BSA and OFAC compliance in a number of ways including, the FBA examination process, the issuance of rules and regulations, the issuance of supervisory guidance, and through regular participation in organized public events focusing on these issues. This fact sheet summarizes key aspects of federal supervisory and enforcement strategy and practices in the area of correspondent banking.

The vast majority (about 95%) of BSA/OFAC compliance deficiencies identified by the FBAs, FinCEN, and OFAC are corrected by the institution's management without the need for any enforcement action or penalty.

Federal Banking Agencies' Expectations for U.S. Depository Institutions

The FBAs expect U.S. depository institutions to have robust BSA and OFAC compliance programs that include appropriate customer due diligence so that the institutions have a clear understanding of FFI risk profiles and expected account activity. This information helps U.S. depository institutions make informed decisions regarding the risks associated with their FFI relationships and the level and nature of suspicious activity monitoring needed to manage those risks effectively.

In order for U.S. depository institutions to develop a clear understanding of FFI risk profiles and determine how best to manage the risks associated with these relationships, they are expected to obtain and review sufficient information about their FFI relationships, including the types of customers the FFI serves and the markets in which the FFI is active. This approach allows the U.S. depository institution to conduct an adequate assessment of the risks present in: (i) the FFI's business and markets, (ii) the type, purpose and anticipated activity, (iii) the nature and duration of the relationship with the FFI, and (iv) the supervisory regime of the jurisdiction in which the FFI is licensed, and to design and implement controls to manage these risks effectively.

Under existing U.S. regulations, there is no general requirement for U.S. depository institutions to conduct due diligence on an FFI's customers. In determining the appropriate level of due diligence necessary for an FFI relationship, U.S. depository institutions should consider the extent to which information related to the FFI's markets and types of customers is necessary to assess the risks posed by the relationship, satisfy the institution's obligations to detect and report suspicious activity, and comply with U.S. economic sanctions. This may require U.S. depository institutions to request additional information concerning the activity underlying the FFI's transactions in accordance with the suspicious activity reporting rules and sanctions compliance obligations.

FBAs' Supervisory Examination Processes

The FBAs apply a risk-based approach to supervision in order to allocate supervisory resources appropriately based on money laundering and terrorist financing risks identified in the supervised institutions. The FBAs' risk-based approach to the examination process guides the scoping, planning and transaction testing portions of federal depository institutions' BSA and OFAC examinations.

The examination process, including the interaction between the examiners and the bank, is integral to the process of ensuring compliance with the BSA and OFAC sanctions programs. These supervisory communications can spur remediation, and indeed, in the vast majority of instances, deficiencies identified during the examination process are resolved promptly after they are brought to the attention of a depository institution's management through the issuance of confidential reports of examination and supervisory letters that contain specific language communicating supervisory findings to the institution.

In cases where prompt remedial action is not taken by management, the corrective action is not effectively implemented or the deficiencies are more serious, the FBAs can consider a range of steps to ensure that actions are implemented or deficiencies are successfully addressed. These

options can vary in levels of severity, allowing the agencies to consider their supervisory responses relative to the seriousness of the identified deficiencies in the particular depository institution. This range of options allows the FBAs flexibility in targeting their supervisory responses to remediate any deficiencies identified. The vast majority of BSA/AML compliance deficiencies identified by the FBAs—approximately 95%—are resolved through the supervisory process without the need for an enforcement action.

FBA Enforcement Actions

Enforcement actions by the FBAs are an extension of the supervisory process and are used to address more serious deficiencies, or situations where deficiencies have not been corrected in the course of the supervisory process.

Enforcement actions reinforce awareness of senior management and boards of directors of the deficiencies identified during the supervisory process and ensure they take prompt remedial actions to correct the identified deficiencies. Enforcement tools may vary and can include informal memoranda of understanding, or formal, public, written agreements, and cease-and-desist orders. The FBAs are required by statute to use their cease-and-desist authority when an institution fails to establish or maintain a BSA compliance program or fails to correct any problem with the program previously reported to the institution. In very limited instances, when corrective action has not been achieved within a reasonable amount of time or serious violations or unsafe or unsound practices or breaches of fiduciary duty have been identified, the FBAs also have the authority to assess civil money penalties (CMPs). CMPs are designed by statute to serve as a deterrent to future violations, practices or breaches of fiduciary duty, to encourage correction of violations, practices or breaches of fiduciary duty, and in the case of individual actions, to emphasize the accountability of individuals.

FinCEN and OFAC

FinCEN and OFAC are also essential to the effectiveness of the U.S. BSA/AML framework and sanctions regime. FinCEN has independent enforcement authority to impose CMPs and may seek equitable relief against financial institutions for non-compliance with the BSA. OFAC administers and enforces the U.S. economic and trade sanctions programs based on U.S. foreign policy and national security threats. In cases where institutions are supervised by the FBAs, the FBAs examine for BSA/AML and OFAC compliance, and in situations involving apparent BSA/AML or sanctions violations resulting from deficiencies, FinCEN and OFAC coordinate with the FBAs. In determining whether an enforcement action is appropriate, FinCEN considers whether the institution responded adequately to the FBA's previous corrective actions or if the institution engaged in significant violations. Similarly, in certain circumstances, OFAC will consult with relevant FBAs regarding the quality and effectiveness of an institution's compliance program when determining the appropriate enforcement response. OFAC investigates cases of sanctions violations, many of which (over 95 percent) are closed with administrative measures,

Criminal Enforcement

In addition to FBA, FinCEN, and OFAC enforcement actions, financial institutions may also be subject to criminal enforcement actions by the U.S. Department of Justice. Criminal prosecutions for BSA/AML and sanctions violations are typically brought against financial institutions only when there is sufficient evidence of willful wrongdoing.

such as cautionary or no action letters. This means that less than five percent of all cases of sanctions-related violations investigated by OFAC have resulted in a civil monetary penalty or other public enforcement response.

Recent Large FBA, FinCEN, and OFAC Enforcement Penalties

Over the past several years, certain major enforcement cases involved large enforcement penalties related to BSA/AML and OFAC sanctions. It is important to note that the largest and most prominent monetary penalties for BSA/AML and sanctions violations in recent years generally involved a sustained pattern of serious violations on the part of depository institutions. With regard to the sanctions violations, these cases did not involve unintentional mistakes, but generally involved intentional evasion of U.S. sanctions over a period of years and/or the failure of the institutions' officers and/or senior management to respond to warning signs that their actions were illegal. Many of these major cases also involved criminal conduct that was prosecuted separately by the Department of Justice.

Conclusion

The goal of BSA compliance programs and OFAC sanctions programs is to ensure a well-functioning, transparent, resilient, and safe and sound financial system. While the Treasury and the FBAs do not utilize a zero tolerance philosophy that mandates the strict imposition of formal enforcement action regardless of the facts and circumstances of the situation, Treasury and the FBAs take the threats posed by criminals, money-launderers, and terrorist financiers very seriously, and continue to use their authorities—in a proportionate and appropriate manner—to safeguard our financial system against abuse.

###



Section 314(b) Fact Sheet

FinCEN previously issued a Section 314(b) Fact Sheet in November 2016. This new fact sheet replaces that previous guidance, and also rescinds a previous piece of guidance FIN-2009-G002 (the “2009 Guidance”).¹ A previous published administrative ruling, FIN-2012-R006 (the “2012 Administrative Ruling”), has also been rescinded.^{2, 3} The discussion related to the scope of the regulatory definition of associations of financial institutions contained in the 2012 Administrative Ruling is reaffirmed and expanded on by this guidance.

What is Section 314(b)?

Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report activities that may involve money laundering or terrorist activities. Participation in information sharing pursuant to Section 314(b) is voluntary, and FinCEN strongly encourages financial institutions to participate.

What are the Benefits of 314(b) Voluntary Information Sharing?

While information sharing pursuant to Section 314(b) is voluntary, it can help financial institutions enhance compliance with their anti-money laundering/counter-terrorist financing (AML/CFT) requirements, most notably with respect to:

- Gathering additional information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals.

1. FinCEN Guidance – Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act (June 16, 2009), <https://www.fincen.gov/resources/advisories/fincen-guidance-fin-2009-g002>.
2. FinCEN Guidance - Administrative Ruling Regarding the Participation of Associations of Financial Institutions in the 314(b) Program (July 25, 2012), <https://www.fincen.gov/sites/default/files/shared/FIN-2012-R006.pdf>.
3. Pursuant to 31 CFR § 1010.716(a)(3), FinCEN may modify or rescind any ruling made pursuant to its administrative ruling authority for good cause. FinCEN has engaged in regular dialogue with financial institutions about the efficacy of the Section 314(b) program and determined there is good cause to provide updated guidance to improve the effectiveness of the Section 314(b) program consistent with the statutory text and legislative intent. This updated guidance is consistent with Section 314(b) and its implementing regulations and FinCEN has determined that it will enhance the program's contribution to the fight against terrorist financing and money laundering.

December 2020

- Shedding more light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.
- Building a more comprehensive and accurate picture of a customer's activities that may involve money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring.
- Alerting other participating financial institutions to customers of whose suspicious activities they may not have been previously aware.
- Facilitating the filing of more comprehensive SARs than would otherwise be filed in the absence of 314(b) information sharing.
- Identifying and aiding in the detection of money laundering and terrorist financing methods and schemes.
- Facilitating efficient SAR reporting decisions - for example, when a financial institution obtains a more complete picture of activity through the voluntary information sharing process and determines that no SAR is required for transactions that may have initially appeared suspicious.⁴

Who is Eligible to Participate in Section 314(b) Information Sharing?

Financial institutions subject to an anti-money laundering program requirement under FinCEN regulations, and any association of such financial institutions, are eligible to share information under Section 314(b). This currently includes the following types of financial institutions:

- Banks (31 CFR 1020.540)
- Casinos and Card Clubs (31 CFR 1021.540)
- Money Services Businesses (31 CFR 1022.540)
- Brokers or Dealers in Securities (31 CFR 1023.540)
- Mutual Funds (31 CFR 1024.540)
- Insurance Companies (31 CFR 1025.540)
- Futures Commission Merchants and Introducing Brokers in Commodities (31 CFR 1026.540)

4. For more information on the benefits of voluntary information sharing under Section 314(b), including examples of ways in which SAR narratives have referenced 314(b), see Issue 23 of the SAR Activity Review – Trends, Tips & Issues at https://www.fincen.gov/sites/default/files/sar_report/sar_tti_23.pdf.

December 2020

- Dealers in Precious Metals, Precious Stones, or Jewels (31 CFR 1027.540)
- Operators of Credit Card Systems (31 CFR 1028.540)
- Loan or Finance Companies (31 CFR 1029.540)
- Housing Government Sponsored Enterprises (31 CFR 1030.540)
- Associations consisting of the financial institutions listed above⁵

What Information can be Shared Pursuant to 314(b)?

As noted above, this fact sheet revokes the 2009 Guidance, the 2012 Administrative Ruling, and the prior version of this fact sheet issued in November 2016.

Financial institutions or associations of financial institutions may share information with each other regarding individuals, entities, organizations, and countries for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering. Information sharing among financial institutions is critical to identifying, reporting, and preventing crime.

Specifically, financial institutions or an association of financial institutions sharing information under the safe harbor created by Section 314(b) may share information relating to activities that a financial institution or association suspects may involve possible terrorist financing or money laundering. This may occur, for instance, when the financial institution or association is sharing information about specific transactions involving the proceeds of one or more specified unlawful activities (“SUA”), as described in 18 U.S.C. § 1956, which lists the predicate crimes that apply to a money laundering offense. The SUAs listed in 18 U.S.C. § 1956 include an array of fraudulent and other criminal activities, including fraud against individuals, organizations, or governments, computer fraud and abuse, and other crimes.

However, to rely on the Section 314(b) safe harbor, a financial institution or an association of financial institutions need not have specific information indicating that the activity in regards to which it proposes to share information directly relates to proceeds of an SUA or to transactions involving the proceeds of money laundering, nor must a financial institution or association have reached a conclusive determination that the activity is suspicious. Instead, it is sufficient that the financial institution or association has a reasonable basis to believe that the information shared relates to activities that may involve money laundering or terrorist activity, and it is sharing the information for an appropriate purpose under Section 314(b) and its implementing regulations. Therefore a financial institution or association can

5. FinCEN provides further guidance below on the types of permissible associations of financial institutions

December 2020

share information in reliance on the Section 314(b) safe harbor relating to activities it suspects may involve money laundering or terrorist activity, even if the financial institution or association cannot identify specific proceeds of an SUA being laundered.

Furthermore, a financial institution or an association of financial institutions may, in reliance on the Section 314(b) safe harbor, share information related to activities that may involve possible terrorist activity or money laundering even if such activities do not constitute a “transaction,” as defined in 31 CFR 1010.100(bbb) or elsewhere. For example, a financial institution or association may share information on *attempts* to engage in transactions that the financial institution or association suspects may involve money laundering or terrorist activity and the financial institution or association is sharing the information for an appropriate purpose under Section 314(b) and its implementing regulations. By the same reasoning, a financial institution or association may share information on attempts to induce others to engage in transactions, such as in a money mule scheme, where the other conditions of Section 314(b) are satisfied.

Section 314(b) and its implementing regulations impose no limitations on the sharing of personally identifiable information under the Section 314(b) safe harbor where otherwise consistent with Section 314(b) and its implementing regulations. Nor do Section 314(b) or its implementing regulations impose restrictions on the type or medium of information that can be shared in reliance on the Section 314(b) safe harbor, such as video surveillance footage or cyber-related data such as IP addresses. Section 314(b) information sharing can likewise be verbal as well as written. Of course, financial institutions and associations of financial institutions must maintain adequate procedures to protect the security and confidentiality of all information shared pursuant to Section 314(b) and only use such information for the purposes laid out in Section 314(b) and its implementing regulations. See 31 CFR 1010.540(b)(4)(i)-(ii).

In cases where a financial institution files a SAR that has benefited from Section 314(b) information sharing, FinCEN encourages financial institutions to note this in the narrative in order for FinCEN to identify and communicate specific examples of the benefits of the Section 314(b) program. Please note, however, that while information may be shared related to possible terrorist financing or money laundering that resulted in, or may result in, the filing of a SAR, Section 314(b) does not authorize a participating financial institution to share a SAR itself or to disclose any information that would reveal the existence of a SAR.⁶ However, as discussed below, financial institutions sharing information pursuant to Section 314(b) may work together to file joint SARs.

6. SAR confidentiality standards are governed by applicable SAR regulations. See, e.g., 31 CFR 1020.320

December 2020

Can an entity that is not a financial institution under the BSA and its implementing regulations, such as a compliance services provider, form and operate an association of financial institutions whose members can engage in information sharing covered by the Section 314(b) safe harbor?

Yes, FinCEN does not require the organization that forms and operates an association of financial institutions whose members engage in information sharing protected by the Section 314(b) safe harbor to itself be a regulated financial institution under the BSA and its implementing regulations.⁷ Furthermore, there is no Section 314(b) requirement that an entity forming and operating an association of financial institutions be a subsidiary or corporate affiliate of a financial institution.

Any entity forming an association of financial institutions must, of course, conform its activities with the other requirements of Section 314(b), including the use and security requirements of 31 CFR § 1010.540(b)(4).

Can an unincorporated association governed by a contract among the group of financial institutions that constitutes its members engage in information sharing covered by the Section 314(b) safe harbor?

Yes. Section 314(b) permits unincorporated associations to engage in information sharing pursuant to the Section 314(b) safe harbor. Such unincorporated associations can exist based on contracts among their participants. Of course, such unincorporated associations must conform their membership and activities to all of the requirements of Section 314(b). All members of such an unincorporated association must be financial institutions consistent with the definition of that term in 31 CFR § 1010.540(a)(1). Furthermore, an unincorporated association must operate in compliance with other requirements of Section 314(b), including the use and security requirements of 31 CFR § 1010.540(b)(4).

How do Financial Institutions or Associations of Financial Institutions Participate in 314(b)?

FinCEN regulations (31 CFR 1010.540) set forth the requirements that must be satisfied in order to benefit from 314(b) safe harbor protection, as outlined below. A financial institution or association of financial institutions will only benefit from the safe harbor protection if it follows the conditions for participation in the program:

7. Although the 2012 Administrative Ruling is revoked by this guidance, the determination in that ruling that the applicant met the technical requirements to be considered an association of financial institutions is consistent with FinCEN's updated guidance herein. In particular, FinCEN reiterates its confirmation in the 2012 Administrative Ruling that a limited liability company whose membership is comprised entirely of financial institutions, deemed eligible under the regulations implementing section 314(b), would meet the technical requirements to be considered an association of financial institutions under section 314(b) and FinCEN's regulations implementing section 314(b).

December 2020

Submit a Registration to FinCEN

Information regarding the 314(b) registration process is available on FinCEN's website (<https://www.fincen.gov/section-314b>). Financial institutions and associations interested in participating in the 314(b) program must first register with FinCEN's Secure Information Sharing System (SISS) if they are not already a registered SISS user. Upon logging in to SISS, users can then navigate to the "314(b)" tab and submit a 314(b) registration. All registrations are processed within two business days of receipt, and participants will receive an acknowledgment via e-mail.

Sharing Information with Other 314(b) Participants

Prior to sharing information under Section 314(b), financial institutions and associations must take reasonable steps, such as checking the FinCEN 314(b) participant list, to verify that the other financial institution or association is also a 314(b) registrant. To facilitate the identification of 314(b) program participants, SISS provides tools to search the 314(b) participant list for other participants or download the participant list in its entirety. FinCEN updates the list in real-time. Financial institutions and associations may establish policies and procedures that designate more than one person with the authority to participate in the financial institution's 314(b) program.⁸

Safeguard Shared Information and use only for AML/CFT Purposes

Financial institutions and associations must establish and maintain procedures to safeguard the security and confidentiality of shared information, and must only use shared information for the purpose of:

- Identifying and, where appropriate, reporting on activities that may involve terrorist financing or money laundering;
- Determining whether to establish or maintain an account, or to engage in a transaction; or
- Assisting in compliance with anti-money laundering requirements.

8. Although a financial institution participating in the 314(b) program must provide, at a minimum, one point of contact to FinCEN as part of its registration, other employees may participate in Section 314(b) information sharing consistent with the financial institution's policies and procedures.

December 2020

May financial institutions that share information pursuant to Section 314(b) file joint SARs?

FinCEN's SAR regulations allow for the submission of joint SARs by financial institutions.⁹ When financial institutions identify suspicious activity through collaboration pursuant to Section 314(b), they may consider whether a joint SAR would be the most efficient way to provide highly useful information to law enforcement.

Financial institutions should keep in mind that Section 314(b) does not relax the prohibition against SAR disclosures, nor does it otherwise address SAR confidentiality. Financial institutions participating in information sharing pursuant to Section 314(b) remain prohibited from disclosing a SAR or any information that would reveal the existence of a SAR notwithstanding Section 314(b).

However, financial institutions participating in Section 314(b) that are considering filing or have filed a joint SAR may freely discuss the prospective or already filed joint SAR amongst themselves.

Updating Point of Contact Information and Additional Resources

Changes, updates or deletions of current 314(b) registration information can be made through SISS. A detailed 314(b) User Guide is also available in SISS. For additional questions related to 314(b) information sharing, FinCEN can be reached via phone at 866-326-8314 or sys314a@fincen.gov.

9. All FinCEN SAR regulations include a rule of construction that accounts for the possibility of financial institutions filing joint SARs. See 31 C.F.R. 1020.320(e)(1)(ii)(A)(2)(i) (banks); 31 C.F.R. 1021.320(e)(1)(ii)(A)(2) (casinos); 31 C.F.R. 1022.320(e)(1)(ii)(A)(2) (MSBs); 1023.320(e)(1)(ii)(A)(2)(i) (broker-dealers); 31 C.F.R. 1024.320(d)(1)(ii)(A)(2) (mutual funds); 31 C.F.R. 1025.320(e)(1)(ii)(A)(2) (insurance companies); 1026.320(e)(1)(ii)(A)(2)(i) (futures commission merchants and introducing brokers in commodities); 31 C.F.R. 1029.320(d)(1)(ii)(A)(2) (loan or finance companies); 31 C.F.R. 1030.320(d)(1)(ii)(A)(2) (housing government sponsored enterprises).

December 2020

USA PATRIOT ACT / Title III Questions

True or False

- _____ 1. With the passage of the PATRIOT Act, Congress indicated that when opening a new account, financial institutions must perform an OFAC check on all new account holders.
- _____ 2. A financial institution's CIP program must be logic based.
- _____ 3. Providing a federally "worded" notice within 90 days after the account is opened is one of the five "logistical/operational" functions performed by financial institutions.
- _____ 4. Sales of monetary instruments to non-clients meet the expanded definition of an account under the CIP rule.
- _____ 5. Financial institutions must "CIP" the primary owner of a joint account only.
- _____ 6. Physical address is one of the four required minimum components that must be obtained prior to opening any new account.
- _____ 7. The biggest "on-going" issue within the financial services industry with CIP is adequate personnel resources to accomplish all assigned tasks.
- _____ 8. The 314(a) records search must begin when the timing is convenient.
- _____ 9. The 314(a) records search must be completed before the end of the current month.
- _____ 10. The 314(a) records search must include the beneficial owners of legal entity customers.
- _____ 11. Unless specifically requested, the 314(a) search process looks for "accounts" currently open or closed within the last year.
- _____ 12. The insurance broker is actually responsible for filing the FinCEN Form 111.
- _____ 13. Any unusual method of payment, particularly by cash or cash equivalents is a Federal example of a "high-risk" insurance.
- _____ 14. PEP reviews are limited only to Foreign Heads of State.
- _____ 15. FinCEN's expectations for obtaining beneficial ownership information for certain accounts or customer relationships only applies to the Section 312 account categories.

RECORDKEEPING REQUIREMENTS

I. INTRODUCTION

- A. Overview** - The Bank Secrecy Act requires banks to create or obtain, and then preserve, certain records relating to customer transactions for potential examination by the bank's regulators, law enforcement and/or other government agencies. Some of these records, such as those dealing with large currency transactions and suspicious transactions, must be transmitted directly to a designated government agency. This chapter will discuss those records which need only be retained by the bank and made accessible to proper governmental requests for review.
- B. Method of Record Retention** Records may consist of originals, copies, microfilm copies or electronic records of the payment order. Records made in the ordinary course of business may be used to meet these requirements. If not generated by routine recordkeeping, the records are to be prepared in writing by the bank.
- C. Length of Record Retention and Access to Records** - Required records must be retained for a period of five years and must generally be accessible within a reasonable period of time. When the request is from the bank's principal Federal regulator and pertains to terrorist or money laundering activities, the records must be accessible within 120 hours of the request. If law enforcement issues a written request for information on foreign correspondent bank accounts, the records must be made available within seven days.

II. RECORDS REQUIRED TO BE MAINTAINED

- A. Extensions of Credit** - The name and address of the borrower, the amount of the credit, its nature or purpose and date must be obtained by the financial institution. This requirement is applicable only to extensions of credit in excess of \$10,000 not secured by real property.
- B. Taxpayer Identification Numbers (TINs)** - Banks must obtain the appropriate TIN for customers purchasing a certificate of deposit or opening a deposit or share account. Internal Revenue Service guidelines determine what constitutes a TIN and which number is to be used.

What Name and Number To Give the Requester			
For this type of account:	Give the name and SOCIAL SECURITY number of:	For this type of account:	Give the name and EMPLOYER IDENTIFICATION number of:
1. Individual	The individual	7. Disregarded entity not owned by an individual	The owner
2. Two or more individuals (joint account)	The actual owner of the account or, if combined funds, the first individual on the account ¹	8. A valid trust, estate or pension trust	Legal entity ⁴
3. Custodian account of a minor (Uniform Gift or Transfers to Minors Act)	The minor ²	9. Corporate or LLC electing corporate status on Form 8832 or Form 2553	The corporation
4. a. The usual revocable savings trust (grantor is also trustee	The grantor-trustee ¹	10. Association, club, religious, charitable, educational or other tax-exempt organization	The organization
b. So-called trust account that is not a legal or valid trust under state law	The actual owner ¹	11. Partnership or multi-member LLC	The partnership
5. Sole proprietorship or disregarded entity owned by an individual	The owner ¹	12. A broker or registered nominee	The broker or nominee
6. Grantor trust filing under Optional Form 1099 Filing Method 1 (see Regulation section 1.671-4(b)(2)(i)(A))	The grantor ³	13. Account with the Department of Agriculture in the name of a public entity (such as a state or local government, school district or prison) that receives agricultural program payments	The public entity
		14. Grantor trust filing under the Form 1041 Filing Method or the Optional Form 1099 Filing Method 2 (see Regulation section 1.671-4(b)(2)(i)(B))	The trust
¹ List first and circle the name of the person whose number you furnish. If only one person on a joint account has an SSN, that person's number must be furnished. ² Circle the minor's name and furnish the minor's SSN. ³ You must show your individual name and you may also enter your business or "DBA" name on the "Business name/disregarded entity" name line. You may use either your SSN or EIN (if you have one), but the IRS encourages you to use your SSN. ⁴ List first and circle the name of the trust, estate, or pension trust. (Do not furnish the TIN of the personal representative or trustee unless the legal entity itself is not designated in the account title.) Also see <i>Special rules for partnerships</i> on page 1. *Note. Grantor also must provide a Form W-9 to trustee of trust.			
Source: Compiled from IRS Form W-9 and the "B-Notice"			

- C. Signature Cards** - Documents granting signature authority over each deposit or share account including notations of specific identifying information verifying the identity of the signer, if such are normally made. (Retained for five years after account is closed.)
- D. Transaction Records** - Each statement, ledger card or other record on each deposit or share account.
- E. On-us Checks** - Each check, draft or money order over \$100 drawn on the bank or issued and payable by it. (Instruments drawn on certain high activity accounts, dividends, payroll, etc., are exempted.) (The UCC covers the retention requirements when physical checks are not returned to the customer in the periodic statement.)
- F. Debits to Customer Accounts** - All debits or charges in excess of \$100 other than bank or periodic charges.

- G. Checks Deposited** - All bank records prepared or received in the ordinary course of business which would be necessary to reconstruct and trace items in excess of \$100 deposited in a transaction account.

NOTE: For Bank Secrecy Act recordkeeping purposes, the definition of a transaction account includes all accounts subject to check, including money market deposit accounts.

- H. Funds Transferred to or from U.S.** - A record of each advice, request, or instruction received or given regarding any transaction resulting in the transfer of currency or other monetary instruments, funds, checks, investment securities, or credit of more than \$10,000 to or from any person, account or place outside the United States. (Records regarding canceled transactions of this type are required only if they are normally made.)
- I. Items From Transfers Outside U.S.** - Each item, including checks, drafts or transfers of credit, of more than \$10,000 remitted or transferred to a person, account or place outside the United States.
- J. Records of Transfers Outside U.S.** - A record of each remittance or transfer of funds, currency, checks, investment securities, other monetary instruments or credits of more than \$10,000 to a person, account or place outside the United States.
- K. Foreign Checks Presented For Payment** - Checks or drafts in excess of \$10,000 drawn on or issued by a foreign bank which the domestic bank has paid or presented to a nonbank drawee for payment.
- L. Items Received From Foreign Banking Institutions** - Each item, including checks, drafts or transfers of credit of more than \$10,000 received directly and not through a domestic financial institution, by letter, cable or any other means, from a bank, broker or dealer in foreign exchange outside the United States.
- M. Records of Receipts From Foreign Banking Institutions** - A record of each receipt of currency, other monetary instruments, investment securities or checks, and each transfer of funds or credit, of more than \$10,000 received on any one occasion directly and not through a domestic financial institution, from a bank, broker or dealer in foreign exchange outside the United States.
- N. Certificates Sold** - The name, address and TIN of the purchaser of each certificate of deposit, a description of the instrument and notation of the method of payment as well as the date of the transaction.
- O. Certificates Redeemed** - The name, address and TIN of any person presenting a certificate of deposit for payment, a description of the instrument and the date of the transaction.
- P. Deposit Slips or Credit Tickets** - All deposit slips and credit tickets reflecting transactions in excess of \$100 and equivalent records for direct deposits and wire transfers. The amount of currency involved must be reflected on the slip or ticket.

NOTE: Many items fall under the heading of "credit tickets." Included are general ledger tickets, loan payment coupons, etc. The record retention requirement is not limited to credits to deposit accounts.

Q. Currency Transaction Reports - Copies of all CTRs filed.

R. Sales of Official and Traveler's Checks - When a transaction or group of contemporaneous transactions involving U.S. coins or currency in an amount of \$3,000 to \$10,000 (inclusive) causes a bank to issue or sell a bank check or draft; cashier's check; traveler's check or money order to an individual, special identification and recordkeeping requirements are applicable. Information retained corresponds to the accountholder status of the purchaser:

Information to Be Obtained:	Deposit Accountholder	Non-Accountholder
Name of purchaser.	X	X
Date of purchase.	X	X
Type(s) of instrument(s) purchased.	X	X
Serial number(s) of the instrument(s) purchased.	X	X
Amount in dollars of each of the instrument(s) purchased.	X	X
Address of the purchaser.		X
Social Security/Alien Identification Number of the purchaser.		X
Date of birth of the purchaser.		X
Verification of Purchaser's Identity:		
Use signature cards or other records at the bank, provided the accountholder's name and address were previously verified, and that information was recorded on the signature card or other file record.	X	
Examination of a document which is normally acceptable within the banking community as a means of identification when cashing checks for nondepositors, and which contains the name and address of the purchaser. If used, the bank will record the specific identifying information on the record.	X	X

- These records shall be maintained for a period of five years. Contemporaneous purchases of the same or different types of instruments totaling \$ 3,000 or more shall be treated as one purchase, just as multiple purchases during one business day totaling \$ 3,000 or more shall also be treated as one purchase if the bank has knowledge that these purchases have occurred. Deposit accounts include transaction accounts, savings accounts, and time deposits. (The requirement to maintain these records on a centralized log was eliminated in October of 1994).
- In December 2002, FinCEN published guidance pertaining to the depositing of currency into accounts prior to issuing the above referenced monetary instruments. FinCEN takes the position that "when a customer purchases a monetary instrument between \$3,000 and \$10,000 using currency that customer first deposits into their account the transaction is still subject to this recordkeeping." FinCEN "anticipates" that most banks already maintain most of this required information.

III. RECORDKEEPING FOR FUNDS TRANSFERS AND TRANSMITTALS OF FUNDS BY BANKS

- A. Overview** - Each domestic bank involved in a funds transfer must collect and retain certain information, depending upon its role in the particular funds transfer, the amount of the funds transfer, and the relationship of the parties to the transaction with the bank.
- B. Payment Order Processing** - For each payment order that it accepts in the amount of \$3,000 or more, a financial institution shall obtain and retain, for five years, the following information:

Originator's Bank	Intermediary Bank	Beneficiary's Bank
<ul style="list-style-type: none">• Name and address of the originator;• Amount of payment order;• Execution date;• Any payment instructions received from the originator with the payment order;• The beneficiary's bank; and• as many of the following as are received with the order:<ul style="list-style-type: none">– Name and address of the beneficiary;– The account number of the beneficiary; and,– Any other specific identifiers.	<ul style="list-style-type: none">• An original, microfilm, other copy, or electronic record of the payment order.	<ul style="list-style-type: none">• An original, microfilm, other copy, or electronic record of the payment order.

- C. Non-Customer verification** - In the case of a payment order either from an originator, or to a beneficiary, who are not established customers banks shall obtain and retain additional information:

Non-Customer Originator	Non-Customer Beneficiary
<ul style="list-style-type: none">• Order made in person: bank shall verify the identity of the originator placing the order, and record the name and address, the Tin or Alien ID number, as well as the type of identification used (including any identifying numbers) in the record.• Order not made in person: bank shall obtain above information, and record the method of payment (e.g. check or credit card transaction) for the funds transfer.	<ul style="list-style-type: none">• Proceeds delivered in person: bank shall verify the identity of the person receiving the proceeds and shall record and retain name, address, type of identification document used, and TIN/EIN/alien identification number.• Proceeds delivered other than in person: bank shall retain a copy of the check or payment instrument, as well as the name and address of the person to which it was sent.

1. An "established customer" is a person with an account with the institution, including a loan account, or deposit, or other asset account, or is a person with respect to which the bank has obtained and maintains on file, the person's name and address, as well as the TIN/EIN/or alien identification number, and to which the bank provides financial services relying on that information.

- D. Retrievability** - The information that both the originating and beneficiary banks must retain shall be retrievable by both the name and the account number (where applicable) of the individuals involved in the payment. Neither the Fed nor the Treasury require the use of automated retrieval systems. Both agencies do suggest however, that banks consider implementing automated systems based on the anticipated demand for funds transfer records, and the bank's current method(s) for keeping records.
- E. Exceptions** - The below listed funds transfers are not subject to these recordkeeping requirements.
1. Funds transfers less than \$ 3,000.
 2. Funds transfers governed by the Electronic Fund Transfer Act (Reg E), or processed through an automated clearinghouse, automated teller machine, or point of sale system.
 3. Funds transfer where the originator and the beneficiary are any of the following:
 - a. A bank;
 - b. Wholly-owned domestic subsidiary of a bank chartered in the United States;
 - c. Broker or dealer in securities;
 - d. Wholly-owned domestic subsidiary of a broker or dealer in securities;
 - e. The United States;
 - f. A state or local government; or
 - g. A federal, state, or local government agency or instrumentality.
 4. Funds transfers where both the originator and the beneficiary are the same person, and the originator's bank and the beneficiary's bank are the same bank.
- F. Increased Transparency for Cross-Border Payments** – In December 2009, the regulatory agencies released guidance supporting the Basel Committee's concern on the transparency in cross-border cover payments messages, and reinforcing the Wolfsberg Group's message standards document from 2007. Basically, DFIs should not omit, delete, or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other financial institution in the payment process, and DFIs should strongly encourage their correspondent banks to observe these principles. (See FDIC FIL 72-2009).

- G. Travel Rule** - For each payment order that it accepts in the amount of \$ 3,000 or more, a bank shall obtain and include in the payment transmittal, certain information covering the originator, the beneficiary, and the transmitter's financial institution, ensuring that this information "travels" with the payment transaction.

See FinCEN Guidance FIN-2010-G004 (11/09/2010) for updated Questions and Answers covering the Funds "Travel" Regulations.

Transmitter's Financial Institution	Intermediary Financial Institution
<ul style="list-style-type: none">• Name and account number (where applicable) of the transmitter;• Address of the transmitter;• Identity of the transmitter's financial institution;• Amount of the transmittal;• Execution date of the transmittal order;• Identity of the recipients financial institution;• And as many of the following items as are received with the transmittal order:<ul style="list-style-type: none">• Name and address of the recipient;• Account number of the recipient;• Other specific identifiers of the recipient.	<ul style="list-style-type: none">• All of the information included in the payment order by the transmitter's financial institution, plus;• Name and address or numerical identifier of the transmitter's financial institution.

The same exceptions listed in Section E apply to the travel rule.

NOTE: Financial institutions must use the transmitter's true name and address in the transmittal order for funds transfer; coded names or pseudonyms will no longer be allowed. The transmittal order may use either the transmitter's street address or mailing address. However, the mailing address may only be used when the financial institution maintains the transmitter's street address on file and that information is retrievable upon request by law enforcement.

- H. Record Retentions** - Other record retention schedules may be established by state law, state regulations or informal recommendations adopted by banking associations. Banks generally adhere to the schedule adopted in their state except where it is extended by federal regulations. Retention schedules do not ordinarily focus on transaction type as does the BSA; their time frames normally deal with record type. **Since BSA supersedes any state or federal retention requirement of a lesser period, both schedules should be specifically reviewed when developing comprehensive recordkeeping policies.**
- I. Law Enforcement Access** - Although banks are required to maintain certain records, they are not automatically available to law enforcement agencies. They can only be reached through legal process. For example, the Right to Financial Privacy Act limits the access of the federal government to bank records. State privacy laws and court decisions may limit access of other government units.
- J. Cross-Border Electronic Transmittals of Funds (CBETF)** - FinCEN has published an NPRM proposing the actual reporting of certain CBETF

transactions, and to require an annual filing by all financial institutions of a list of the TINs of account holders who transmitted or received CBETFs. The comment period closed December 29, 2010 – with Final Rule possibly issued after January 1, 2012. (75 FR 60377-60397, September 13, 2010).

K. Privacy - Both the regulations on the privacy of consumer financial information (Regulation P) and the interagency guidelines establishing the standards for safeguarding customer information impose annual privacy-related requirements covering all the records in this chapter. Banks are expected to:

1. ensure the security and confidentiality of these records;
2. protect these records against any threats and hazards; and
3. protect these records from unauthorized access.

L. Exam Procedures - Contained within the current interagency BSA/AML examination manual are the core examination procedures covering an institution's recordkeeping program. Highly qualitative and subjective in nature, the Federal examiner will form a conclusion about the ability of policies, procedures, and processes to meet the regulatory requirements associated with the recordkeeping requirements by completing a number of reviews which include, but are not limited to:

1. Determining if the institution maintains the required records for sales of cashier's checks, travelers checks (in any form), and money orders for currency in amounts between \$3,000 and \$10,000 inclusive to purchasers who have deposit accounts with the institution;
2. Determining if the institution's policies, procedures, and processes permit the sales of monetary instruments to purchasers who do not have deposit accounts with the institution, and if so, determining if the required records of such sales are maintained.
3. Verifying that the institution obtains and maintains the required records on recordable funds transfers;
4. Verifying that the institution transmits the required "Travel Rule" information as required for appropriate funds transfers;
5. If the institution sends or receives funds transfers to or from institutions in foreign countries, assessing whether the institution has policies, procedures, and processes to determine whether the amounts, frequencies, and countries of origin or destination are consistent with the nature of the business or occupation of the client.

Financial institutions may obtain copies of the exam procedures from www.ffiec.gov/bsa_aml_infobase/

RECORD RETENTION QUESTIONS

True or False

- _____ 1. To fulfill BSA requirements banks must maintain an additional set of required records, keeping them separate from other records of a similar type.
- _____ 2. In a joint account the TIN used should be that of the first individual named in the account title.
- _____ 3. When redeeming a certificate of deposit, the TIN of any of the owners must be obtained.
- _____ 4. Records required by BSA must be kept for five years.
- _____ 5. In meeting the requirement that bank records include a statement of purpose for certain loans, purpose statements such as "personal" and "business" are adequate.
- _____ 6. If a customer deposits 27 checks drawn on other banks, each above \$100, into a checking account the depository bank must be able to reproduce them.
- _____ 7. If loan payment is more than \$100 and any portion of the amount received is in cash the amount of currency should be noted on the credit ticket.
- _____ 8. Banks are required to obtain the date of birth of all purchasers of travelers checks in cash of \$3,000 or more.
- _____ 9. Banks are no longer required to maintain the monetary instruments log.
- _____ 10. Wire transfers and ACH transactions, in excess of \$10,000, are the only payments subject to the recordkeeping rules.
- _____ 11. Banks are no longer required to include the name, address and account number of the transmitter in the text of a payment order.
- _____ 12. The Travel Rule only applies to foreign wire transfers.
- _____ 13. If the Travel Rule Data is not included with an inbound entry, the receiving institution must reject the entry.
- _____ 14. The funds transfer recordkeeping requirements obligate a financial institution to accept a funds transfer request from any person requesting such.
- _____ 15. If state law or regulation specifies that a bank record also required by BSA need be kept only three years it is acceptable to follow the shorter period.

(Blank Page)

therefore: (1) Is not a “significant regulatory action” under Executive Order 12866; (2) is not a “significant rule” under Department of Transportation (DOT) Regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a regulatory evaluation as the anticipated impact is so minimal. Since this is a routine matter that will only affect air traffic procedures and air navigation, it is certified that this proposed rule, when promulgated, will not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

Environmental Review

This proposal will be subjected to an environmental analysis in accordance with FAA Order 1050.1F, “Environmental Impacts: Policies and Procedures,” prior to any FAA final regulatory action.

List of Subjects in 14 CFR Part 73

Airspace, Prohibited areas, Restricted areas.

The Proposed Amendment

In consideration of the foregoing, the Federal Aviation Administration proposes to amend 14 CFR part 73 as follows:

PART 73—SPECIAL USE AIRSPACE

- 1. The authority citation for part 73 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g); 40103, 40113, 40120; E.O. 10854, 24 FR 9565, 3 CFR, 1959–1963 Comp., p. 389.

§ 73.41 Massachusetts [Amended]

- 2. Section 73.41 is amended as follows:

* * * * *

R-4102A Fort Devens, MA [Amended]

Boundaries. Beginning at lat. 42°31'11" N, long. 71°38'29" W; to lat. 42°30'55" N, long. 71°37'51" W; to lat. 42°30'12" N, long. 71°38'05" W; to lat. 42°29'38" N, long. 71°37'41" W; to lat. 42°28'21" N, long. 71°39'14" W; to lat. 42°28'11" N, long. 71°39'32" W; to lat. 42°28'11" N, long. 71°39'38" W; to lat. 42°28'15" N, long. 71°39'45" W; to lat. 42°28'25" N, long. 71°40'08" W; to lat. 42°28'54" N, long. 71°41'00" W; to lat. 42°29'08" N, long. 71°41'06" W; to lat. 42°29'52" N, long. 71°41'08" W; to lat. 42°30'17" N, long. 71°41'29" W; to lat. 42°30'19" N, long. 71°41'19" W; to lat. 42°30'37" N, long. 71°40'30" W; to lat. 42°30'43" N, long. 71°40'17" W; to lat. 42°30'52" N, long. 71°40'14" W; to lat. 42°30'54" N, long. 71°40'10" W; to lat. 42°30'53" N, long. 71°40'02" W; to lat. 42°30'48" N, long. 71°39'57" W; to lat. 42°30'47" N, long. 71°39'45" W; to lat. 42°30'55" N, long.

71°39'31" W; to lat. 42°30'58" N, long. 71°39'18" W; to lat. 42°30'57" N, long. 71°39'09" W; to lat. 42°30'52" N, long. 71°38'42" W; to lat. 42°30'58" N, long. 71°38'33" W; to lat. 42°31'06" N, long. 71°38'37" W; thence to the point of beginning. *Designated altitudes.* Surface to, but not including, 2,000 feet MSL. *Time of designation.* Intermittent, 0730–2200 local time, daily; other times by NOTAM issued 24 hours in advance. *Controlling agency.* FAA, Boston Approach Control. *Using agency.* Commander, U.S. Army Garrison, Fort Devens, MA.

R-4102B Fort Devens, MA [Amended]

Boundaries. Beginning at lat. 42°31'11" N, long. 71°38'29" W; to lat. 42°30'55" N, long. 71°37'51" W; to lat. 42°30'12" N, long. 71°38'05" W; to lat. 42°29'38" N, long. 71°37'41" W; to lat. 42°28'21" N, long. 71°39'14" W; to lat. 42°28'11" N, long. 71°39'32" W; to lat. 42°28'11" N, long. 71°39'38" W; to lat. 42°28'15" N, long. 71°39'45" W; to lat. 42°28'25" N, long. 71°40'08" W; to lat. 42°28'54" N, long. 71°41'00" W; to lat. 42°29'08" N, long. 71°41'06" W; to lat. 42°29'52" N, long. 71°41'08" W; to lat. 42°30'17" N, long. 71°41'29" W; to lat. 42°30'19" N, long. 71°41'19" W; to lat. 42°30'37" N, long. 71°40'30" W; to lat. 42°30'43" N, long. 71°40'17" W; to lat. 42°30'52" N, long. 71°40'14" W; to lat. 42°30'54" N, long. 71°40'10" W; to lat. 42°30'53" N, long. 71°40'02" W; to lat. 42°30'48" N, long. 71°39'57" W; to lat. 42°30'47" N, long. 71°39'45" W; to lat. 42°30'55" N, long. 71°39'31" W; to lat. 42°30'58" N, long. 71°39'18" W; to lat. 42°30'57" N, long. 71°39'09" W; to lat. 42°30'52" N, long. 71°38'42" W; to lat. 42°30'58" N, long. 71°38'33" W; to lat. 42°31'06" N, long. 71°38'37" W; thence to the point of beginning.

Designated altitudes. 2,000 feet MSL to 3,995 feet MSL.

Time of designation. Intermittent, 0730–2200 local time, daily; other times by NOTAM issued 24 hours in advance.

Controlling agency. FAA, Boston Approach Control.

Using agency. Commander, U.S. Army Garrison, Fort Devens, MA.

* * * * *

Issued in Washington, DC, on March 29, 2021.

George Gonzalez,

Acting Manager, Rules and Regulations Group.

[FR Doc. 2021–06739 Filed 4–2–21; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network

31 CFR Part 1010

RIN 1506–AB49

Beneficial Ownership Information Reporting Requirements

AGENCY: Financial Crimes Enforcement Network (FinCEN), Treasury.

ACTION: Advance notice of proposed rulemaking.

SUMMARY: FinCEN is issuing this advance notice of proposed rulemaking (ANPRM) to solicit public comment on questions pertinent to the implementation of the Corporate Transparency Act (CTA), enacted into law as part of the National Defense Authorization Act for Fiscal Year 2021 (NDAA). This ANPRM seeks initial public input on procedures and standards for reporting companies to submit information to FinCEN about their beneficial owners (the individual natural persons who ultimately own or control the reporting companies) as required by the CTA. This ANPRM also seeks initial public input on FinCEN's implementation of the related provisions of the CTA that govern FinCEN's maintenance and disclosure of beneficial ownership information subject to appropriate protocols.

DATES: Written comments on this ANPRM must be received on or before May 5, 2021.

ADDRESSES: Comments may be submitted by any of the following methods:

- *Federal E-rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments. Refer to Docket Number FINCEN–2021–0005 and RIN 1506–AB49.

- *Mail:* Policy Division, Financial Crimes Enforcement Network, P.O. Box 39, Vienna, VA 22183. Refer to Docket Number FINCEN–2021–0005 and RIN 1506–AB49.

FOR FURTHER INFORMATION CONTACT: The FinCEN Regulatory Support Section at 1–800–767–2825 or electronically at frc@fincen.gov.

SUPPLEMENTARY INFORMATION:

I. Scope of ANPRM

This ANPRM seeks comment on FinCEN's implementation of certain provisions in Section 6403 of the CTA.¹

¹ The CTA is Title LXIV of the National Defense Authorization Act for Fiscal Year 2021, Public Law 116–283 (January 1, 2021). Section 6403 of the CTA, among other things, amends the Bank Secrecy Act

Section 6403 requires reporting companies (corporations, limited liability companies (LLCs), and similar entities, subject to certain statutory exemptions) to submit to FinCEN specified information on their beneficial owners—the individual natural persons who own or control them—as well as specified information about the persons who form or register those reporting companies. Section 6403 further requires FinCEN to maintain this information in a confidential, secure, and non-public database, and it authorizes FinCEN to disclose the information to certain government agencies for certain purposes specified in the CTA, and to financial institutions to assist in meeting their customer due diligence obligations. In both cases, these disclosures are subject to appropriate protocols to protect confidentiality. This ANPRM seeks comment on numerous questions as FinCEN begins to develop proposed regulations implementing these provisions. While only the regulations implementing the reporting requirements must be promulgated by January 1, 2022, with an effective date to be determined, FinCEN also seeks comment at this time on its implementation of the related database maintenance use and disclosure provisions. Section 6403's mandate that the final rule on customer due diligence requirements for financial institutions be revised will be the subject of a separate rulemaking, about which the public will receive notice and opportunity to comment.

II. Background

A. The Bank Secrecy Act

Enacted in 1970 and amended most recently by the Anti-Money Laundering Act of 2020, which includes the CTA, the Bank Secrecy Act (BSA) aids in the prevention of money laundering, terrorism financing, and other illicit activity.² The purposes of the BSA include, among other things, “requir[ing] certain reports or records that are highly useful in—(A) criminal, tax, or regulatory investigations, risk assessments, or proceedings; or (B)

intelligence or counterintelligence activities, including analysis, to protect against terrorism” and “establish[ing] appropriate frameworks for information sharing” among financial institutions and government authorities.³

Congress has authorized the Secretary of the Treasury (the Secretary) to administer the BSA. The Secretary has delegated to the Director of FinCEN the authority to implement, administer, and enforce compliance with the BSA and associated regulations.⁴ FinCEN is authorized to require financial institutions or nonfinancial trades or businesses to maintain procedures to ensure compliance with the BSA and the regulations promulgated thereunder and to guard against money laundering, the financing of terrorism, and other forms of illicit finance.⁵

B. Beneficial Ownership of Legal Entities

Legal entities such as corporations and LLCs play an important role in the U.S. economy. By limiting individual liability, corporations and LLCs allow owners to manage the risks associated with participating in business ventures. They also facilitate the formation of capital, making it easier to finance large business projects and structure the relationships among individuals engaged in an enterprise. They often can be formed with relatively few formalities and abbreviated (if any) regulatory review and approval, and their availability can be viewed as a stimulus to investment, entrepreneurship, and economic activity.

At the same time, legal entities can be misused to conceal and facilitate illicit activity. As Congress recognized in the CTA, “malign actors seek to conceal their ownership of corporations, limited liability companies, or other similar entities in the United States to facilitate illicit activity, including money laundering, the financing of terrorism, proliferation financing, serious tax fraud, human and drug trafficking, counterfeiting, piracy, securities fraud, financial fraud, and acts of foreign corruption[.]”⁶ Furthermore, Congress underscored that “money launderers and others involved in commercial activity intentionally conduct transactions through corporate structures in order to evade detection, and may layer such structures . . . across various secretive jurisdictions such that each time an investigator

obtains ownership records for a domestic or foreign entity, the newly identified entity is yet another corporate entity, necessitating a repeat of the same process.”⁷ The ability to engage in activity and obtain financial services in the name of a legal entity without disclosing the identities of the natural persons who own or control the entity—the natural persons whose interests the legal entity most directly serves—enables those natural persons to conceal their interests. As FinCEN has previously highlighted, such concealment “facilitates crime, threatens national security, and jeopardizes the integrity of the financial system.”⁸

U.S. government reports have consistently identified the ability to operate through legal entities without ready identification of their beneficial owners as a key illicit finance risk for the U.S. financial system. The 2018 National Money Laundering Risk Assessment noted that legal entities are misused by illicit actors to disguise criminal proceeds, and that the lack of readily available beneficial ownership information hampers law enforcement investigations, asset seizures and forfeitures, and international cooperation, as well as the ability of financial institutions to conduct customer due diligence (CDD) and identify suspicious activity.⁹ Further, the 2020 National Strategy to Combat Terrorist and Other Illicit Financing (2020 National Strategy) found that large-scale schemes that generate substantial proceeds for perpetrators and smaller white-collar cases alike routinely involve shell companies.¹⁰ As the Federal Bureau of Investigation (FBI) stated in recent Congressional testimony, the strategic use of shell companies “makes investigations exponentially more difficult and laborious. The burden of uncovering true beneficial owners can often handicap or delay investigations, frequently requiring duplicative, slow-moving legal process in several jurisdictions to gain the necessary information.”¹¹ Moreover, as the 2020

⁷ CTA Section 6402(4).

⁸ Notice of Proposed Rulemaking: Customer Due Diligence Requirements for Financial Institutions, 79 FR 45151, 45153 (August 4, 2014).

⁹ U.S. Department of the Treasury, National Money Laundering Risk Assessment (2018) (2018 NMLRA), pp. 28–30, https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf.

¹⁰ U.S. Department of the Treasury, National Strategy for Combating Terrorist and Other Illicit Financing (2020) (2020 National Strategy), p. 14, <https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf>.

¹¹ Testimony of Steven M. D'Antuono, Acting Deputy Assistant Director, Criminal Investigative

by adding a new Section 5336, Beneficial Ownership Information Reporting Requirements, to Subchapter II of Chapter 53 of Title 31, United States Code. To the greatest extent possible, this ANPRM will cite to new 31 U.S.C. 5336.

² Section 6003(1) of the Anti-Money Laundering Act of 2020, Division F of the National Defense Authorization Act for Fiscal Year 2021, Public Law 116–283 (January 1, 2021), which includes the CTA, defines the Bank Secrecy Act as comprising Section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b), Chapter 2 of Title I of Public Law 91–508 (12 U.S.C. 1951 *et seq.*), and Subchapter II of Chapter 53 of Title 31, United States Code.

³ 31 U.S.C. 5311(1), (5).

⁴ Treasury Order 180–01 (Jan. 14, 2020).

⁵ 31 U.S.C. 5318(a)(2).

⁶ CTA Section 6402(3).

National Strategy noted, “while some federal law enforcement agencies may have the resources required to undertake complex (and costly) investigations [of this sort], the same is often not true for state, local, and tribal law enforcement.”¹² The burden imposed on investigations by the concealment of beneficial ownership information and the difficulty of obtaining accurate beneficial ownership information thus significantly hampers U.S. anti-money laundering (AML) and countering the financing of terrorism (CFT) efforts.

The United States has taken steps to increase corporate transparency. For example, in October 2001, Congress began requiring U.S. financial institutions that maintain correspondent accounts for certain categories of foreign banks to obtain beneficial ownership information about those banks, including “the identity of each of the owners of the foreign bank, and the nature and extent of the ownership interest of each such owner.”¹³ In 2016, FinCEN promulgated the CDD Rule,¹⁴ which, among other things, requires banks, broker-dealers, mutual funds, futures commission merchants, and introducing brokers in commodities to collect beneficial ownership information at the time they open new accounts for legal entity customers, including corporations and LLCs.¹⁵

But these steps are only a partial solution.¹⁶ For example, U.S. legal

entities could make payments through foreign accounts to acquire U.S.-based assets and then use those assets to engage in illicit activity without ever undergoing CDD. Further, U.S. legal entities without any U.S.-based accounts could be engaged in illicit activity outside the United States without having ever been subjected to CDD.

Moreover, requiring financial institutions to obtain beneficial ownership information at the time of account opening, as the CDD Rule requires, does not make beneficial ownership information about U.S. legal entities available to law enforcement before an account is opened. Because states have different practices governing the formation of legal entities in the United States, the extent to which information about the beneficial owners of a U.S. legal entity may be otherwise available to law enforcement can vary widely from state to state.

The U.S. government has long recognized that the difficulty of obtaining accurate, up-to-date beneficial ownership information constitutes a fundamental risk that due diligence by U.S. financial institutions cannot completely mitigate. Consequently, the U.S. government has identified this deficiency as the top priority for strengthening the U.S. AML/CFT regime, which, as Congress has noted, is essential to protect U.S. national security.¹⁷ The Financial Action Task Force (FATF), the intergovernmental organization that sets the international standards for combatting money laundering and the financing of terrorism and proliferation, of which the United States is a founding member, has set minimum standards for beneficial ownership transparency, against which over 200 jurisdictions are assessed. Many countries, including the United Kingdom and all member states of the European Union, have incorporated elements derived from these standards into their domestic legal and/or regulatory frameworks.¹⁸ The 2016

regarding CDD and beneficial ownership of legal entities”).

¹⁷ CTA Section 6402(5)(B). See 2020 National Strategy, p. 40; 2018 NMLRA, pp. 28–30. See also Miller, Rena S. and Rosen, Liana W., Beneficial Ownership Transparency in Corporate Formation, Shell Companies, Real Estate, and Financial Transactions, Congressional Research Service (July 8, 2019), <https://crsreports.congress.gov/product/pdf/R/R45798>.

¹⁸ The FATF is an international, inter-governmental task force whose purpose is the development and promotion of international standards and the effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, the financing of proliferation, and other related threats to the integrity of the international financial system.

FATF Mutual Evaluation Report of the United States underscored the seriousness of this deficiency as the lack of beneficial ownership transparency was one of the main reasons for the United States’ failing grade regarding the effectiveness of the transparency of its beneficial ownership regime.¹⁹ FATF has also collaborated with the Egmont Group of Financial Intelligence Units on a study that identifies key techniques used to conceal beneficial ownership and identifies issues for consideration that include coordinated national action to limit the misuse of legal entities.²⁰ Furthermore, the United States and other major economies have made commitments to enhance beneficial ownership transparency through the then-Group of Eight (G8) and Group of Twenty (G20).²¹ The CTA addresses that commitment.

C. The CTA

The CTA, which Congress enacted on January 1, 2021, establishes a new framework for the reporting, maintenance, and disclosure of beneficial ownership information to:

- Set a clear federal standard for incorporation practices;
- Protect vital U.S. national security interests;

Among other things, it has established standards on transparency and beneficial ownership of legal persons, so as to deter and prevent the misuse of corporate vehicles. The FATF Recommendations require countries to ensure that “adequate, accurate, and timely information on the beneficial ownership and control” of corporate vehicles is available and can be accessed by the competent authorities in a timely fashion. See FATF Recommendation 24, Transparency and Beneficial Ownership of Legal Persons, The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (updated October, 2020), <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>; FATF Guidance, Transparency and Beneficial Ownership at par. 3 (October 2014), <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf>.

¹⁹ See FATF, Mutual Evaluation of the United States (2016), p. 4 (key findings) and Ch. 7.

²⁰ FATF-Egmont Group, Concealment of Beneficial Ownership (2018), https://www.egmontgroup.org/sites/default/files/filedepot/Concealment_of_BO/FATF-Egmont-Concealment-beneficial-ownership.pdf.

²¹ See, e.g., United States G–8 Action Plan for Transparency of Company Ownership and Control (June 2013), <https://obamawhitehouse.archives.gov/the-press-office/2013/06/18/united-states-g-8-action-plan-transparency-company-ownership-and-control>; G8 Lough Erne Declaration (July 2013), <https://www.gov.uk/government/publications/g8-lough-erne-declaration>; G20 High Level Principles on Beneficial Ownership (2014), http://www.g20.utoronto.ca/2014/g20_high_level_principles_beneficial_ownership_transparency.pdf; United States Action Plan to Implement the G–20 High Level Principles on Beneficial Ownership (Oct. 2015), <https://obamawhitehouse.archives.gov/blog/2015/10/16/us-action-plan-implement-g-20-high-level-principles-beneficial-ownership>.

Division, Federal Bureau of Investigation, before the Senate Banking, Housing, and Urban Affairs Committee, May 21, 2019.

¹² 2020 National Strategy, p. 14.

¹³ 31 U.S.C. 5318(i)(2), added by Section 312(a) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Pub. L. 107–56).

¹⁴ 81 FR 29398 (May 11, 2016).

¹⁵ 31 CFR 1010.230.

¹⁶ See U.S. Money Laundering Threat Assessment Working Group, U.S. Money Laundering Threat Assessment, pp. 48–49 (2005), <https://www.treasury.gov/resource-center/terrorist-illicit-finance/documents/mlta.pdf>. See also Miller, Rena S. and Rosen, Liana W., Beneficial Ownership Transparency in Corporate Formation, Shell Companies, Real Estate, and Financial Transactions, Congressional Research Service (July 8, 2019), <https://crsreports.congress.gov/product/pdf/R/R45798>. In promulgating the CDD Rule, FinCEN noted that the beneficial ownership collection and verification requirements imposed on financial institutions at the account opening stage for legal entities was one part of a strategy that also involved the collection of beneficial ownership information at the time of incorporation. See 81 FR 29398, 29401 (“[C]larifying and strengthening CDD is an important component of Treasury’s broader three-part strategy to enhance financial transparency of legal entities. Other key elements of this strategy include: (i) . . . the collection of beneficial ownership information at the time of the legal entity’s formation and (ii) facilitating global implementation of international standards

- Protect interstate and foreign commerce;
- Better enable critical national security, intelligence, and law enforcement efforts to counter money laundering, the financing of terrorism, and other illicit activity; and
- Bring the United States into compliance with international AML/CFT standards.²² Section 6403 of the CTA amends the BSA by adding a new section at 31 U.S.C. 5336 that requires the reporting of beneficial ownership information at the time of formation or registration, along with protections to ensure that the reported beneficial ownership information is maintained securely and accessed only by authorized persons for limited uses. The CTA requires the Secretary to promulgate implementing regulations that prescribe procedures and standards governing the reporting and use of such information, to include procedures governing the issuance of “FinCEN identifiers” for beneficial ownership information reporting.²³ The CTA requires FinCEN to maintain beneficial ownership information in a secure, non-public database that is highly useful to national security, intelligence, and law enforcement agencies, as well as federal functional regulators.²⁴

Through this ANPRM, FinCEN seeks input on how best to implement the reporting requirements of the CTA, as well as the CTA’s provisions regarding FinCEN’s maintenance and disclosure of reported information, from regulated parties; the governments of the states, U.S. possessions, local jurisdictions, and Indian tribes; law enforcement; regulatory agencies; other consumers of BSA data; and any other interested parties. FinCEN sets forth below specific questions based upon the statutory requirements and welcomes comments on any other issues relevant to the implementation of the CTA.²⁵

²² CTA Section 6402(5).

²³ See 31 U.S.C. 5336(b)(5), added by CTA Section 6403(a). How FinCEN will issue these identifiers, whether individuals and legal entities will use (and will need to be issued) different types of identifiers, and whether other types of identifiers may be useable as FinCEN identifiers are among the issues about which the CTA is silent. This ANPRM accordingly includes some questions relating to the FinCEN identifier.

²⁴ CTA Section 6402(7)(A), (8)(C). The Federal functional regulators are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, and any other federal regulator that examines financial institutions for compliance with the BSA. CTA Section 6003(3) (citing 15 U.S.C. 6809).

²⁵ The CTA requires FinCEN to undertake a separate process, subsequent to the issuance of a final rule on legal entity beneficial ownership

III. Requirements of the CTA

In general, the CTA requires a reporting company²⁶—in accordance with rules to be issued by FinCEN—to submit to FinCEN information that identifies the beneficial owner(s)²⁷ and applicant(s)²⁸ of the reporting company.²⁹ Specifically, reporting companies must report, for each identified beneficial owner and applicant, the following information: (i) Full legal name; (ii) date of birth; (iii) current residential or business street address; and (iv) a unique identifying number from an acceptable identification document or the individual’s FinCEN identifier.³⁰

The CTA defines a beneficial owner of an entity as an individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise (i) exercises substantial control over the entity, or (ii) owns or controls not less than 25 percent of the ownership interests of the entity.³¹ The CTA defines a reporting company as a corporation, LLC, or other similar entity that is (i) created by the filing of a document with a secretary of state or a similar office under the law of a state or Indian tribe, or (ii) formed under the law of a foreign country and registered to do business in the United States by the filing of a document with a secretary of state or a similar office under the laws of a state or Indian tribe. The CTA exempts certain categories of entities from the reporting requirement.³²

reporting, to revise CDD requirements for financial institutions in light of the new legal entity reporting requirements. While FinCEN welcomes comments in response to this ANPRM that address the effects of different design choices with respect to legal entity reporting on the ultimate shape of financial institution CDD requirements, persons wishing to comment on such issues should be aware that they will have another opportunity at a later time to comment on the revision of CDD requirements, when FinCEN undertakes that separate process.

²⁶ Defined at 31 U.S.C. 5336(a)(11), added by CTA Section 6403(a).

²⁷ Defined at 31 U.S.C. 5336(a)(3), added by CTA Section 6403(a).

²⁸ Defined at 31 U.S.C. 5336(a)(2), added by CTA Section 6403(a).

²⁹ 31 U.S.C. 5336(b)(1), (2)(A), added by CTA Section 6403(a).

³⁰ 31 U.S.C. 5336(b)(2)(A), added by CTA Section 6403(a).

³¹ 31 U.S.C. 5336(a)(3), added by CTA Section 6403(a). The definition contains certain exceptions, including, under certain circumstances: (i) Minors whose parent or guardian file their own beneficial ownership information; (ii) individuals who act as nominees, intermediaries, custodians, or agents; (iii) individuals acting solely as employees of an entity; (iv) individuals with interests through rights of inheritance; and (v) individuals who are creditors. See 31 U.S.C. 5336(a)(3)(B), added by CTA Section 6403(a).

³² 31 U.S.C. 5336(a)(11)(B), added by CTA Section 6403(a). The definition of reporting company

The CTA also requires that FinCEN issue a “FinCEN identifier” to an individual or entity that has submitted the required beneficial ownership information, if the individual or entity so requests.³³ A FinCEN identifier is to be a unique identifier for each individual or entity that may be used for subsequent reporting to FinCEN in lieu of providing certain other information.³⁴

The CTA requires FinCEN to maintain the reported beneficial ownership information in a secure, non-public database for not fewer than five years after the date on which the reporting company terminates.³⁵

The CTA prohibits the unauthorized disclosure of beneficial ownership information collected by FinCEN, including authorized recipients’ subsequent disclosures for unauthorized purposes.³⁶ Pursuant to the CTA, FinCEN may disclose beneficial ownership information upon receipt of: (i) A request, through appropriate protocols, from a federal agency engaged in national security, intelligence, or law enforcement activity, for use in furtherance of such activity;³⁷ (ii) a request, through appropriate protocols, from a non-federal law enforcement agency with specified court authorization;³⁸ (iii) a request from a federal agency on behalf of certain foreign requestors under specified conditions;³⁹ (iv) a request by a financial institution subject to CDD requirements, with the consent of the reporting company, to facilitate compliance with CDD requirements under applicable law;⁴⁰ and (v) a

specifically exempts 24 categories of entities, including certain types of registered entities (e.g., various companies registered under federal securities laws and the Commodity Exchange Act, FinCEN-registered money transmitters, and registered public accounting firms); banks; credit unions; public utility companies; certain tax exempt entities; entities with specified levels of operations in the United States; entities owned or controlled by other entities that qualify for one of several other specified exemptions; and certain kinds of dormant entities, among others. The Secretary, with the concurrence of the Attorney General and the Secretary of Homeland Security, may by regulation also exempt additional categories of entities.

³³ 31 U.S.C. 5336(b)(2)(A)(iv), (b)(3), added by CTA Section 6403(a).

³⁴ 31 U.S.C. 5336(a)(6), (b)(2)(A)(iv), (b)(3), added by CTA Section 6403(a).

³⁵ 31 U.S.C. 5336(c)(1), added by CTA Section 6403(a); CTA Section 6402(7).

³⁶ 31 U.S.C. 5336(c)(2)(A), added by CTA Section 6403(a).

³⁷ 31 U.S.C. 5336(c)(2)(B)(i)(I), added by CTA Section 6403(a).

³⁸ 31 U.S.C. 5336(c)(2)(B)(i)(II), added by CTA Section 6403(a).

³⁹ 31 U.S.C. 5336(c)(2)(B)(ii), added by CTA Section 6403(a).

⁴⁰ 31 U.S.C. 5336(c)(2)(B)(iii), added by CTA Section 6403(a).

request by a Federal functional regulator or other appropriate regulatory agency under certain circumstances.⁴¹ The CTA also authorizes officers and employees of the Department of the Treasury to access beneficial ownership information consistent with their official duties and subject to procedures and safeguards prescribed by the Secretary.⁴²

The CTA requires the Secretary to promulgate regulations prescribing procedures and standards governing beneficial ownership reporting and the FinCEN identifier by January 1, 2022.⁴³ These regulations will specify a subsequent effective date, which will be informed by information received pursuant to the notice and comment process. FinCEN intends to provide a reasonable timeframe for stakeholders to implement the regulations.

The regulations promulgated pursuant to the CTA are required to specify certain procedures, methods, and standards. Some of these specifications must be included in the regulations that are to be promulgated within a year of the CTA's enactment:

- Prescribing procedures and standards governing reporting of beneficial ownership information and any FinCEN identifier;⁴⁴
- Specifying the information required to be reported and the reporting method;⁴⁵
- Specifying the method for reporting changes in beneficial ownership (for both entities and persons holding FinCEN identifiers);⁴⁶ and
- Specifying reporting requirements for exempt subsidiaries and exempt grandfathered entities that cease to be exempt.⁴⁷

Others do not have to be included in the CTA regulations required by January 1, 2022, but the specific requirements of the reporting regulations that must be finalized by that date may affect these other specifications:

- The form and manner in which information shall be provided by FinCEN to a financial institution for CDD, and to certain regulatory agencies for certain purposes;⁴⁸

- Protocols to protect the security and confidentiality of beneficial ownership information, to include obligations on requesting agencies;⁴⁹ and

- Establishment of a safe harbor for persons seeking to amend previously submitted but inaccurate beneficial ownership information.⁵⁰

Further, the CTA requires the Secretary to take certain actions in developing these regulations. This includes an obligation to reach out to members of the small business community and other appropriate parties to ensure efficiency and effectiveness of the process for the entities subject to the requirements of the CTA.⁵¹ Additionally, in promulgating the required regulations prescribing procedures and standards governing reporting of beneficial ownership information and any FinCEN identifier, the CTA requires FinCEN, to the greatest extent practicable, to:

- Establish partnerships with State, local, and Tribal governmental agencies;
- Collect required identity information of beneficial owners through existing federal, state, and local processes and procedures;
- Minimize burdens on reporting companies associated with the collection of the required information, in light of the private compliance costs placed on legitimate businesses, including by identifying any steps taken to mitigate the costs relating to compliance with the collection of information; and
- Collect the required information in a form and manner that ensures the information is highly useful in (a) facilitating important national security, intelligence, and law enforcement activities, and (b) confirming beneficial ownership information provided to financial institutions in order to facilitate financial institutions' compliance with AML, CFT, and CDD requirements under applicable law.⁵²

IV. Questions for Comment

FinCEN invites comments on all aspects of the CTA, but specifically seeks comments on the questions listed below. FinCEN encourages commenters to reference specific question numbers to facilitate FinCEN's review of comments.

Definitions

(1) The CTA requires reporting of beneficial ownership information by "reporting companies," which are defined, subject to certain exceptions, as including corporations, LLCs, or any "other similar entity" that is created by the filing of a document with a secretary of state or a similar office under the law of a state or Indian tribe or formed under the law of a foreign country and registered to do business in the United States by the filing of such a document.

a. How should FinCEN interpret the phrase "other similar entity," and what factors should FinCEN consider in determining whether an entity qualifies as a similar entity?

b. What types of entities other than corporations and LLCs should be considered similar entities that should be included or excluded from the reporting requirements?

c. If possible, propose a definition of the type of "other similar entity" that should be included, and explain how that type of entity satisfies the statutory standard, as well as why that type of entity should be covered. For example, if a commenter thinks that state-chartered non-depository trust companies should be considered similar entities and required to report, the commenter should explain how, in the commenter's opinion, such companies satisfy the requirement that they be formed by filing a document with a secretary of state or "similar office."

(2) The CTA limits the definition of reporting companies to corporations, LLCs, and other similar entities that are "created by the filing of a document with a secretary of state or a similar office under the law of a State or Indian Tribe" or "registered to do business in the United States by the filing of a document with a secretary of state or a similar office under the laws of a State or Indian Tribe."

a. Does this language describe corporate filing practices and the applicable law of the states and Indian tribes sufficiently clearly to avoid confusion about whether an entity does or does not meet this requirement?

b. If not, what additional clarifications could make it easier to determine whether this requirement applies to a particular entity?

(3) The CTA defines the "beneficial owner" of an entity, subject to certain exceptions, as "an individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise" either "exercises substantial control over the entity" or "owns or controls not less than 25 percent of the ownership

⁴¹ 31 U.S.C. 5336(c)(2)(B)(iv), added by CTA Section 6403(a).

⁴² 31 U.S.C. 5336(c)(5), added by CTA Section 6403(a).

⁴³ 31 U.S.C. 5336(b)(5), added by CTA Section 6403(a).

⁴⁴ 31 U.S.C. 5336(b)(4)(A), added by CTA Section 6403(a).

⁴⁵ 31 U.S.C. 5336(b)(1)(A)–(C), (2)(A), added by CTA Section 6403(a).

⁴⁶ 31 U.S.C. 5336(b)(1)(D), (3)(A)(ii), added by CTA Section 6403(a).

⁴⁷ 31 U.S.C. 5336(b)(1)(B), (2)(D), (2)(E), added by CTA Section 6403(a).

⁴⁸ 31 U.S.C. 5336(c)(2)(C), added by CTA Section 6403(a).

⁴⁹ 31 U.S.C. 5336(c)(3), added by CTA Section 6403(a).

⁵⁰ 31 U.S.C. 5336(h)(3)(C), added by CTA Section 6403(a).

⁵¹ 31 U.S.C. 5336(g), added by CTA Section 6403(a).

⁵² 31 U.S.C. 5336(b)(1)(F), added by CTA Section 6403(a). FinCEN anticipates that fulfillment of these requirements will involve in-depth engagement with federal as well as state, local, and tribal government agencies.

interests of the entity.” Is this definition, including the specified exceptions, sufficiently clear, or are there aspects of this definition and specified exceptions that FinCEN should clarify by regulation?

a. To what extent should FinCEN’s regulatory definition of beneficial owner in this context be the same as, or similar to, the current CDD rule’s definition or the standards used to determine who is a beneficial owner under 17 CFR 240.13d–3 adopted under the Securities Exchange Act of 1934?

b. Should FinCEN define either or both of the terms “own” and “control” with respect to the ownership interests of an entity? If so, should such a definition be drawn from or based on an existing definition in another area, such as securities law or tax law?

c. Should FinCEN define the term “substantial control”? If so, should FinCEN define “substantial control” to mean that no reporting company can have more than one beneficial owner who is considered to be in substantial control of the company, or should FinCEN define that term to make it possible that a reporting company may have more than one beneficial owner with “substantial control”?

(4) The CTA defines the term “applicant” as an individual who “files an application to form” or “registers or files an application to register” a reporting company under applicable state or tribal law. Is this language sufficiently clear, in light of current law and current filing and registration practices, or should FinCEN expand on this definition, and if so how?

(5) Are there any other terms used in the CTA, in addition to those the CTA defines, that should be defined in FinCEN’s regulations to provide additional clarity? If so, which terms, why should FinCEN define such terms by regulation, and how should any such terms be defined?

(6) The CTA contains numerous defined exemptions from the definition of “reporting company.” Are these exemptions sufficiently clear, or are there aspects of any of these definitions that FinCEN should clarify by regulation?

(7) In addition to the statutory exemptions from the definition of “reporting company,” the CTA authorizes the Secretary, with the concurrence of the Attorney General and the Secretary of Homeland Security, to exempt any other entity or class of entities by regulation, upon making certain determinations.⁵³ Are there any

categories of entities that are not currently subject to an exemption from the definition of “reporting company” that FinCEN should consider for an exemption pursuant to this authority, and if so why?

(8) If a trust or special purpose vehicle is formed by a filing with a secretary of state or a similar office, should it be included or excluded from the reporting requirements?

(9) How should a company’s eligibility for any exemption from the reporting requirements, including any exemption from the definition of “reporting company,” be determined?

a. What information should FinCEN require companies to provide to qualify for these exemptions, and what verification process should that information undergo?

b. Should there be different information requirements for operating companies and holding companies, for active companies and dormant companies, or are there other bases for distinguishing between types of companies?

c. Should exempt entities be required to file periodic reports to support the continued application of the relevant exemption (e.g., annually)?

Reporting of Beneficial Ownership Information

(10) What information should FinCEN require a reporting company to provide about the reporting company itself to ensure the beneficial ownership database is highly useful to authorized users?

(11) What information should FinCEN require a reporting company to provide about the reporting company’s corporate affiliates, parents, and subsidiaries, particularly given that in some cases multiple companies can be layered on top of one another in complex ownership structures?

(12) Should a reporting company be required to provide information about the reporting company’s corporate affiliates, parents, and subsidiaries as a matter of course, or only when that information has a bearing on the reporting company’s ultimate beneficial owner(s)?

(13) What information, if any, should FinCEN require a reporting company to provide about the nature of a reporting company’s relationship to its beneficial owners (including any corporate intermediaries or any other contract, arrangement, understanding, or relationship), to ensure that the beneficial ownership database is highly useful to authorized users?

(14) Persons currently obligated to file reports with FinCEN overwhelmingly

do so electronically, either on a form-by-form basis or in batches using proprietary software developed by private-sector technology service providers.

a. Should FinCEN allow electronic filing of required information about reporting companies (including the termination of such companies), beneficial owners, and applicants under the CTA?

b. Should FinCEN allow or support any mechanisms other than direct electronic filing?

c. Should FinCEN allow or support direct batch filing of required information?

d. Should there be any differences among the mechanisms used for different types of information or different types of filers?

e. Should any additional or alternative reporting system involve the collection of information from the states and Indian tribes, and if so how?

f. Should the filing mechanisms for reporting companies be different for entities that were previously exempt for one reason or another (including exempt subsidiaries and exempt grandfathered entities under section 5336(b)(2)(D) and (E)) and lose that exemption? If so how?

(15) Section 5336(b)(2)(C) requires written certifications to be filed with FinCEN by exempt pooled investment vehicles described in section 5336(a)(11)(B)(xviii) that are formed under the laws of a foreign country.

a. By what method should these certifications be filed?

b. What information should be included in these certifications?

c. Should there be a mechanism through which such filings could be made to foreign authorities and forwarded to FinCEN, or should such filings have to be made directly to FinCEN?

d. What information should be included in these certifications (e.g., what information would allow authorities to follow up on certifications containing false information)?

e. Should these certifications be accessible to database users, and if so, should they be accessible on the same terms as beneficial ownership information of reporting companies?

(16) What burdens do you anticipate in connection with the new reporting requirements? Please identify any burdens with specificity, and estimate the dollar costs of these burdens if possible. How could FinCEN minimize any such burdens on reporting companies associated with the collection of beneficial ownership information in a manner that ensures the information is highly useful in

⁵³ 31 U.S.C. 5336(a)(11)(B)(xxiv), added by CTA Section 6403(a).

facilitating important national security, intelligence, and law enforcement activities and confirming beneficial ownership information provided to financial institutions, consistent with its statutory obligations under the CTA?

(17) Section 5336(e)(1) requires the Secretary to take reasonable steps to provide notice to persons of their reporting obligations.

a. What steps should be taken to provide such notice?

b. Should those steps include direct communications such as mailed notices, and if so to whom should notices be mailed?

c. What type of information should be included in such a notice, for example, the purposes and uses of the data, and how to access and correct the information?

d. Should the notice be followed by an explicit acknowledgement of the reporting company, or consent of the beneficial owner or applicant if the owner or applicant is submitting the information, to the handling of beneficial ownership information as stated in the notice and applicable law?

(18) Section 5336(e)(2) requires states and Indian tribes, as a condition of receiving certain funds, to have their Secretary of State or a similar office in each state or Indian tribe periodically provide notice of reporting obligations and a copy of, or internet link to, the reporting company form created by FinCEN.

a. How should this requirement be implemented?

b. What form should the notice take?

c. Should this notice be provided yearly, or on some other periodic schedule?

(19) What should reporting companies or individuals holding FinCEN identifiers be required to do to satisfy the requirement of section 5336(b)(1)(D) that they update in a timely manner the information they have submitted when it changes, such as when beneficial owners or holders of FinCEN identifiers (i) transfer substantial control to other individuals; (ii) change their legal names or their reported residential or business street addresses; or (iii) die; or (iv) when a previously acceptable identification document expires? For example, should the reporting companies or individuals be required to file a new report, or provide notice only of the information that has changed?

(20) Should reporting companies be required to affirmatively confirm the continuing accuracy of previously submitted beneficial ownership information on a periodic basis (e.g., annually)? How should such

confirmation be communicated to FinCEN?

(21) For those reporting companies without FinCEN identifiers, what should be considered a “timely manner”⁵⁴ for updating a change in beneficial ownership?

a. Should this period differ based on the type of reporting company?

b. What factors should be taken into account in determining this period?

c. How much time should reporting companies be given to update beneficial owner information upon a change of ownership?

d. What are the benefits or drawbacks of allowing a longer period to report a change of beneficial ownership?

(22) Section 5336(h)(3)(C) contains a safe harbor for persons who seek to correct previously submitted but inaccurate beneficial ownership information pursuant to FinCEN regulations. How should FinCEN’s regulations define the scope of this safe harbor? Should the nature of the inaccuracy (e.g., a misspelled address versus the complete omission of a beneficial owner) be relevant to the availability of the safe harbor?

(23) What steps should reporting companies be required to take to support and confirm the accuracy of beneficial ownership information?

a. Should reporting companies be required to certify the accuracy of their information when they submit it?

b. If so, what should this certification cover?

c. Should reporting companies be required to submit copies of a beneficial owner’s acceptable identification document?

(24) What steps should FinCEN take to ensure that beneficial ownership information being reported is accurate and complete?

a. With respect to other BSA reports, FinCEN e-filing protocols prohibit filings from being made with certain blank fields, and automatically format certain fields to ensure that letters are not entered for numbers and vice versa, etc. The filing protocols, however, do not involve independent FinCEN verification of information filed. Should FinCEN take similar or additional steps in connection with the filing of beneficial ownership information?

b. If so, what similar or additional steps should FinCEN take?

(25) Should a reporting company be required to report information about a company’s “applicant” or “applicants” (the individual or individuals who file the application to form or register a

reporting company) in any report after the reporting company’s initial report to FinCEN? Why or why not?

FinCEN Identifier

(26) In what situations will an individual or entity wish to use the FinCEN identifier? How can FinCEN best protect both the privacy interests underlying an individual’s or entity’s desire to use the FinCEN identifier, and the identifying information that must be provided to FinCEN by an individual or entity wishing to obtain and use the FinCEN identifier?

(27) What form should the FinCEN identifier take?

a. How long should it be?

b. Should it be alphabetical, numeric, or alphanumeric?

c. Should it contain embedded information such as a filing year, a geographic code, a sequential number, or numbers shared among related persons or entities, or should it be generated independently for each individual or entity?

d. Should it resemble or be derived from another identifier provided by another authority?

e. Should it resemble the document numbers of other reports filed with FinCEN under the BSA?

f. Should the form of FinCEN identifiers for individuals and legal entities be different? If so, how and why?

(28) How can FinCEN best ensure a one-to-one relationship between individuals or entities and their FinCEN identifiers, in light of the possibility that individuals and entities may mistakenly or intentionally attempt to apply for more than one FinCEN identifier?⁵⁵

(29) How can FinCEN best protect FinCEN identifiers from being used without individuals’ and entities’ authorization? Should protections include specific regulatory requirements or prohibitions?

(30) As noted in the CTA, in some cases multiple companies can be layered on top of one another in complex ownership structures. Given that there may be multiple entities within an ownership structure of a reporting company that are identified by FinCEN identifiers, how can FinCEN implement the FinCEN identifier in a way that reduces the burden to financial

⁵⁴ 31 U.S.C. 5336(b)(3)(A)(ii), added by CTA Section 6403(a).

⁵⁵ For example, this could happen when different employees of the same organization, without realizing, apply independently for a FinCEN identifier, or when an individual applies more than once using identity numbers from different forms of identification mistakenly thinking it is necessary to obtain a separate FinCEN identification for each company of which the individual is a beneficial owner.

institutions of using the FinCEN database when reporting companies with complex ownership structures seek to open an account?

(31) What should the process be to obtain a FinCEN identifier?

a. a) Should the FinCEN identifier be secured by an applicant or beneficial owner prior to filing an application to form a corporation, LLC, or other similar entity under the laws of a state or Indian tribe?

b. b) How, if at all, should FinCEN verify an individual's identity before providing a FinCEN identifier?

c. c) If an applicant or beneficial owner chooses not to apply for a FinCEN identifier, should FinCEN create any limitations—in addition to those in the statutory definition of “acceptable identification document”—on the types of unique identifying numbers that can be submitted?

Security and use of Beneficial Ownership and Applicant Information

(32) When a state, local, or tribal law enforcement agency requests beneficial ownership information pursuant to an authorization from a court of competent jurisdiction to seek the information in a criminal or civil investigation, how, if at all, should FinCEN authenticate or confirm such authorization?

(33) Should FinCEN provide a definition or criteria for determining whether a court has “competent jurisdiction” or has “authorized” such an order? If so, what definition or criteria would be appropriate?

(34) As a U.S. Government agency, FinCEN is subject to strict security and privacy laws, regulations, and other requirements that will protect the security and confidentiality of beneficial ownership and applicant information. What additional security and privacy measures should FinCEN implement to protect this information and limit its use to authorized purposes, which includes facilitating important national security, intelligence, and law enforcement activities as well as financial institutions' compliance with AML, CFT, and CDD requirements under applicable law? Would it be sufficient to make misuse of such information subject to existing penalties for violations of the BSA and FinCEN regulations, or should other protections be put in place, and if so what should they be?

(35) How can FinCEN make beneficial ownership information available to financial institutions with CDD obligations so as to make that information most useful to those financial institutions?

a. Please describe whether financial institutions should be able to use that information for other customer identification purposes, including verification of customer information program information, with the consent of the reporting company?

b. Please describe whether FinCEN should make financial institution access more efficient by permitting reporting companies to pre-authorize specific financial institutions to which such information should be made available?

c. In response to requests from financial institutions for beneficial ownership information, pursuant to 31 U.S.C. 5336(c)(2)(A), what is a reasonable period within which FinCEN should provide a response? Please also describe what specific information should be provided.

(36) How should FinCEN handle updated reporting for changes in beneficial ownership when beneficial ownership information has been previously requested by financial institutions, federal functional regulators, law enforcement, or other appropriate regulatory agencies?

a. If a requestor has previously requested and received beneficial ownership information concerning a particular legal entity, should the requester automatically receive notification from FinCEN that an update to the beneficial ownership information was subsequently submitted by the legal entity customer?

b. If so, how should this notification be provided?

c. Should a requesting entity have to opt in to receive such notification of updated reporting?

(37) One category of authorized access to beneficial ownership information from the FinCEN database involves “a request made by a Federal functional regulator or other appropriate regulatory agency.”⁵⁶ How should the term “appropriate regulatory agency” be interpreted? Should it be defined by regulation? If so, why and how?

(38) In what circumstances should applicant information be accessible on the same terms as beneficial ownership information (*i.e.*, to agencies engaged in national security, intelligence, or law enforcement; to non-federal law enforcement agencies; to federal agencies, on behalf of certain foreign requestors; to federal functional regulators or other agencies; and to financial institutions subject to CDD requirements). If financial institutions are not required to consider applicant information in connection with due

diligence on a reporting company opening an account, for example, should a financial institution's terms of access to applicant information differ from the terms of its access to beneficial ownership information?

Cost, Process, Outreach, and Partnership

(39) What specific costs would CTA requirements impose—in terms of time, money, and human resources—on small businesses? Are those costs greater for certain types of small businesses than others? What specifically can FinCEN do to minimize those costs, for all small businesses or for some types in particular?

(40) Are there alternatives to a single reporting requirement for all reporting companies that could create a less costly alternative for small businesses?

(41) How can FinCEN best reach out to members of the small business community to ensure the efficiency and effectiveness of the filing process for entities subject to the requirements of the CTA?

(42) Are there other business constituencies to which FinCEN should reach out, and if so, who are they?

(43) How can FinCEN best reach out to financial institutions to ensure the efficiency and effectiveness of the process by which financial institutions could potentially access the beneficial ownership information held by FinCEN?

(44) What burdens would CTA requirements impose on state, local, and tribal governmental agencies? In particular, what additional time, money, and human resources would state, local, and tribal governments have to secure and expend—or reallocate from other duties, and if the latter what duties would be compromised or services impaired? How, if at all, would any of these burdens or allocations of time or money vary according to the size or other characteristics of a jurisdiction—would smaller jurisdictions find it easier or harder to handle the costs associated with CTA requirements?

(45) How should FinCEN minimize any burdens on state, local, and tribal governmental agencies associated with the collection of beneficial ownership information, while still achieving the purposes of the CTA?

(46) How can FinCEN best partner with state, local, and tribal governmental agencies to achieve the purposes of the CTA?

(47) How can FinCEN collect the identity information of beneficial owners through existing Federal, state, local, and tribal processes and procedures?

⁵⁶ 31 U.S.C. 5336(c)(2)(B)(iv), added by CTA Section 6403(a).

a. Would FinCEN use of such processes or procedures be practicable and appropriate?

b. Would FinCEN use of or reliance on existing processes and procedures help to lessen the costs to state, local, and tribal government agencies, or would it increase those costs?

c. Would FinCEN use of existing Federal, state, local, and tribal processes and procedures help to lessen the costs to small businesses affected by CTA requirements, or would it increase those costs?

(48) The process of forming legal entities may have ramifications that extend beyond the legal and economic consequences for legal entities themselves, and the reporting of beneficial ownership information about legal entities may have ramifications that extend beyond the effect of mobilizing such information for AML/CFT purposes. How can FinCEN best engage representatives of civil society stakeholders that may not be directly affected by a beneficial ownership information reporting rule but that are concerned for such larger ramifications?

V. Regulatory Planning and Review

This advance notice of proposed rulemaking is a significant regulatory action under Executive Order 12866 and has been reviewed by the Office of Management and Budget.

VI. Conclusion

Implementing an effective system to identify, collect, and permit authorized uses of beneficial ownership information will strengthen U.S. national security and the integrity of the U.S. financial system, and protect people from harm. With this ANPRM, FinCEN seeks input on how FinCEN should implement such a system, consistent with the requirements of the CTA, to maximize benefits while minimizing burdens on reporting companies. FinCEN seeks input from the public on the questions set forth above, including from regulated parties; state, local, and Tribal governments; law enforcement; regulators; other consumers of BSA data; and any other interested parties. FinCEN also welcomes comments on all aspects of the ANPRM and any other aspects of implementation of the CTA. FinCEN encourages all interested parties to provide their views.

By the Department of the Treasury.

AnnaLou Tirol,

Deputy Director, Financial Crimes Enforcement Network.

[FR Doc. 2021-06922 Filed 4-1-21; 8:45 am]

BILLING CODE 4810-02-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 165

[Docket Number USCG-2021-0131]

RIN 1625-AA87

Security Zone; Christina River, Newport, DE

AGENCY: Coast Guard, Department of Homeland Security (DHS).

ACTION: Notice of proposed rulemaking.

SUMMARY: The Coast Guard is proposing to establish a security zone for the protection of Very Important Persons (VIPs) as they transit by vehicle on the route 141 bridge over the Christina River near Newport, Delaware. The security zone will be enforced intermittently and only during times of a protected VIP transit over the bridge and will restrict vessel traffic while the zone is being enforced. This proposed rulemaking would prohibit persons and vessels from entering or remaining within the security zone unless authorized by the Captain of the Port Delaware Bay or a designated representative. We invite your comments on this proposed rulemaking. **DATES:** Comments and related material must be received by the Coast Guard on or before May 5, 2021.

ADDRESSES: You may submit comments identified by docket number USCG-2021-0131 using the Federal eRulemaking Portal at <https://www.regulations.gov>. See the "Public Participation and Request for Comments" portion of the **SUPPLEMENTARY INFORMATION** section for further instructions on submitting comments.

FOR FURTHER INFORMATION CONTACT: If you have questions about this proposed rulemaking, call or email Petty Officer Jennifer Padilla, Sector Delaware Bay, Waterways Management Division, U.S. Coast Guard; telephone 215-271-4814, Jennifer.L.Padilla@uscg.mil.

SUPPLEMENTARY INFORMATION:

I. Table of Abbreviations

CFR Code of Federal Regulations
DHS Department of Homeland Security
FR Federal Register
NPRM Notice of proposed rulemaking
§ Section
U.S.C. United States Code
VIPs Very Important Persons

II. Background, Purpose, and Legal Basis

These VIP visits require the implementation of heightened security

measures for protection of VIPs who may travel on the route 141 bridge over the Christina River in Newport, Delaware. Due to the roadway passing over the Christina River, this security zone is necessary to protect VIPs, the public, and the surrounding waterway. To date in the year 2021 there have been 4 requests for security zones at this location. As a result, the Coast Guard had to issue numerous temporary security zones. Continued requests for this security zone are expected through 2024.

The purpose of this proposed rulemaking is to protect the VIPs and the public from destruction, loss, or injury from sabotage, subversive acts, or other malicious or potential terrorist acts. The Coast Guard is proposing this rulemaking under authority in 46 U.S.C. 70034 (previously 33 U.S.C. 1231).

III. Discussion of Proposed Rule

The Captain of the Port Delaware Bay (COTP) is proposing to establish a security zone for the protection of Very Important Persons (VIPs) as they transit by vehicle on the route 141 bridge over the Christina River near Newport, Delaware. This rule is necessary to expedite the establishment and enforcement of this security zone when short notice is provided to the COTP for VIPs traveling over the route 141 bridge. The security zone is bounded on the east by a line drawn from 39°42.55' North Latitude (N), 075°35.88' West Longitude (W), thence southerly to 39°42.50' N, 075°35.87' W proceeding from shoreline to shoreline on the Christina River in a westerly direction where it is bounded by the South James Street Bridge at 39°42.63' N, 075°36.53' W. No vessel or person would be permitted to enter the security zone without obtaining permission from the COTP or a designated representative. The regulatory text we are proposing appears at the end of this document.

IV. Regulatory Analyses

We developed this proposed rule after considering numerous statutes and Executive orders related to rulemaking. Below we summarize our analyses based on a number of these statutes and Executive orders, and we discuss First Amendment rights of protestors.

A. Regulatory Planning and Review

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits. This NPRM has not been designated a "significant regulatory action," under

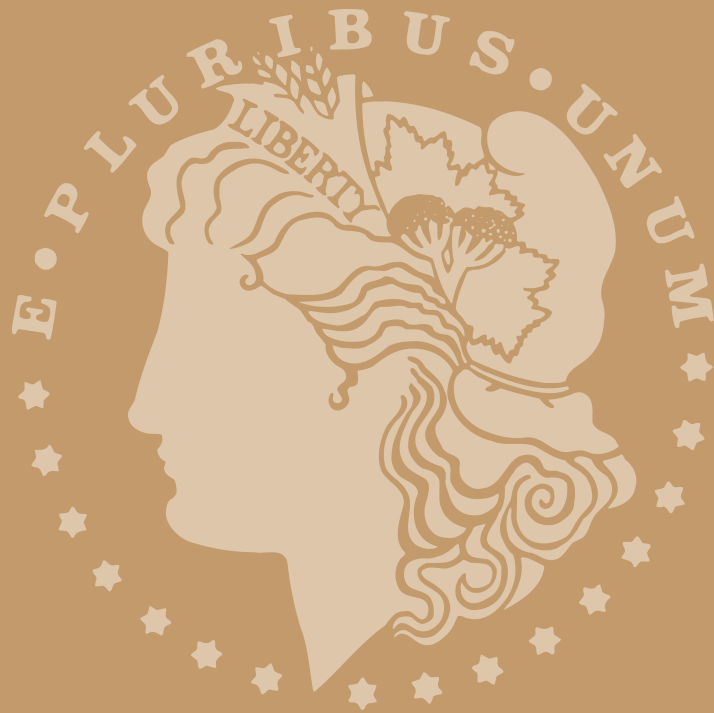


ProBank Austin

Thank you for your participation in today's seminar. We value your feedback, comments and suggestions. Your evaluation of our programs helps us to develop the best, most practical and comprehensive programs possible.

Complete your evaluation online from any computer, tablet, or mobile device using the link ProBank will email to you at the completion of the program. If a multiple-day program, you will receive your link on the last day.

*Thank you.
ProBank Austin*



ProBank Austin

950 Breckenridge Lane, Suite 280, Louisville, KY 40207

(800) 523-4778

www.probank.com