

For Verification of Attendance for CRCM, <https://probank.cnf.io>

- ▶ Navigate to <https://probank.cnf.io> and tap the session titled "VIRGINIA BANKERS ASSOCIATION - BSA SCHOOL - DAY 1"
- ▶ OR just point your phone's camera at the QR code to join directly



1

Wednesday, February 16
NEW YORK DEPOSIT DOCUMENTATION 9:00am - 4:00pm ▶ Mark Burnside
REAL ESTATE LENDING COMPLIANCE - DAY 1 9:00am - 4:00pm ▶ Andrea Cohen
VIRGINIA BANKERS ASSOCIATION - BSA SCHOOL - DAY 1 9:00am - 4:00pm ▶ Mark W. Cover
COMPLIANCE OFFICER BOOT CAMP - DAY 2 10:00am - 5:00pm ▶ Leah Hamilton
DEPOSIT ACCOUNTS FOR MINORS 2:00pm - 3:30pm ▶ K. Natalie Straus
Thursday, February 17
VIRGINIA BANKERS ASSOCIATION - BSA SCHOOL - DAY 2 9:00am - 4:00pm ▶ Mark W. Cover
ADVANCED TRIO 10:00am - 5:00pm ▶ Mark Burnside
COMPLIANCE OFFICER BOOT CAMP - DAY 3 10:00am - 5:00pm ▶ Leah Hamilton
HELOCs: START TO FINISH 10:00am - 1:00pm ▶ Andrea Cohen

2

The screenshot shows the ProBank Austin login interface. The header includes the ProBank Austin logo and the URL "https://www.probankaustin.com/secure/login". The main section is titled "Check in To This Session" and contains the following fields and buttons:

- Username:** A text input field with the value "Blank".
- Password:** A text input field with the value "Owner".
- Email Address:** A text input field with the value "mlb@probank.com".
- On the Web CPE Credit:** A dropdown menu with "No" selected.
- How to identify:** A dropdown menu with "In Person" selected.
- Check in Now:** A blue button.
- Sign Up to Bank:** A grey button.

A blue oval callout bubble with the text "Check 'No' for CPEs" points to the "On the Web CPE Credit" dropdown menu.

3

The screenshot shows the ProBank Austin dashboard after a successful login. The header includes the ProBank Austin logo and the URL "https://www.probankaustin.com/secure/dashboard". The main section contains the following elements:

- Check Out of Session:** A green button.
- Logout:** A green button.
- Good Job!** A green banner with a checkmark icon.
- Thank you for logging in!** A grey banner.
- Sign Out:** A grey button.

4

Vendor Opportunities - AML / Risk Management

(NOTE: Not a ProBANK Austin endorsement of any product or vendor.)

- Verafin – FRAMLx = Fraud Detection + AML” www.verafin.com
- “BAM+” - BSA and Anti-Money Laundering System – Abrigo www.abrigo.com
- “Patriot Officer” - GlobalVision Systems Inc. (Oliver Song) www.gv-systems.com
- Fortent “Best Practice AML Solution” (www.fortent.com) – link to IBM.
- FIServ – “Financial Crime Risk Management (FCRM)” // www.fiserv.com
- FIS (Fidelity Information Systems) – AML Compliance Mgmt. www.fisglobal.com
- Bridger Insight/Choicepoint – “AML Compliance Software” – http.secure.bridgerinsight.choicepoint.com-
- Mantas – “Anti-Money Laundering” – www.mantas.com
- SAS – “Anti-Money Laundering,” “Money Laundering Detection,” www.SAS.com
- COCC – Sentry Services AML Solution – www.cocc.com
- Rdc Inc. -- AML Edge & AML XP - www.rdc.com
- ‘Suspicious Activity Monitor’ - Wayne Barnett Software, www.barnettsoftware.com
- “Yellow Hammer BSA” - Jack Henry // www.jackhenrybanking.com
- Accuity (formally Thompson TFP) - Solutions for AML et al. www.AccuitySolutions.com.
- GIFTS Software – “GIFTSWEB EDD” www.giftssoft.com
- Wolters Kluwer/PCi -- “Wiz Sentri BSA/AML”, www.wolterskluwerfs.com
- CSI – “BSA/AML/Fraud Solutions” – www.csiweb.com/Solutions
- BankDetect – RiskTracker – AML www.bankdetect.com
- Actimize – “CDD Solution” – with LexisNexis – www.actimize.com
- Focus Technology- “ML Shield” – www.FocusTechnologyGroup.com
- Accurint – “Locate and Research Tool” – part of LexisNexis // www accurint.com
- Bouton and Associates – “BSA Tracker”, www.gisbanker.com
- DCI Inc. – BSA Navigator - www.datacenterinc.com/bsa_navigator.aspx

ProBANK
Advisor
Trusted
Compliance
Advice.



5



Dating
or
Defrauding?

A NATIONAL AWARENESS CAMPAIGN

6

6

FINANCIAL CRIMES

ENFORCEMENT NETWORK

HOME

ABOUT

RESOURCES

NEWSROOM

CAREERS

ADVISORIES

GLOSSARY

Search

Joint Release: Federal Agencies Launch Joint Effort to Alert Online Daters and Social Media Users of Romance Scams That Have Cost Americans Millions

Contact:
CFTC, Donna Faulk-White: Dfaulk-white@cftc.gov
CFPB, Raul Cisneros: press@consumerfinance.gov
DHS/ICE, Mike Alvarez: icemedia@ice.dhs.gov
U.S. Postal Inspection Service, Jessica Adams: ISMediaInquiries@uspis.gov
FinCEN, Jayna Desai: press@fincen.gov
Immediate Release: February 07, 2022

WASHINGTON—Today, five federal agencies joined forces to remind the public about the ongoing dangers of romance scams. The Commodity Futures Trading Commission, the Consumer Financial Protection Bureau (CFPB), the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE), the U.S. Postal Inspection Service, and the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) have launched *Dating or Defrauding?*, a national awareness effort to alert the public to romance scams that target victims largely through dating apps or social media. The campaign is supported by [USAGov/Outreach](#), a division of the U.S. General Services Administration's Technology Transformation Services.

Romance scams are not new, but with the proliferation of online dating apps, social media, and even messaging apps, new types of scams are emerging that target new audiences and have drained victims of millions of dollars. According to the Federal Trade Commission (FTC), 2020 was a record year for romance scams. Consumer reports to the FTC indicate that the number of romance scam complaints continued to increase through 2021. A year-over-year comparison through the third quarter showed a 48 percent increase in reported romance frauds.

The joint federal agencies' initiative shows the public how to recognize the scams before they give any money or assets and provides steps to take if they are victimized. Over the coming weeks, the interagency Dating or Defrauding? awareness campaign will reach the public via social media, local and national media outreach, and public-private partnerships to encourage them to be vigilant when making online love connections.

This effort is spearheaded through the following federal agency offices: CFTC's Office of Customer Education and Outreach, CFPB's Office for Older Americans, DHS/ICE's Homeland Security Investigations, the U.S. Postal Inspection Service, and Treasury's FinCEN.

7

Dating or Defrauding? Protect Yourself Against Romance Scams With Help From the Government

Dating
or
Defrauding?

A NATIONAL AWARENESS CAMPAIGN

According to the FBI's Internet Crime Complaint Center (IC3), in 2020 alone, people who experienced romance scams lost over \$600M. Romance scammers target people looking for love on dating apps and social media. But how can you tell the difference between dating or defrauding?

From February 7 to March 11, join agencies from across the government as they help you protect your heart and your wallet. Learn how to recognize romance scams and report them to the right authorities.

Explore the 'Dating or Defrauding?' campaign, what agencies are participating in the effort and where to go online or on the phone for help.

8

Abo

Federal Reserve Releases Synthetic Identity Fraud Mitigation Toolkit to Educate, Fight Fraud

02/08/22

[Back to Press Releases](#)

fedpaymentsimprovement.org

Federal Reserve Releases Synthetic Identity Fraud Mitigation Toolkit to Educate, Fight Fraud

The Federal Reserve today released a [Synthetic Identity Fraud Mitigation Toolkit](#) to provide financial institutions, consumers and businesses with an online repository of insights and resources on synthetic identity fraud.

"Synthetic identity fraud, where fraudsters create an identity out of pieces of real and/or fictitious information, continues to grow and resulted in an estimated \$20 billion in losses (Off-site) for U.S. financial institutions in 2020," said Jim Cunha, executive vice president, Federal Reserve Bank of Boston. "Following years of research and collaboration with fraud experts, the Fed is taking the next step to support the payments industry in its battle against synthetic identity fraud by developing this toolkit."

The toolkit is designed to increase awareness about this type of fraud, enable the payments industry to better identify and fight it, and foster payments industry collaboration to improve synthetic identity fraud mitigation.

The initial release of the toolkit includes downloadable resources that focus on the following:

- Synthetic Identity Fraud: The Basics – explains what synthetic identity fraud is, why you should care, and why fraudsters commit this type of fraud.
- How Synthetic Identities are Used – describes what is hiding in your portfolio and how fraudsters use synthetics to commit fraud and increase their payouts.
- When Synthetics Become a Reality – additional information on common synthetic use cases.
- Detecting a Synthetic Identity – provides tools to help colleagues and consumers identify and prevent synthetic identity fraud.

The second release of the toolkit later this year will expand on the insights and resources in the toolkit's initial release with next-level strategies for validating identities and detecting suspected synthetic identity fraud.

9

HOW TO SPOT A SYNTHETIC

SOCIAL SECURITY NUMBER INFORMATION MISMATCH

- Multiple identities tied to the same Social Security number
- Social Security number issued after 2011, but customer date of birth is before this date (e.g., 1995)

INCONSISTENCIES IN CREDIT PROFILE INFORMATION

- Anticipated credit file depth does not match customer information provided. For example, the customer lists a date of birth as 01/01/1980, but the credit file is less than 12 months old
- Use of secured lines to quickly establish credit, with no other tradelines
- High number of authorized user accounts with few to no individual liability accounts

CUSTOMER ACCOUNT INFORMATION LINKS TO OTHER, ALREADY ESTABLISHED ACCOUNTS BELONGING TO OTHER CUSTOMERS

- Same address, phone number or digital footprint information (such as IP address)

VELOCITY CHECKS AGAINST THE CUSTOMER INFORMATION PROVIDED: WAS THE CUSTOMER CONTACT INFORMATION RECENTLY ISSUED?

- Email address, phone number or other contact information that was issued less than 12 months ago may be indicative of a synthetic identity

10

10

FINANCIAL CRIMES

ENFORCEMENT NETWORK

HOME

ABOUT

RESOURCES

NEWSROOM

CAREERS

ADVISO

Enter the terms you wish to search for.

Search

FinCEN Issues Proposed Rule for Suspicious Activity Report Sharing Pilot Program to Combat Illicit Finance Risks

Contact: press@fincen.gov
 Immediate Release: January 24, 2022
 External Link: [Pilot Program on Sharing of Suspicious Activity Reports and Related Information...](#)

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today issued a [Notice of Proposed Rulemaking \(NPRM\)](#) that proposes and solicits public comment on the establishment of a limited-duration pilot program for sharing suspicious activity reports (SARs), in accordance with Section 6212 of the Anti-Money Laundering Act of 2020.

The pilot program would permit a financial institution with a SAR reporting obligation to share SARs and information related to SARs with the institution's foreign branches, subsidiaries, and affiliates for the purpose of combating illicit finance risks, subject to approval and conditions set by FinCEN. The proposed rule aims to ensure that the sharing of information is limited by the requirements of federal and state law enforcement, takes into account potential concerns of the intelligence community, and is subject to appropriate standards and requirements regarding data security and the confidentiality of personally identifiable information.

"This NPRM builds on the experience that FinCEN has gained in administering existing pilot programs and once finalized, will assist financial institutions in further combating illicit finance risks. We expect that the pilot program will provide valuable feedback to FinCEN as longer-term approaches towards SAR sharing with foreign affiliates are considered," said FinCEN Acting Director Himamauli Das. "We urge stakeholders to provide input to assist us in developing a program that will help combat illicit finance risks and promote enterprise-wide risk management, while ensuring adequate safeguards are in place to protect SAR confidentiality."

FinCEN's previously issued guidance on sharing SARs within a corporate organizational structure stated that financial institutions may share SARs with foreign head offices, controlling companies (whether domestic or foreign), and domestic affiliates. If finalized, the proposed rule would establish a limited-duration pilot program to allow SAR sharing with foreign affiliates, which would also provide FinCEN with valuable feedback about the value of such SAR sharing for participating financial institutions and for FinCEN and law enforcement.

The proposed rule seeks public comment on questions related to the establishment of a SAR sharing pilot program, such as expected costs and benefits, technical challenges, the merits of quarterly reporting, and how to protect SAR confidentiality. Answers to these questions will help inform the final rule that FinCEN issues and the annual Congressional briefings that FinCEN is required to provide.

FinCEN strongly encourages all interested parties, including those that may want to participate in the SAR sharing pilot program when it is finalized, to submit written comments. Comments on the NPRM should be submitted by March 28, 2022.

11


Pilot Program on Sharing of Suspicious Activity Reports and Related Information with Foreign Branches, Subsidiaries and Affiliates

- RFC – Published on 01/25/22
- 87 FR 3719 – 3729
- Comment Due March 28, 2022

12

12

FINANCIAL CRIMES



ENFORCEMENT NETWORK

HOME

ABOUT

RESOURCES

NEWSROOM

CAREERS

ADVISORIES

GLOSSARY

Search

FDIC and FinCEN Launch Digital Identity Tech Sprint

Contact: Brian Sullivan, FDIC
 202-412-1436
brsullivan@fdic.gov

Jayna Desai, FinCEN
 703-905-3770
Jayna.Desai@fincen.gov

FDIC: PR-3-2022
Immediate Release: January 11, 2022

WASHINGTON – The Federal Deposit Insurance Corporation (FDIC) and the Financial Crimes Enforcement Network (FinCEN) today announced a Tech Sprint to develop solutions for financial institutions and regulators to help measure the effectiveness of digital identity proofing—the process used to collect, validate, and verify information about a person. Through the Tech Sprint, FDIC’s tech lab (FDITECH) and FinCEN seek to increase efficiency and account security; reduce fraud and other forms of identity-related crime, money laundering, and terrorist financing; and foster customer confidence in the digital banking environment.

Digital identity proofing is a foundational element to enable digital financial services to function properly. This element is challenged by the proliferation of compromised personally identifiable information (PII), the increasing use of synthetic identities, and the presence of multiple, varied approaches for identity proofing. The FDIC and FinCEN ask Tech Sprint participants to answer the following question:


“What is a scalable, cost-efficient, risk-based solution to measure the effectiveness of digital identity proofing to ensure that individuals who remotely (i.e., not in person) present themselves for financial activities are who they claim to be?”

In the coming weeks, FDIC and FinCEN will open registration for this Tech Sprint. Interested individuals will have approximately two weeks to submit applications. The Tech Sprint will encompass a review of applications, grouping of individuals into teams that will work together over approximately three weeks to develop solutions to this challenge question, and invitations to participate in a virtual “Demo Day” of short team presentations to a panel of experts for evaluation.

At the conclusion of the Tech Sprint, the FDIC will publish all team presentations and recognize teams based on several criteria detailed in the forthcoming prize notice. Neither the FDIC nor FinCEN are offering monetary prizes associated with the Tech Sprint. Additional questions about the Tech Sprint can be sent to Innovation@FDIC.gov. Read more about FDIC and FinCEN’s Tech Sprint, [Measuring the Effectiveness of Digital Identity Proofing for Digital Financial Services](#)

###

13



Why FDITECH

What We Do

Sprint Program

Rapid Phased Prototyping

Featured

Join Us

Sprint Program

A tech sprint program brings a diverse set of stakeholders (e.g., non-profits, private sector individuals/companies, and academics) together in collaborative settings for a short period of time to intensely focus on creating solutions to challenges of importance to the organization hosting the tech sprint. A ‘sprint’ simply refers to a short period (typically 2-3 weeks) where teams turn ideas into value. The hosting organization will provide the problem statement and selected teams will devote their collective energy and expertise towards addressing specific challenges. A tech sprint will culminate with a Demonstration Day where each team shares findings with a panel of evaluating experts.

14

Measuring the Effectiveness of Digital Identity Proofing for Digital Financial Services

Remotely-delivered financial services, a phenomenon already growing but accelerated by the pandemic, depend on digital technology for successful execution. Digital technology also plays a core role in the compliance aspects of remotely-delivered financial services, from client onboarding and identification, to customer due diligence and anti-money laundering responsibilities, to risk management. Cost effective and efficient technology solutions ensure these financial services are broadly available and affordable, particularly for resource-constrained firms like community banks.

Digital identity proofing is a foundational element to enable digital financial services to function properly. This element is challenged by the proliferation of compromised personally identifiable information (PII), the increasing use of synthetic identities, and the presence of multiple, varied approaches to identity proofing. Simultaneously, technological developments are enabling dynamic identity evidence such as state mobile driver's licenses (mDLs) or other identity credentials that are frequently updatable and interoperable, as well as behavioral analytics. The FDIC and FinCEN seek solutions to measure the effectiveness of digital identity proofing for greater reliance in assessment and calibration of risks, by having Tech Sprint participants answer the question:

"What is a scalable, cost-efficient, risk-based solution to measure the effectiveness of digital identity proofing to ensure that individuals who remotely (i.e., not in person) present themselves for financial activities are who they claim to be?"

Ideally, the solutions developed from this Tech Sprint will inform future FDIC, FinCEN, and industry-led efforts, plans, and programs to increase efficiency and account security; reduce fraud and other forms of identity-related financial crime, money laundering, and terrorist financing; and foster customer confidence in the digital banking environment.

15

Considerations

There is no "one size fits all" approach to this problem. Innovations developed for this Tech Sprint could encompass a range of outcomes such as:

- developing a scoring model for digital identity proofing sources and processes;
- findings and research-backed observations on how to enhance assessing existing solutions;
- applications of artificial intelligence/machine learning programs to identify and "red flag" questionable identities leading to dynamic scoring; or
- creating other technical solutions that help answer the question posed by the problem statement.

Participants may focus on any aspect of the problem statement, and as that focus is developed, the FDIC and FinCEN encourages consideration of the following questions:

- Does the solution include new or unique data, processes, or technologies that could enhance assurance of the legitimacy of digital identity evidence, including new forms of authoritative source identifiers when onboarding new customers in a remote banking environment?
- Does the solution consider new forms of digital identifiers from authoritative sources, such as state motor vehicle administrations or the Social Security Administration? Is the solution interoperable or compatible with the multitude of platforms used by financial services firms, particularly community banks?
- Does the solution consider applicability to identity proofing that may apply to a multitude of financial products, including legacy financial products and evolving digital assets?
- How might community banks, the largest financial institutions, and third-party service providers partner to collectively determine and test the solution?
- How might the solution improve the risk and compliance process or align identity confidence with a risk profile?
- What would a technical implementation of the solution look like, and how might it be implemented sector-wide? What role should government play in such an implementation, if any?
- Is the solution cost-effective and scalable to any size financial institution, including community banks, does it create value for other business applications, and can it be easily implemented and understood by non-technical staff?

16

How to Participate

Registration will be required and will be available on this webpage by the end of January 2022 for all participants.

Individuals who are interested in participating should submit a registration form. The Tech Sprint will encompass a review of submissions, grouping of individuals into teams that will work together over approximately three weeks to develop solutions to this challenge question, and invitations to participate in a "Demo Day" of short team presentations to a panel of experts for evaluation.

At the conclusion of the Tech Sprint, the FDIC will publish all team presentations and recognize teams based on several criteria detailed in the forthcoming prize notice. Neither the FDIC nor FinCEN are offering monetary prizes associated with the Tech Sprint.

A tentative timeline for the Measuring the Effectiveness of Digital Identity Proofing for Digital Financial Services Tech Sprint follows (dates are subject to change); please check back frequently as more information becomes available:

End of January 2022: Registration opens.

Mid-February 2022: Registration closes.

End of February 2022: FDIC and FinCEN review registration applications and invite a select number of individuals to participate in the Tech Sprint. FDIC and FinCEN will form teams from individuals selected to participate that will work together on their proposed solution for a period of approximately three weeks.

Mid-March 2022: Selected teams come together for a Demonstration Day with a panel of expert judges.

Additional questions about this Tech Sprint can be sent to innovation@FDIC.gov

17

FINANCIAL CRIMES



ENFORCEMENT NETWORK

HOME ABOUT RESOURCES NEWSROOM CAREERS ADVISORIES GLOSSARY

Search

FDIC and FinCEN Open Registration for Digital Identity Tech Sprint

Contact:

Brian Sullivan, FDIC
202-412-1436
bsullivan@fdic.gov

Jayna Desai, FinCEN
703-905-3770
Jayna.Desai@fincen.gov

Immediate Release: February 01, 2022

WASHINGTON – The Federal Deposit Insurance Corporation (FDIC) and the Financial Crimes Enforcement Network (FinCEN) today opened the registration period for interested parties to participate in a Tech Sprint to help measure the effectiveness of digital identity proofing—the process used to collect, validate, and verify information about a person.

Through the Tech Sprint, FDIC's tech lab (FDITECH) and FinCEN seek to increase efficiency and account security; reduce fraud and other forms of identity-related crime, money laundering, and terrorist financing; and foster customer confidence in the digital banking environment. Read more about FDIC and FinCEN's Tech Sprint, [Measuring the Effectiveness of Digital Identity Proofing for Digital Financial Services](#)

Digital identity proofing is a foundational element to enable digital financial services to function properly. This element is challenged by the proliferation of compromised personally identifiable information (PII), the increasing use of synthetic identities, and the presence of multiple, varied approaches for identity proofing. The FDIC and FinCEN seek participants to answer the following question:

“What is a scalable, cost-efficient, risk-based solution to measure the effectiveness of digital identity proofing to ensure that individuals who remotely (i.e., not in person) present themselves for financial activities are who they claim to be?”

Interested individuals may submit applications requesting participation by 5 p.m. ET on February 15, 2022. Additional questions about the Tech Sprint can be sent to innovation@FDIC.gov.

18

HOME
ABOUT
RESOURCES
NEWSROOM
CAREERS
ADVISORIES
GLOSSARY

Search

FinCEN Launches Regulatory Process for New Real Estate Sector Reporting Requirements to Curb Illicit Finance

RE_ANPRM_FRN_120321_FINAL_508.pdf
577.27 KB

Contact: press@fincen.gov
Immediate Release: December 06, 2021

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) announced today an [Advance Notice of Proposed Rulemaking \(ANPRM\)](#) to solicit public comment on a potential rule to address the vulnerability of the U.S. real estate market to money laundering and other illicit activity. The systemic money laundering vulnerabilities presented by the U.S. real estate sector, and consequently, the ability of illicit actors to launder criminal proceeds through the purchase of real estate, threatens U.S. national security and the integrity of the U.S. financial system.

FinCEN has long been concerned with the potential for corrupt officials and illicit actors to launder the proceeds of criminal activity through the purchase of real estate in the United States and has worked to increase transparency in the real estate sector. Given the relative stability of the real estate sector as store of value, the opacity of the real estate market, and gaps in industry regulation, the U.S. real estate market continues to be used as a vehicle for money laundering and can involve businesses and professions that facilitate (even if unwittingly) acquisitions of real estate in the money laundering process.

Real estate transactions involving loans or other financing by regulated financial institutions, such as banks, which are subject to federal anti-money laundering rules, are less susceptible to money laundering because those institutions are required to report suspicious activity to FinCEN. For example, when most American families buy a home with a mortgage, the bank that makes the loan is subject to rules that require it to identify the buyer and report suspicious activity. In contrast, when real estate is purchased without such financing, it can be nearly impossible to trace the beneficial owners behind shell companies that are often used to purchase the real estate. As a result, corrupt officials and criminals engaging in illicit activity can exploit the U.S. real estate sector to launder their ill-gotten wealth.

The ANPRM announced today will assist FinCEN in preparing a proposed rule that would enhance the transparency of the domestic real estate market on a nationwide basis and protect the U.S. real estate market from exploitation by criminals and corrupt officials.

19

86 FR 69589 – 69602 – 12/08/21

87 FR 7068 – 7069 – Comment Period

Extended till 02/21/22 on 02/08/22

86 FR 69589 – 69602 – 12/08/21

87 FR 7068 – 7069 – Comment Period

Extended till 02/21/22 on 02/08/22

86 FR 69589 – 69602 – 12/08/21

87 FR 7068 – 7069 – Comment Period

Extended till 02/21/22 on 02/08/22

20



Administ

Fact Sheet: U.S. Strategy on Countering Corruption

DECEMBER 06, 2021 • STATEMENTS AND RELEASES

"Corruption threatens United States national security, economic equity, global anti-poverty and development efforts, and democracy itself. But by effectively preventing and countering corruption and demonstrating the advantages of transparent and accountable governance, we can secure a critical advantage for the United States and other democracies."

President Joe Biden
June 3, 2021

Corruption is a cancer within the body of societies—a disease that eats at public trust and the ability of governments to deliver for their citizens. The deleterious effects of corruption impact nearly all aspects of society. It exacerbates social, political, and economic inequality and polarization; impedes the ability of states to respond to public health crises or to deliver quality education; degrades the business environment and economic opportunity; drives conflict; and undermines faith in government. Those that abuse positions of power for private gain steal not just material wealth, but human dignity and welfare.

21

UNITED STATES STRATEGY ON COUNTERING CORRUPTION

<https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf>

PURSUANT TO THE NATIONAL SECURITY STUDY
MEMORANDUM ON ESTABLISHING THE FIGHT AGAINST
CORRUPTION AS A CORE UNITED STATES NATIONAL
SECURITY INTEREST

DECEMBER 2021



THE WHITE HOUSE
WASHINGTON

22



TABLE OF CONTENTS

INTRODUCTION	4
THE IMPACTS OF CORRUPTION.....	6
OUR APPROACH.....	8
STRATEGIC PILLARS	9
PILLAR ONE: Modernizing, Coordinating, and Resourcing U.S. Government Efforts to Better Fight Corruption.....	9
PILLAR TWO: Curbing Illicit Finance.....	10
PILLAR THREE: Holding Corrupt Actors Accountable	11
PILLAR FOUR: Preserving and Strengthening the Multilateral Anti-Corruption Architecture.....	13
PILLAR FIVE: Improving Diplomatic Engagement and Leveraging Foreign Assistance Resources to Advance Policy Objectives.....	13

23

Curbing illicit finance: Corrupt actors and their facilitators rely on vulnerabilities in the United States and international financial systems to obscure ownership of assets and launder the proceeds of their illicit activities. As the world's largest economy, the United States bears responsibility to address gaps in our own regulatory system and work with our allies and partners to do the same. This means addressing deficiencies, including by:

- Issuing beneficial ownership transparency regulations that help identify bad actors hiding behind opaque corporate structures.
- Enacting first-of-their-kind regulations that target those closest to real estate transactions to reveal when real estate is used to hide ill-gotten cash or to launder criminal proceeds.
- Working with the Congress and within existing regulations to make it harder for certain gatekeepers to the financial system – including lawyers, accountants, and trust and company service providers – to evade scrutiny.
- Working with partner countries through multilateral fora, diplomatic engagement, law enforcement cooperation, and capacity building to strengthen their anti-money laundering regimes to bring greater transparency to the international financial system.

24

24

Computer-Security Incident Notification – Final Rule 11/23/2021 – 86 FR 66424 - 66444

November 18, 2021

Agencies approve final rule requiring computer-security incident notification

Board of Governors of the Federal Reserve System

Federal Deposit Insurance Corporation

Office of the Comptroller of the Currency

For release at 3:00 p.m. EST

Share 

Federal bank regulatory agencies today announced the approval of a final rule to improve the sharing of information about cyber incidents that may affect the U.S. banking system. The final rule requires a banking organization to notify its primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after the banking organization determines that a cyber incident has occurred. Notification is required for incidents that have materially affected—or are reasonably likely to materially affect—the viability of a banking organization's operations, its ability to deliver banking products and services, or the stability of the financial sector.

In addition, the final rule requires a bank service provider to notify affected banking organization customers as soon as possible when the provider determines that it has experienced a computer-security incident that has materially affected or is reasonably likely to materially affect banking organization customers for four or more hours.

Compliance with the final rule is required by May 1, 2022.

25

--

(4) *Computer-security incident* is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

(7) *Notification incident* is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's—

- (i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;
- (ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or
- (iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

(8) *Person* has the same meaning as set forth at 12 U.S.C. 1817(6)(8)(A).

26

Revisions to Operating Circular 5

Summary of Key Changes

Effective June 30, 2021, the Federal Reserve Banks are amending Operating Circular 5, Electronic Access. These revisions are designed to provide further guidance and detail related to notifying the Reserve Banks of any information loss or security incident involving an Electronic Connection. The changes are mostly reflected in Section 1.4, although Section 5.0 and Appendix A are also impacted.

Section 1.4 previously required that each Institution notify the Reserve Banks of any monetary or information loss, or security incident involving an Electronic Connection. The revisions to Section 1.4 expand upon that requirement by providing specific contact information for notifications and describing in more detail the circumstances in which such notice is required. To help ensure that Institutions provide the notice, Section 5.0 and Appendix A were amended to require that Institutions and their Service Providers document, within their applicable policies and procedures, the requirement to notify the Reserve Banks via the specific contact information provided.

A redlined version reflecting all changes to the prior version of Operating Circular 5 (dated October 15, 2020) will remain available on [FRBservices.org](https://frbbservices.org) during the transition window. The definitive text of revised Operating Circular 5 is also posted on [FRBservices.org](https://frbbservices.org).

Your continued use of Federal Reserve Bank services on or after June 30, 2021 constitutes agreement to the new terms of the operating circular.

27

The Institution or its Service Provider must immediately notify the Reserve Banks by telephone at (888) 333-7010, with written confirmation via email at ccc.technical.support@kc.frb.org, of any suspected, threatened or known cyber event, fraud, malware detection, compromise, or other security incident or breach, that relates to or has the potential to impact an Electronic Connection, Access Control Feature, or the use of a Reserve Bank financial service, including (but not limited to) circumstances in which the Institution or the Service Provider have a reasonable basis to know or suspect that such event:

- impacts or may impact software or hardware that the Institution or Service Provider use to engage or interface with an Electronic Connection or an Access Control Feature;
- impacts or may impact software or data stored on servers or other electronic media shared with Reserve Bank data or applications;
- impacts or may impact hardware, software or data that are used to generate transactions, messages, or other information that will be transmitted through an Electronic Connection;
- caused or may have caused the Institution or its Service Provider to generate an unauthorized transaction;
- causes or may cause the Institution or Service Provider to modify its operations while investigating or mitigating the impact of the event;
- requires notification by the Institution or its Service Provider to its prudential regulator, or by a Service Provider to the Institution, pursuant to any law, regulation, or supervisory requirement;
- resulted in or may have resulted in the loss of, unauthorized access to, compromise of, or tampering with an Access Control Feature; or
- resulted or may have resulted in the unauthorized disclosure or use of Confidential Information or the Security Procedures described in Appendix A.

28

28



CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS

Office of Consumer Affairs and Business Regulation
DIVISION OF BANKS

1000 Washington Street, 10th Floor, Boston, MA 02118-6400
(617) 956-1500 Fax (617) 956-1599 TDD (617) 956-1577
www.Mass.Gov/DOB

MIKE KENNEALY
SECRETARY OF HOUSING AND
ECONOMIC DEVELOPMENT

EDWARD A. PALLESCCHI
UNDERSECRETARY

MARY L. GALLAGHER
COMMISSIONER

September 23, 2021

To the Chief Executive Officer Addressed:

RE: Supervisory Alert Regarding Charging Multiple Non-Sufficient Fund Fees (NSF) for Representation of Unpaid Transactions

This Supervisory Alert is to make the industry aware of a developing consumer protection issue related to the disclosure of representation non-sufficient funds (NSF) fees which may present possible legal risk and/or risk of regulatory scrutiny to financial institutions. The Division conducts comprehensive reviews of consumer protection laws and regulations and verifies that financial institutions provide consumer account disclosures which are clear and conspicuous. Regulation DD which implements the Truth-in-Savings Act,¹ Regulation E which implements the Electronic Fund Transfers Act,² Massachusetts General Laws chapter 93A section 2(a), and Section 5(a) of the Federal Trade Commission Act³ regarding Unfair or Deceptive Acts or Practices (UDAP) establish guidelines and business standards requiring product disclosures and terms to have sufficiently clear and conspicuous information for consumers to make reasonable and informed financial decisions. Financial institutions should clearly disclose the amount of any fees and how fees may be imposed in connection with deposit accounts to avoid possible confusion by consumers and potential for heightened risk of deceptive practices.

What is a Representation Fee?

Financial institutions commonly charge a NSF fee when a merchant transaction is presented for payment from a consumer account and declined due to the customer having insufficient funds to cover the transaction. A representation NSF fee may occur when a merchant attempts to present the same transaction again in an effort to obtain the declined funds. This type of repeated merchant payment transaction can trigger the assessment of multiple NSF fees by a depository institution if the transaction is presented more than once. For example, if an Automated Clearing Housing (ACH) or other item is presented for payment and declined due to insufficient funds and subsequently represented for payment and declined again due to insufficient funds, some financial institutions will charge a NSF fee for both the original presentment and each representation thereafter.

29

Consumer protection risks associated with the representation of NSF fees

Recent class action lawsuits against financial institutions have alleged breach of contract due to the omission of important terms related to the assessment of representation fees. Some suits have eventually settled, resulting in customer reimbursements and legal fees.

Standard industry deposit account agreements and fee schedules supplied by vendors who provide payment processing software or services to financial institutions may not properly explain an institution's actual NSF fee practice as disclosed to the customer. While some disclosures and account agreements explain that one NSF fee will be charged "per item" or "per transaction," these commonly used forms may not consistently explain that the same processed item may trigger multiple NSF fees. In other words, when an item has already been declined one or more times and is represented again by the merchant seeking payment, multiple NSF fees may be triggered for the customer which may be an inconsistent practice with what was disclosed to the customer.

Additionally, deposit account disclosure and agreement practices are reviewed by state and federal financial regulators for unfair and/or deceptive acts or practices. Violations of state or federal UDAP laws may result in the payment of restitution and/or civil money penalties by financial institutions that charge representation fees.

We want to alert you of the potential legal, regulatory, and UDAP risks related to the relevant account disclosures and account agreements, and we strongly recommend that you review all applicable disclosures and processes to ensure that you are in compliance with the above referenced laws and regulations. Questions to consider are whether NSF fees are being charged as expected either through an internal system or third-party service provider. Furthermore, you may want to review deposit disclosures and contract language to ensure the manner in which NSF fees are charged is being communicated clearly and consistent to what a consumer could reasonably expect.

While regulatory policies around representation are under review and subject to further development, be advised that active and future examinations may require corrective measures based on examination findings. If you have questions about the Division's policy expectations regarding representation fees, please call Deputy Commissioner of Consumer Protection and Outreach, Mayte Rivera, at 617 956-1557 or at mayte.rivera@mass.gov.

Thank you for your attention to this matter.

Sincerely,

Mary L. Gallagher
Commissioner of Banks

30

FINANCIAL CRIMES

ENFORCEMENT NETWORK

HOME

ABOUT ▾

RESOURCES ▾

NEWSROOM ▾

CAREERS ▾

ADVISORIES

GLOSSARY

Agencies Invite Comment on Proposed Rule under Bank Secrecy Act

Immediate Release: October 23, 2020

The Financial Crimes Enforcement Network (FinCEN) and the Federal Reserve Board today invited comment on a proposed rule that would amend the recordkeeping and travel rule regulations under the Bank Secrecy Act. FinCEN and the Board, pursuant to their shared authority, are proposing amendments to the recordkeeping rule jointly, while FinCEN, pursuant to its sole authority, is proposing amendments to the travel rule.

Under the current recordkeeping and travel rule regulations, financial institutions must collect, retain, and transmit certain information related to funds transfers and transmittals of funds over \$3,000. The proposed rule lowers the applicable threshold from \$3,000 to \$250 for international transactions. 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.

Comments will be accepted for 30 days after publication in the *Federal Register*.

Read the Notice of Proposed Rulemaking [here](#).

###

31

NATIONAL DEFENSE AUTHORIZATION ACT for FY 2021 // P.L. 166-92

- An Act to authorize appropriations for fiscal year 2021 for military activities of the Department of Defense, and for other purposes.
- Division F – Anti-Money Laundering Act (AMLA) 2020
- Titles LXI through LXV, including the Corporate Transparency Act.

32

Anti-Money Laundering Act (AMLA)

- Enacted as part of the National Defense Authorization Act for FY 2021, AMLA 2020 includes substantial reforms and changes to modernize BSA, including:
 - Beneficial Ownership “changes” – through the Corporate Transparency Act – companies will provide Beneficial Ownership information to FinCEN during the process of formation or registration of the company – how this impacts DFIs is unclear until regulations are promulgated by Treasury – one year time limit;
 - Address inefficiencies in SAR and CTR filing – process, forms and dollar reporting limits;

-33-



33

Anti-Money Laundering Act (AMLA) (cont.)

- Increasing penalties for BSA and AML violations – including additional “damages” for repeat offenders, increased monetary amounts, and new prohibitions imposed on those who commit “egregious” violations of BSA;
- Expand definition of “financial institution” within BSA to include a “person engaged in the trade of antiquities”. AMLA also expands the definition of “monetary instrument” to include “values that substitute for currency” (virtual currencies); and
- Multiple GAO and Treasury studies (7) – including CTRs, beneficial ownership, TBML, money laundering by China, et al.

-34-



34

Anti-Money Laundering Act (AMLA)(cont.)

- Greater government resources to address money laundering – FinCEN to establish domestic liaisons and well as foreign intelligence units stationed in U.S. Embassies;
- Treasury to publish public priorities for anti-money laundering and the countering the financing of terrorism policy. These priorities must be consistent with the national strategy for countering the financing of terrorism and related forms of illicit finance – priorities were published on June 30th – DFIs will have to incorporate them into their programs, once regulation is promulgated ;
- “BSA-specific” whistleblower incentives and protections; and
- “Legally-Formalize” The FinCEN Exchange process to facilitate a voluntary public-private information sharing partnership among law enforcement agencies, national security agencies, financial institutions, and FinCEN

35

35



ANTI-MONEY LAUNDERING ACT OF 2020

Message from the FinCEN Director: 180-Day Update on AML Act Implementation and Achievements (June 30, 2021)

AML/CFT Priorities (AML Act Section 6101)
[AML/CFT Priorities \(June 30, 2021\)](#)
[Statement for Banks \(June 30, 2021\)](#)
[Statement for Non-Bank Financial Institutions \(June 30, 2021\)](#)
[News Release \(June 30, 2021\)](#)

Arts and Antiquities (AML Act Section 6110)
[Advance Notice of Proposed Rulemaking \(September 23, 2021\)](#)
[News Release \(September 23, 2021\)](#)
[Notice \(March 9, 2021\)](#)

Threat Pattern and Trend Information (AML Act Section 6206)
[Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in Bank Secrecy Act Data \(December 20, 2021\)](#)
[Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 \(October 15, 2021\)](#)

Financial Crimes Tech Symposium (AML Act Section 6211)
[FinCEN Statement \(February 24, 2021\)](#)

SAR Sharing Pilot Program (AML Act Section 6212)
[News Release \(January 24, 2022\)](#)
[Notice of Proposed Rulemaking \(January 24, 2022\)](#)

Review of Regulations and Guidance (AML Act Section 6216)
[News Release \(December 14, 2021\)](#)
[Request for Information \(December 14, 2021\)](#)

Assessment of No-Action Letters (AML Act Section 6305)
[News Release \(June 30, 2021\)](#)
[Report \(June 28, 2021\)](#)

Corporate Transparency Act || Beneficial Ownership (AML Act Title LXIV (Sections 6401-6403))
[Notice of Proposed Rulemaking \(NPRM\) \(December 7, 2021\)](#)
[NPRM News Release \(December 7, 2021\)](#)
[NPRM Fact Sheet \(December 7, 2021\)](#)
[Advance Notice of Proposed Rulemaking \(ANPRM\) \(April 5, 2021\)](#)
[ANPRM News Release \(April 1, 2021\)](#)

36

FINANCIAL CRIMES



ENFORCEMENT NETWORK

HOME

ABOUT

RESOURCES

NEWSROOM

CAREERS

ADVISORIES

GLOSSARY

FinCEN Seeks Comments on Modernization of U.S. AML/CFT Regulatory Regime

Contact: Office of Strategic Communications, press@fincen.gov
Immediate Release: December 14, 2021

WASHINGTON — Today, FinCEN is issuing a request for information (RFI) *Federal Register :: Public Inspection: Review of Bank Secrecy Act Regulations and Guidance* seeking comments on ways to streamline, modernize, and update the anti-money laundering and countering the financing of terrorism (AML/CFT) regime of the United States. FinCEN is particularly interested in comments on ways to modernize risk-based AML/CFT regulations and guidance, issued pursuant to the Bank Secrecy Act (BSA) so that they, on a continuing basis, protect U.S. national security in a cost-effective and efficient manner. Today's RFI also supports FinCEN's efforts to conduct a formal review of BSA regulations and related guidance, which is required by Section 6216 of the Anti-Money Laundering Act of 2020. FinCEN will report to Congress the findings of the review, including administrative and legislative recommendations.

"We recognize that the illicit finance threat landscape continues to evolve and that technology and innovation now play an important role in the efficient application of resources to combat illicit finance. I urge all relevant stakeholders to review the RFI and comment on ways that FinCEN can modernize AML/CFT regulations and guidance and better promote a risk-based approach to AML/CFT compliance," said FinCEN Acting Director Himamauli Das.

This formal review will help FinCEN ensure that BSA regulations and guidance continue to safeguard the U.S. financial system from threats to national security posed by various forms of financial crime, and that BSA reporting and recordkeeping requirements continue to be highly useful in countering financial crime. The formal review also will allow FinCEN to identify regulations and guidance that are outdated, redundant, or otherwise do not promote a risk-based AML/CFT compliance regime for financial institutions, or that do not conform with U.S. commitments to meet international AML/CFT standards. In consultation with specified stakeholders, FinCEN will make appropriate changes to regulations and guidance, as appropriate, to improve their efficiency. In addition, the formal review will assist FinCEN in identifying recommendations for administrative and legislative changes.

FinCEN strongly encourages all interested parties (including regulated entities; state, local, and Tribal governments; law enforcement; regulators; and other consumers of BSA data) to submit written comments, which will help inform FinCEN's report to Congress. Comments should be submitted by February 14, 2022.

37

Modernization of AML/CFT Regime

12/15/21

- 86 FR 71201 –
- 71207
- 26 Questions to
- “stimulate”
- thought

Financial Crimes Enforcement Network

31 CFR Chapter X

[Docket No. FINCEN-2021-0008]

Review of Bank Secrecy Act Regulations and Guidance

AGENCY: Financial Crimes Enforcement Network, Treasury.

ACTION: Request for information and comment.

SUMMARY: The Financial Crimes Enforcement Network (FinCEN) is issuing this request for information (RFI) to solicit comment on ways to streamline, modernize, and update the anti-money laundering and countering the financing of terrorism (AML/CFT) regime of the United States. In particular, FinCEN seeks comment on ways to modernize risk-based AML/CFT regulations and guidance, issued pursuant to the Bank Secrecy Act (BSA), so that they, on a continuing basis, protect U.S. national security in a cost-effective and efficient manner. This RFI also supports FinCEN's ongoing formal review of BSA regulations and guidance required pursuant to Section 6216 of the Anti-Money Laundering Act of 2020 (the AML Act). Section 6216 requires the Secretary of the Treasury (the Secretary) to solicit public comment and submit a report, in consultation with specified stakeholders, to Congress by January 1, 2022, that contains the findings and determinations that result from the formal review, including administrative and legislative recommendations.

DATES: Written comments on this RFI must be received on or before February 14, 2022.

38

AMLA 2020 – New Penalties

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).

39



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

40

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.

41

FINANCIAL CRIMES



ENFORCEMENT NETWORK

HOME

ABOUT

RESOURCES

NEWSROOM

CAREERS

ADVISORIES

GLOSSARY

Search

FinCEN Launches Regulatory Process For New Antiquities Regulations

Contact: Strategic Communications, 703-905-3770
Immediate Release: September 23, 2021

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today issued an Advance Notice of Proposed Rulemaking (ANPRM) to solicit public comment on a range of questions related to the implementation of amendments to the Bank Secrecy Act (BSA) regarding the trade in antiquities. This ANPRM is the first in a series of regulatory actions that FinCEN will undertake to implement Section 6110 of the Anti-Money Laundering Act of 2020 (AML Act), which became law on January 1, 2021 (see [The Anti-Money Laundering Act of 2020](#) | [FinCEN.gov](#) for more details on FinCEN's implementation of that legislation).

"This regulatory action demonstrates FinCEN's continued commitment to implement the AML Act," said Acting Director Himamauli Das. "I encourage industry and other stakeholders to comment on this ANPRM, which will strengthen the outcome of the rulemaking process."

Section 6110 of the AML Act amended the BSA by including as a type of financial institution a person engaged in the trade of antiquities, including an advisor, consultant, or any other person who engages as a business in the solicitation or the sale of antiquities. Section 6110 requires the Secretary of the Treasury to issue proposed rules to carry out the amendment.

The trade in antiquities may be exploited by money launderers and terrorist financiers to evade detection by law enforcement and to launder their illicit funds through the U.S. financial

42

citizen, lawfully permanent resident or the United States as defined by the Immigration and Nationality Act, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person located in the United States.”¹⁰ It also defines “United States Infrastructure as a Service Provider” to mean “any United States Person that offers any Infrastructure as a Service Product.”¹¹

a. What should the Department consider when determining whether a foreign subsidiary of a parent U.S. IaaS provider entity would be subject to the regulations implementing E.O. 13984? What implications for international commerce would there be, if any, if foreign subsidiaries were covered by the rule?

Overarching Inquiries:

(13) What key differences in industry makeup, market dynamics, and general business practices should be taken into consideration when drafting E.O. 13984’s proposed rule language compared with similar regulatory frameworks in other industries (such as the Financial Crimes Enforcement Network’s Customer Due Diligence and 311 Special Measure regulations)?

(14) Foreign malicious cyber actors often are able to acquire and provide fake names, government documents, and other identification records, making it increasingly difficult for IaaS providers to verify identities in a timely fashion. Do commenters believe that the Department should place more emphasis on ongoing customer-due-diligence efforts instead of initial Account creation requirements? How might this approach better accomplish E.O. 13984’s goal to deter foreign

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network

31 CFR Chapter X

RIN 1506-AB50

Anti-Money Laundering Regulations for Dealers in Antiquities

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 the implementation of Section 6110 of the Anti-Money Laundering Act of 2020 (the AML Act). AML Act Section 6110 amends the Bank Secrecy Act (BSA) to include in the definition of “financial institution” a “person engaged in the trade of antiquities, including an advisor, consultant, or any other person who engages as a business in the solicitation or the sale of antiquities, subject to regulations prescribed by the Secretary [of the Treasury].” The AML Act requires the Secretary of the Treasury (the Secretary) to issue proposed rules to carry out that amendment not later than 360 days after enactment of the AML Act. This ANPRM seeks initial public comment on questions that will assist FinCEN in preparing the proposed rules.

DATES: Written comments are welcome, and must be received on or before October 25, 2021.

ADDRESSES: Comments may be submitted, identified by Regulatory Identification Number (RIN) 1506-AB50.

preparing proposed rules to implement Section 6110(a)(1) of the AML Act.¹ AML Act Section 6110(a)(1) amends the BSA by adding to the BSA’s definition of “financial institution” “a person engaged in the trade of antiquities, including an advisor, consultant, or any other person who engages as a business in the solicitation or the sale of antiquities, subject to regulations prescribed by the Secretary.”² Section 6110(b)(1) requires the Secretary to issue proposed rules not later than 360 days after enactment of the AML Act to carry out that amendment.

II. Background

A. The BSA

Enacted in 1970 and amended most recently by the AML Act, the BSA aids in the prevention of money laundering, terrorism financing, and other illicit financial activity. 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.”³

Congress has authorized 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 Pursuant to this authority, FinCEN is authorized to impose anti-money laundering (AML) and countering the financing of terrorism (CFT) program requirements for financial institutions. Specifically, to guard against money laundering and the financing of terrorism through financial

43

FINANCIAL CRIMES



ENFORCEMENT NETWORK

[HOME](#)
[ABOUT](#)
[RESOURCES](#)
[NEWSROOM](#)
[CAREERS](#)
[ADVISORIES](#)
[GLOSSARY](#)

FinCEN Issues Proposed Rule for Beneficial Ownership Reporting to Counter Illicit Finance and Increase Transparency

Contact: press@fincen.gov
Immediate Release: December 07, 2021

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today issued a [Notice of Proposed Rulemaking \(NPRM\)](#) to implement the beneficial ownership information reporting provisions of the Corporate Transparency Act (CTA). The proposed rule is designed to protect the U.S. financial system from illicit use and impede malign actors from abusing legal entities, like shell companies, to conceal proceeds of corrupt and criminal acts. Such abuses undermine U.S. national security, economic fairness, and the integrity of the U.S. financial system.

The proposed rule addresses, among other things, who must report beneficial ownership information, when they must report, and what information they must provide. Collecting this information and providing access to law enforcement, financial institutions, and other authorized users will diminish the ability of malign actors to hide, move, and enjoy the proceeds of illicit activities.

“FinCEN is taking aggressive aim at those who would exploit anonymous shell corporations, front companies, and other loopholes to launder the proceeds of crimes, such as corruption, drug and arms trafficking, or terrorist financing,” said Acting FinCEN Director Himamauli Das.

Reflecting the Biden Administration’s commitment to curbing corruption and increasing transparency, the proposed rule will be further highlighted at the forthcoming Summit for Democracy. The proposed rule also reflects stated concerns in the newly released [U.S. Government Strategy on Countering Corruption](#), which addresses the money laundering risks posed by anonymous shell companies as well as the need to protect the international financial system from abuse by corrupt and other illicit actors. It is also consistent with the efforts of the Financial Action Task Force and G7 and G20 leaders to curtail the ability of illicit actors to hide wealth behind anonymous shell companies.

The CTA, part of the Anti-Money Laundering Act of 2020, established beneficial ownership information reporting requirements for certain types of corporations, limited liability companies, and other similar entities created in or registered to do business in the United States. The proposed rule implements these reporting requirements and reflects FinCEN’s careful consideration of public comments received in response to its April 5, 2021, [Advance Notice of Proposed Rulemaking](#) on the same topic. The proposed rule represents the culmination of years of bipartisan efforts by Congress, the Treasury, national security agencies, law enforcement, and other stakeholders to bolster the United States’ corporate transparency framework. FinCEN is committed to implementing these statutory obligations in a robust manner while minimizing burdens on reporting companies.

As part of a whole-of-government commitment to democracy, Treasury is taking a number of actions to fight corruption and prevent it from undermining trust in democratic institutions. In addition to this NPRM, on December 6, FinCEN announced an [Advance Notice of Proposed Rulemaking](#) to solicit public comment on a potential rule to address the vulnerability of the U.S. real estate market to money laundering and other illicit activity. Treasury is uniquely equipped to combat corruption at home and abroad by strengthening the U.S. financial system to prevent corrupt and other illicit actors from hiding or using their illicit proceeds in the United States.

FinCEN strongly encourages all interested parties, including those that would be affected by the proposed beneficial ownership information reporting rule, to submit written comments. Comments on the NPRM will be accepted for 60 days following publication in the [Federal Register](#).

[Fact Sheet: Beneficial Ownership Information Reporting Notice of Proposed Rulemaking](#)

###

44

86 FR 69920 – 69974 – 12/08/21

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: Notice of proposed rulemaking
(NPRM).
SUMMARY: FinCEN is promulgating
proposed regulations to require certain
entities to file reports with FinCEN that
identify two categories of individuals:
The beneficial owners of the entity; and
individuals who have filed an
application with specified governmental
authorities to form the entity or register
it to do business. The proposed
regulations would implement Section
6403 of the Corporate Transparency Act
(CTA), enacted into law as part of the
National Defense Authorization Act for
Fiscal Year 2021 (NDAA), and describe
who must file a report, what
information must be provided, and
when a report is due. Requiring entities
to submit beneficial ownership and
company applicant information to
FinCEN is intended to help prevent and
combat money laundering, terrorist
financing, tax fraud, and other illicit
activity. Once finalized, these proposed
regulations will affect a large number of
entities doing business in the United
States. This document also invites
comments from the public regarding all
aspects of the proposed regulations as
well as comments in response to
specific questions.
DATES: Written comments on this
proposed rule may be submitted on or
before February 7, 2022.
ADDRESSES: Comments may be
submitted by any of the following
methods:

1
b
d
p
o
b
o
b
b
F
p
b
r
e
t
b
c
i
c
b
b
i
s
l
a
r
e
t
s
o
n
b
i
A
l
p
n
C
C
p
k
a
t
s
v
e.

45

Key Elements of the Proposed Beneficial Ownership Information Reporting Regulation

The Notice of Proposed Rulemaking would help stop bad actors from using legal entities to hide illicit funds behind anonymous shell companies or other opaque corporate structures.

The proposed rule describes who must file a BOI report, what information must be reported, and when a report is due. Specifically, the proposed rule would require reporting companies to file reports with FinCEN that identify two categories of individuals: (1) the beneficial owners of the entity; and (2) individuals who have filed an application with specified governmental or tribal authorities to form the entity or register it to do business.

Reporting Companies

- The proposed rule identifies two types of reporting companies: domestic and foreign. A domestic reporting company would include a corporation, limited liability company, or any other entity created by the filing of a document with a secretary of state or similar office under the law of a state or Indian tribe. A foreign reporting company would include a corporation, limited liability company, or other entity formed under the law of a foreign country and that is registered to do business in any state or tribal jurisdiction. Under the proposed rule and in keeping with the CTA, twenty-three types of entities would be exempt from the definition of "reporting company."
- FinCEN expects that these definitions would include limited liability partnerships, limited liability limited partnerships, business trusts, and most limited partnerships, in addition to corporations and LLCs, because such entities appear typically to be created by a filing with a secretary of state or similar office.
- Other types of legal entities, including certain trusts, would appear to be excluded from the definitions to the extent that they are not created by the filing of a document with a secretary of state or similar office. FinCEN recognizes that the creation of many trusts does not involve the filing of such a formation document. The NPRM, however, seeks public comment on state and Indian Tribe law practices regarding trust formation to better understand and define the scope of the rule.

Beneficial Owners

- Under the proposed rule, a beneficial owner would include any individual who (1) exercises substantial control over a reporting company, or (2) owns or controls at least 25 percent of the ownership interests of a reporting company. The proposed regulation defines the terms "substantial control" and "ownership interest" and sets forth standards for determining whether an individual owns or controls 25 percent of the ownership interests of a reporting company. In keeping with the CTA, the proposed rule exempts five types of individuals from the definition of "beneficial owner."
- In defining the contours of who has "substantial control," the proposed rule sets forth a range of activities that could constitute "substantial control" of a company. This list would capture anyone who is able to make significant decisions on behalf of the entity. FinCEN's approach is designed to close loopholes that would allow corporate structuring that obscures owners or decision-makers. This is crucial to unmasking shell companies.

46

Company Applicants

- In the case of a domestic reporting company, the proposed rule defines a company applicant to be the individual who files the document that forms the entity. In the case of a foreign reporting company, a company applicant would be the individual who files the document that first registers the entity to do business in the United States.
- In both cases, the proposed regulation specifies that anyone who directs or controls the filing of the relevant document by another would also be a company applicant.

Beneficial Ownership Information Reports

- When filing BOI reports with FinCEN, the proposed rule would require a reporting company to identify itself and report four pieces of information about each of its beneficial owners and company applicants: name, birthdate, address, and a unique identifying number from an acceptable identification document (and the image of such document).
- If an individual provides his or her BOI to FinCEN, the individual can obtain a "FinCEN Identifier," which can then be provided to FinCEN in lieu of other required information about the individual.
- The proposed regulations also include a voluntary mechanism to allow reporting of the Taxpayer Identification Number (TIN) for a beneficial owner or company applicant.

Timing

- Under the proposed rule, BOI report timing would depend on (1) when a reporting company was created or registered, and (2) whether the report at issue is an initial report, an updated report providing new information, or a report correcting erroneous information in a previous report.
- Domestic reporting companies created before the effective date of the final regulation would have a year to file their initial reports; reporting companies created or registered after the effective date would have 14 days after their formation to file. The same deadlines would apply to existing and newly registered foreign reporting companies.
- Reporting companies would have 30 days to file updates to their previously filed reports, and 14 days to correct inaccurate reports after they discover or should have discovered the reported information is inaccurate.

Next Steps

- The comment period for the NPRM is open for sixty days until February 7, 2022.
- The BOI reporting NPRM is one of three rulemakings planned to implement the CTA. FinCEN will engage in additional rulemakings to (1) establish rules for who may access BOI, for what purposes, and what safeguards will be required to ensure that the information is secured and protected; and (2) revise FinCEN's customer due diligence rule following the promulgation of the BOI reporting final rule.
- In addition, FinCEN is developing the infrastructure to administer these requirements, such as the beneficial ownership information technology system.

47

U.S. Treasury Department
FINANCIAL CRIMES ENFORCEMENT NETWORK

HOME ABOUT RESOURCES NEWSROOM CAREERS ADVISORIES GLOSSARY Search

FinCEN Statement Regarding Beneficial Ownership Information Reporting and Next Steps

Immediate Release: February 08, 2022

The Financial Crimes Enforcement Network (FinCEN) notes that the comment period to the December 8, 2021 notice of proposed rulemaking (NPRM) requiring the reporting of beneficial ownership information (BOI) (the "Reporting NPRM") has closed. FinCEN received over 230 comments.

The Reporting NPRM is the first in a series of rulemakings that FinCEN will issue to implement the Corporate Transparency Act (CTA). The next step in the CTA rulemaking series will be FinCEN's publication of proposed rules on BOI access and disclosure requirements (the "Access NPRM"), which FinCEN anticipates publishing later this year.

Some commenters requested the opportunity to submit, supplement, or amend, their comments on the Reporting NPRM after having the opportunity to review the Access NPRM. FinCEN is considering these requests. FinCEN anticipates that the dates of any reopened comment period would be published in the Federal Register in conjunction with the Access NPRM.

FinCEN appreciates the many comments on the Reporting NPRM that have already been submitted. FinCEN strongly encourages all interested parties, including those that may be affected by the proposed beneficial ownership information reporting rule, to review the Access NPRM once issued and to submit written comments.

U.S. Treasury Department
FINANCIAL CRIMES ENFORCEMENT NETWORK

Home
About
Contract Opportunities

Resources
Careers
Get News Updates

Contact
Newsroom

USA.gov | Regulations.gov | Treasury.gov | IRS.gov | Freedom of Information Act (FOIA) | NO FEAR Act | Vote.gov | Accessibility | EEO & Diversity Policy | Privacy

48

ANPRM – Beneficial Ownership Reporting Requirements

- On 04/05/21, FinCEN published an ANPRM to solicit public comment on questions pertinent to the implementation of the Corporate Transparency Act. The ANPRM seeks initial public input on procedures and standards for reporting companies to submit information to FinCEN about their beneficial owners;
- 48 explicit questions with various subsets covering a variety of topics, mostly of interest to commercial clients of DFIs;
- Questions from Section 35 & 36 do have implications for DFIs;
- Comment period closes 05/05/21
- 86 FR 17557 - 17565

49

49

Requirement for Smaller Businesses to Disclose Beneficial Ownership Information to FinCEN

- “Reporting Company” definition targets smaller businesses and shell companies by exempting a wide range of entities, including many types of financial institutions and larger U.S. companies (companies that employ more than 20 full-time employees in the United States, had more than \$5 million in gross revenue in the past year, and are operating at a physical office in the United States).
- Establishes requirement for “reporting compan[ies]” to disclose beneficial ownership information to FinCEN, which will be maintained in a nonpublic beneficial ownership database.
- Allows FinCEN to disclose beneficial ownership information to a financial institution with the reporting company’s consent to facilitate the financial institution’s compliance with Customer Due Diligence requirements.
- Major Question – what, if anything happens to our CDD / Beneficial Ownership Regulation and corresponding responsibilities – 3 alternatives: Eliminate; Modify; or No Change to our requirements.

50

50



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

Anti-Money Laundering and Countering the Financing of Terrorism National Priorities

June 30, 2021

The Financial Crimes Enforcement Network (FinCEN),¹ after consulting with the U.S. Department of the Treasury's (Treasury's) Offices of Terrorist Financing and Financial Crimes, Foreign Assets Control (OFAC), and Intelligence and Analysis, as well as the Attorney General, Federal functional regulators,² relevant state financial regulators, and relevant law enforcement and national security agencies, is issuing these first government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) policy (the "Priorities"). These Priorities are being issued pursuant to Section 5318(h)(4)(A) of the Bank Secrecy Act (BSA),³ as amended by Section 6101(b)(2)(C) of the Anti-Money Laundering Act of 2020 (the "AML Act").⁴ As required by Section 5318(h)(4)(C) of the BSA, the Priorities are consistent with Treasury's 2018 and 2020 National Strategy for Combating Terrorist and Other Illicit Financing (the "National Strategy").⁵

As explained in more detail below, the Priorities are, in no particular order: (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing. The establishment of these Priorities is intended to assist all covered institutions⁶ in their efforts to meet their obligations under laws and regulations designed to combat money laundering and counter terrorist financing.

51

FinCEN will issue regulations at a later date that will specify how financial institutions should incorporate these Priorities into their risk-based AML programs.⁷ FinCEN recognizes that not every Priority will be relevant to every covered institution, but each covered institution should, upon the effective date of future regulations to be promulgated in connection with these Priorities, review and incorporate, as appropriate, each Priority based on the institution's broader risk-based AML program. FinCEN, in coordination with relevant federal and state regulators, has also issued [two statements](#) to provide additional guidance to all covered institutions on the applicability of these Priorities at this time, before regulations are promulgated.

I. Methodology

To develop the Priorities, which focus on threats to the U.S. financial system and national security, FinCEN consulted with a number of stakeholders including those with which it was required to consult pursuant to the AML Act. FinCEN also considered a variety of sources of information, including the 2018 and 2020 National Strategies and related risk assessments, prior FinCEN advisories and guidance documents, economic and trade sanctions actions, notices issued by FinCEN and other Treasury components, and previous feedback from law enforcement and covered institutions through the BSA Advisory Group.⁸ References to these sources throughout the Priorities are solely intended to provide background information, and FinCEN is not incorporating by reference these additional sources into the Priorities.

Consistent with Treasury's 2018 National Money Laundering Risk Assessment, which informs the National Strategy, "threats" for purposes of these Priorities are predicate crimes associated with money laundering.⁹ These threats exploit some perceived "vulnerability" in the U.S. financial system that may be in law, regulation, supervision, or enforcement, or may stem from a unique attribute of a product, service, or jurisdiction.¹⁰

In consultation with the agencies and offices listed above, FinCEN will update the Priorities at least once every four years, as required by the AML Act,¹¹ to account for new and emerging threats to the U.S. financial system and national security.

52

FinCEN Announces \$390,000,000 Enforcement Action Against Capital One, National Association for Violations of the Bank Secrecy Act

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

Immediate Release: January 15, 2021

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today announced that Capital One, National Association (Capital One) has been assessed a \$390,000,000 [civil money penalty](#) for engaging in both willful and negligent violations of the Bank Secrecy Act (BSA) and its implementing regulations.

Specifically, FinCEN determined and Capital One admitted to willfully failing to implement and maintain an effective Anti-Money Laundering (AML) program to guard against money laundering. Capital One also admitted that it willfully failed to file thousands of suspicious activity reports (SARs), and negligently failed to file thousands of Currency Transaction Reports (CTRs), with respect to a particular business unit known as the Check Cashing Group. The violations occurred from at least 2008 through 2014, and caused millions of dollars in suspicious transactions to go unreported in a timely and accurate manner, including proceeds connected to organized crime, tax evasion, fraud, and other financial crimes laundered through the bank into the U.S. financial system. As stated in the Assessment of Civil Money Penalty, Capital One admitted to the facts set forth by FinCEN and acknowledged that its conduct violated the BSA and regulations codified at 31 C.F.R. Chapter X.

"The failures outlined in this enforcement action are egregious," said FinCEN's Director Kenneth A. Blanco. "Capital One willfully disregarded its obligations under the law in a high-risk business unit. Information received from financial institutions through the Bank Secrecy Act plays a critical role in protecting our national security, and depriving law enforcement of this information puts our nation and our people at risk. Capital One's failures did just that. Capital One's egregious failures allowed known criminals to use and abuse our nation's financial system unchecked, fostering criminal activity and allowing it to continue and flourish at the expense of victims and other citizens. These kinds of failures by financial institutions, regardless of their size and believed influence, will not be tolerated. Today's action should serve as a reminder to other financial institutions that FinCEN is committed to protecting our national security and the American people from harm and we will bring appropriate enforcement actions where we identify violations."

As outlined in the Assessment, in 2008, after Capital One acquired several other regional banks, Capital One established the Check Cashing Group as a business unit within its commercial bank. The group was comprised of between approximately 90 and 150 check cashers in the New York- and New Jersey-area. Capital One provided banking services to the Check Cashing Group, including providing armored car cash shipments and processing checks deposited by Check Cashing Group customers. During the course of establishing the Check Cashing Group and banking these customers, Capital One was aware of several compliance and money laundering risks associated with banking this particular group, including warnings by regulators, criminal charges against some of the customers, and internal assessments that ranked most of the customers in the top 100 of the bank's highest risk customers for money laundering.

53

Despite the warnings and internal assessments, Capital One willfully failed to implement and maintain an effective AML program in many ways. Capital One's process for investigating suspicious transactions was weak and resulted in the failure to fully investigate and report suspicious activity to FinCEN. Capital One often failed to detect and report suspicious activity by the check cashers themselves, even as it detected and reported activity by the check cashers' customers. And Capital One's implementation of a specialized report to provide insight into larger checks cashed by the Check Cashing Group customers' customers (the check cashers' patrons) failed to properly connect and report suspicious banking activity by certain check cashers.

Capital One also acknowledged failing to file SARs even when it had actual knowledge of criminal charges against specific customers, including Domenick Pucillo, a convicted associate of the Genovese organized crime family. Pucillo was one of the largest check cashers in the New York-New Jersey area, and one of the highest-risk Check Cashing Group customers. Capital One was made aware of Pucillo's participation in potential criminal activity and other risks on several occasions, including learning in early 2013 about potential criminal charges in two different jurisdictions. Despite this information, Capital One failed to timely file SARs on suspicious activity by Pucillo's check cashing businesses, and continued to process over 20,000 transactions valued at approximately \$160 million, including cash withdrawals, for Pucillo's businesses. According to public sources, in May 2019 Pucillo pleaded guilty to conspiring to commit money laundering in connection with loan sharking and illegal gambling proceeds that flowed through his Capital One accounts.

Capital One also admitted to negligently failing to file CTRs on approximately 50,000 reportable cash transactions representing over \$16 billion in cash handled by its Check Cashing Group customers. Specifically, Capital One utilized an internal system that assigned a "cash" code for customer withdrawals to trigger CTR filings. In designing its system, Capital One failed to assign this "cash" code to armored car cash shipments for a number of Check Cashing Group customers. Accordingly, these transactions were not identified as customer cash withdrawals and were not reported to FinCEN through Capital One's CTR reporting systems.

In determining the final amount of the civil money penalty, FinCEN considered Capital One's significant remediation and cooperation with FinCEN's investigation. In addition to exiting the Check Cashing Group and taking specific remedial efforts related to its SAR and CTR filing systems, Capital One has made significant investments in and improvements to its AML program over the past several years. The bank also provided FinCEN with voluminous and well-organized documents, made several presentations of its findings, and signed several agreements tolling the statute of limitations during this investigation. FinCEN strongly encourages financial institutions and other businesses and individuals subject to the BSA to self-disclose any violations of FinCEN's regulations and cooperate with its enforcement investigations.

54

FINANCIAL CRIMES

ENFORCEMENT NETWORK

HOME

ABOUT

RESOURCES

NEWSROOM

CAREERS

ADVISORIES

GLOSSARY

Search

FinCEN Announces \$8 Million Civil Money Penalty against CommunityBank of Texas, National Association for Violations of the Bank Secrecy Act

Contact: Office of Strategic Communications, press@fincen.gov
 Immediate Release: December 16, 2021

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today announced that it has assessed an \$8 million [civil money penalty](#) on CommunityBank of Texas, N.A. (CBOT) for willful violations of the Bank Secrecy Act (BSA) and its implementing regulations.

Specifically, CBOT admitted that it willfully failed to implement and maintain an effective anti-money laundering (AML) program that was reasonably designed to guard against money laundering. CBOT also admitted that it willfully failed to report hundreds of suspicious transactions to FinCEN involving illegal financial activity by its customers and processed by, at, or through the bank even after the bank became aware that certain customers were subjects of criminal investigations. The violations occurred from at least 2015 through 2019 and caused millions of dollars in suspicious transactions to go unreported to FinCEN in a timely and accurate manner, including transactions connected to tax evasion, illegal gambling, money laundering, and other financial crimes.

“CommunityBank of Texas willfully disregarded its lawful obligations to implement and maintain an effective AML program and to identify and report suspicious transactions to FinCEN,” said FinCEN’s Acting Director Himamauli Das. “The failures of CommunityBank of Texas enabled criminal activity by depriving regulators and law enforcement of critical financial intelligence. Today’s action should serve as a reminder to banks of all sizes that FinCEN and our regulatory partners will work closely together to ensure that banks comply with the Bank Secrecy Act and its implementing regulations in order to combat money laundering and promote national security.”

As a result of its own investigation, the Office of the Comptroller of the Currency (OCC) assessed a civil penalty of \$1 million for related violations. As many of the facts and circumstances underlying the OCC’s civil penalty also form the basis of FinCEN’s Consent Order, FinCEN agreed to credit the \$1 million civil penalty imposed by the OCC. Taken together, CBOT will pay a total of \$8 million to the U.S. Treasury as a penalty for its violations, with \$7 million representing FinCEN’s penalty and \$1 million representing the OCC’s penalty.

FinCEN notes its appreciation for the close collaboration and invaluable assistance provided by the OCC, the Dallas Field Office of the Internal Revenue Service – Criminal Investigation, Homeland Security Investigations Houston, and the Federal Bureau of Investigation Beaumont Resident Agency.

For additional information regarding the facts and circumstances associated with this enforcement action, including the specific BSA violations and their underlying causes, please see the Consent Order between FinCEN and CBOT [here](#).

55

FINANCIAL CRIMES

ENFORCEMENT NETWORK

HOME

ABOUT

RESOURCES

NEWSROOM

CAREERS

ADVISORIES

GLOSSARY

Search

FinCEN Announces \$100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act

Contact: Office of Strategic Communications, 703-905-3770
 Immediate Release: August 10, 2021

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) has assessed a [civil money penalty](#) in the amount of \$100 million against BitMEX, one of the oldest and largest convertible virtual currency derivatives exchanges, for violations of the Bank Secrecy Act (BSA) and FinCEN’s implementing regulations.

BitMEX, which operated as an unregistered futures commission merchant (FCM) and provided money transmission services, willfully failed to comply with its obligations under the BSA. FinCEN’s action is part of a global settlement with the U.S. Commodity Futures Trading Commission (CFTC).

“BitMEX’s rapid growth into one of the largest futures commission merchants offering convertible virtual currency derivatives without a commensurate anti-money laundering program put the U.S. financial system at meaningful risk,” FinCEN’s Deputy Director AnnaLou Tirol said. “It is critical that platforms build in financial integrity from the start, so that financial innovation and opportunity are protected from vulnerabilities and exploitation.”

For over 6 years, BitMEX failed to implement and maintain a compliant anti-money laundering program and a customer identification program, and it failed to report certain suspicious activity. These willful failures expose financial institutions to an increased risk of conducting transactions with money launderers and terrorist financiers, including noncompliant exchanges in high-risk jurisdictions, ransomware attackers, and darknet marketplaces. BitMEX conducted at least \$209 million worth of transactions with known darknet markets or unregistered money services businesses providing mixing services. BitMEX also conducted transactions involving high-risk jurisdictions and alleged fraud schemes. BitMEX failed to file a Suspicious Activity Report (SAR) on at least 588 specific suspicious transactions.

From approximately 2014 through 2020, BitMEX allowed customers to access its platform and conduct derivative trading without appropriate customer due diligence – collecting only an email address and failing to verify customer identity. Despite BitMEX’s public representation that its platform was not conducting business with U.S. persons, FinCEN found that BitMEX failed to implement appropriate policies, procedures, and internal controls to screen for customers that use a virtual private network to access the trading platform and circumvent internet protocol monitoring. In some instances, BitMEX senior leadership altered U.S. customer information to hide the customer’s true location.

In addition to paying a civil money penalty, BitMEX has agreed to engage an independent consultant to conduct a historical analysis of its transaction data, sometimes referred to as a “SAR lookback,” to determine whether BitMEX must file additional SARs on this activity. BitMEX will also engage an independent consultant to conduct two reviews, including relevant testing, to ensure that appropriate policies, procedures, and controls are in place that are effective and reasonably designed and implemented to ensure that BitMEX is not operating wholly or in substantial part in the United States.

This is FinCEN’s first enforcement action against an FCM. FinCEN appreciates the close collaboration with its partners at the CFTC on this matter. The CFTC and BitMEX have separately agreed to a Consent Order requiring the payment of a civil money penalty with additional equitable relief. FinCEN’s \$100 million assessment will be satisfied by immediate payments totaling \$80 million to FinCEN and the CFTC, with \$20 million suspended pending the successful completion of the SAR lookback and independent consultant reviews.

56

FINANCIAL CRIMES



ENFORCEMENT NETWORK

HOME

ABOUT

RESOURCES

NEWSROOM

CAREERS

ADVISORIES

GLOSSARY

FinCEN Announces New Acting Director

Immediate Release: August 03, 2021

WASHINGTON—Financial Crimes Enforcement Network (FinCEN) Acting Director Michael Mosier today announced he will depart FinCEN at the end of the week for a new opportunity, after serving as the organization's acting director. Himamauli "Him" Das, a national security expert with experience at the White House, National Security Council, National Economic Council, and Departments of State and the Treasury, will assume the role of acting director of FinCEN. Today, Treasury launched a public search for a permanent FinCEN director.

"It is an honor to be returning to the Department of the Treasury as acting director of FinCEN to continue the important work the bureau is doing to combat money laundering and disrupt illicit financing, especially as technologies become more sophisticated and as threats are on the rise," said Him Das. "I'm eager to lead this organization as it carries out critical work to safeguard the financial security of the United States and continues to make the implementation of the sweeping Anti-Money Laundering Act of 2020 a top priority."

"We are grateful to Michael for his service and incredibly lucky to have Him come back to Treasury to lead the crucial work of FinCEN. There has never been a more important time to bring the full force of this team of dedicated professionals to the work of disrupting illicit finance including the funding of terrorism," said Deputy Secretary Wally Adeyemo. "Their tireless work will make the American people safer."

"Serving as acting director of FinCEN has been an absolute honor, and I am forever grateful to the committed professionals of the bureau who work tirelessly every day to help advance the integrity and innovative strength of the financial system," said Michael Mosier. "I'm confident that with Him's and Deputy Director AnnaLou Tirol's outstanding leadership, FinCEN will continue its important work of protecting the safety, self-determination, and financial opportunity of the American people."

Das was most recently senior managing director and co-head of CFIUS advisory series at K2 Integrity. Das has vast experience at the U.S. Department of the Treasury where he received the Distinguished Service Award, and spent much of his career combatting illicit financing. Das formerly served as counselor to the Department's General Counsel, Assistant General Counsel for International Affairs, and acting Deputy Assistant Secretary for Trade and Investment at the Treasury Department. Das served as Senior Director for International Trade and Investment at the National Security Council where he oversaw efforts to impose targeted financial sanctions across a range of malign actors. He also served as Deputy Legal Advisor at the National Security Council and attorney at the State Department and was integral to the drafting of the domestic and international framework to combat terrorist financing and the development of the USA PATRIOT Act.

Das has contributed to efforts to develop and deploy innovative technologies to help banks and financial services firms monitor transactions and customers to prevent and identify illicit finance. He has also advised on cryptocurrency policy and enforcement developments.

Das received a J.D. and M.P.P. from the University of California at Berkeley; an M.Sc. from the University of Colorado at Boulder in astrophysics, planetary and atmospheric sciences; and a B.S. in physics from the University of California at Berkeley.

57

Summary

Since the start of the COVID-19 pandemic, the Federal Reserve's national Cash Product Office (CPO), Federal Reserve Bank of Atlanta, and Federal Reserve Bank of Boston have collaborated to conduct three supplemental COVID-19 surveys. These surveys were fielded to better understand how the pandemic disrupted consumer payments and shopping behavior. The three surveys were fielded in April 2020, August 2020, and April 2021 as part of the University of Southern California's COVID-19 longitudinal survey.¹ The third supplemental survey took place between April 15th and May 25th and focused on consumer cash holdings, shopping behavior, and coin use. This paper reports findings from the most recent supplemental COVID-19 survey, which finds that the patterns of consumer behavior established in late summer 2020 in response to the COVID-19 pandemic continue to hold true, despite the facts that COVID-19 cases have decreased and that businesses have reopened for indoor and outdoor services in the United States.

The high-level findings from this survey are:

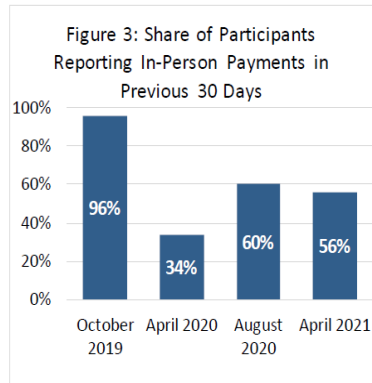
- Consumers continue to hold more store of value cash compared to pre-pandemic amounts.
- Consistent with the findings in the April and August 2020 supplemental surveys, fewer consumers are making in-person payments compared to pre-pandemic levels.
- The share of individuals making in-person payments and using cash in April 2021 declined slightly compared to August 2020.
- Consumers continue to state that they are not affected by coin allocations implemented by the Federal Reserve, and the share of individuals redeeming, or depositing coin remains low.

Overall, the data shows that consumer cash holdings behavior and payment choice continue to deviate from pre-pandemic trends. The average value of store of value cash continued to increase with April 2021 holdings at \$325, an increase of approximately \$80 compared to pre-pandemic values reported in October 2019.^{2,3} While average store of value holdings increased, the average value of money consumers held in their pocket, purse, or wallet remained consistent compared to pre-pandemic levels at around \$70.

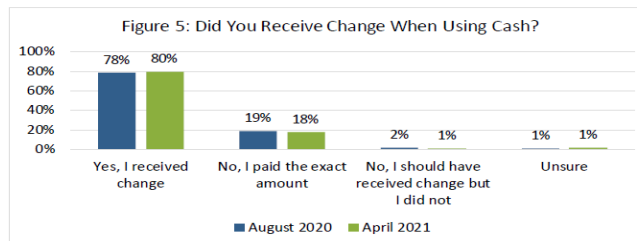
58

2. As of April 2021, 6 in 10 Consumers Shop In-Person

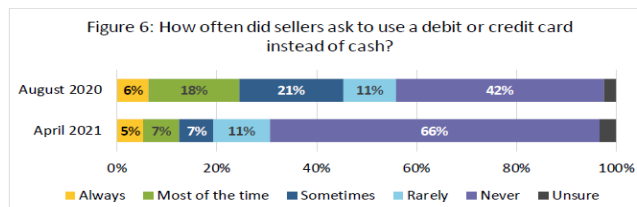
Throughout the pandemic, the share of individuals making in-person payments has remained well below pre-pandemic levels. In April 2020, only one-third of individuals reported making an in-person payment since early March 2020. However, in-person payments rebounded in August 2020 when the second supplemental survey found the share of consumers making at least one in-person payment in the last 30 days jumped from 34 percent to 60 percent; a similar share was reported in April 2021. These results suggest that the shopping habits developed during the pandemic have been slow to change and continue to deviate from pre-pandemic trends, at least until this point.



59



Another reason that people could be making cash payments more frequently is the reduction in merchant steering observed since last summer (Figure 6). Survey respondents were asked how often merchants asked them to use debit or credit cards instead of cash at the in-person point of sale. In August 2020, 45 percent of consumers reported that merchants asked for debit or credit cards at least some of the time,¹³ and this share declined to 19 percent in April 2021. Also, in April, about two-thirds of consumers reported that merchants never asked them to use cards, up 24 percentage points from August.



Therefore, when consumers do make payments in cash and receive change, that change often ends up in one's car or residence in jars or piggy banks. However, given the limited impact on consumers, there remains little incentive for individuals to use, deposit, or redeem their coins

60

60

Conclusion

The third supplemental survey conducted in April 2021 continues to show that consumer shopping behavior has changed throughout the pandemic. As consumers' store of value cash holdings increased to \$326, an \$80 increase compared to October 2019, so too did the value of currency and coin in circulation which reached \$2.18 trillion by the end of May 2021. While the demand for cash remained elevated at the time of writing this paper, the share of people making in-person payments remains depressed and even declined slightly from the 73 percent reported in August to at 56 percent in April. Despite fewer people reporting an in-person payment over the last 30 days, the demand for coin continues to outpace supply. Yet the supply issues for coins are not affecting consumers in a significant way as only four percent report depositing or redeeming coin which may continue to limit circulation as consumers have little incentive to put their coin back into circulation.

In general, the data from the third supplemental survey shows that cash holdings, consumer payments, and shopping behavior have not returned to pre-pandemic levels. As the risk from the pandemic continues, it is difficult to determine whether consumer payment behavior will revert

to trends akin to pre-pandemic levels. For example, consumers might maintain an elevated level of cash holdings and continue making an increased share of payments online. Or, perhaps, individuals may prefer to shop in-person and spend down their cash holdings rather than shopping online. Regardless of how the pandemic will continue to affect consumer payment behavior, the 2021 Diary of Consumer Payment Choice will be helpful in providing early insight into how payments will continue to evolve.

61



ProBank
Austin

Part 1 – Line 2

- On each Part 1 Page completed, only one block in Line 2 can be checked – What if more than one could apply to the reportable situation:
 - If 2d applies, even with multiple options – select 2d;
 - If 2a, 2b, and 2c apply – select 2a;
 - If 2a and 2b apply – select 2a;
 - If 2a and 2c apply – select 2a;
 - If 2b and 2c apply – select 2b.

Part I Person Involved in Transaction(s) 1 of 1			
*2	<input type="checkbox"/> a Person conducting transaction on own behalf	<input type="checkbox"/> b Person conducting transaction for another	<input type="checkbox"/> c Person on whose behalf transaction was conducted
3	<input type="checkbox"/> d Common carrier		
	<input type="checkbox"/> Multiple transactions		

62

The mandatory effective date for complying with the update below is extended from February 1, 2020 to September 1, 2020.

The revised instructions for completing Item 2 of the CTR are as follows:

***2. Person involved in transaction(s)**

- a. Person conducting transaction on own behalf
- b. Person conducting transaction for another
- c. Person on whose behalf transaction is conducted
- d. Common Carrier

Item 2: Select option 2a if the person recorded in Part I conducted the transaction(s) on his or her own behalf. Select option 2b if the person recorded in Part I conducted the transaction(s) on behalf of another person. Options 2a and 2b cannot be selected if box 4b, "If entity" is checked. Select option 2c if the transaction was conducted by another for the person recorded in Part I. If option 2d is selected

because an armored car service under contract with the customer is involved in the transaction(s), the information on the armored car service, not the individual agent of that armored car service, will be recorded in Part I (see FIN-2013-R001). If box 2d is checked to indicate an armored car service under contract with the customer then box 4b, "If entity" must be checked. If more than one Item 2 option applies to a Part I person, a separate Part I section will be prepared on that person for each Item 2 option. For example, if the Part I person makes 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 I on that person reporting option 2a on the personal deposit with that amount and account number in Item 21 "Cash in amount". There will be a second Part I on that person reporting option 2b on the person/entity account transaction with that amount and account number in Item 21.

If you have any questions or concerns regarding this notice, you may contact the BSA E-Filing Help Desk for assistance by opening a support request ticket [here](#). The Help Desk is available Monday through Friday from 8 a.m. to 6 p.m. EST. Please note that the Help Desk is closed on Federal holidays.

01/17/2020

63



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Enforcement Release: December 23, 2021

OFAC Settles with TD Bank, N.A. for \$115,005.04 Related to Apparent Violations of the North Korea Sanctions Regulations and the Foreign Narcotics Kingpin Sanctions Regulations

TD Bank, N.A. ("TDBNA"), a bank incorporated in Wilmington, Delaware, has agreed to remit \$115,005.04 to settle its potential civil liability for two separate matters involving apparent violations of the North Korea Sanctions Regulations and the Foreign Narcotics Kingpin Sanctions Regulations. In the first matter, TDBNA processed 1,479 transactions totaling \$382,685.38 and maintained nine accounts on behalf of employees of the North Korean mission to the United Nations without a license from OFAC. In the second matter, TDBNA maintained two accounts for more than four years for a U.S. resident who was listed on OFAC's list of Specially Designated Nationals and Blocked Persons ("SDN List"). The apparent violations in both cases resulted from multiple sanctions compliance breakdowns, including screening deficiencies and human error, and highlight the importance of maintaining and following proper escalation procedures and ensuring adequate employee training. The settlements reflect OFAC's determination that TDBNA's apparent violations in both matters were voluntarily self-disclosed and were non-egregious.

Matter 1: North Korea-related Apparent Violations

Description of the Apparent Violations of the North Korea Sanctions Regulations

Between December 20, 2016 and August 15, 2018, TDBNA processed 1,479 transactions totaling \$382,685.38, and maintained nine accounts on behalf of five employees of the North Korean mission to the United Nations without a license from OFAC. At account opening, the account holders of all nine accounts presented to TDBNA North Korean passports. However, these passports did not generate an alert during the customer screening process because TDBNA relied heavily on a vendor-supplied Politically Exposed Persons (PEP) list ("PEP list"), which did not include government employees of sanctioned countries. In addition, TDBNA employees often misidentified North Korea (referring to it as Korea or South Korea or using a country code meant for South Korea), or left the citizenship field blank in the customer profiles. As a result, TDBNA's screening system did not flag any of these accounts because the citizenship information was missing or incorrect.

Under the North Korea Sanctions Regulations (NKS), 31 C.F.R. § 510.510(c), a general license authorizing certain transactions with the North Korean Mission to the United Nations specifies that it does not authorize U.S. financial institutions to open and operate accounts for employees of the North Korean mission. It further specifies that U.S. financial institutions are required to obtain OFAC specific licenses to operate accounts for such persons. Because TDBNA did not have a specific license to provide these services, its conduct resulted in the apparent violations of 31 C.F.R. § 510.201.

64

64



65

CONTENTS	
Introduction	1
What Is OFAC?	2
What Are OFAC Sanctions?	3
The SDN List	4
How Do You Block Virtual Currency?	5
Case Study: OFAC Sanctions Involving Virtual Currency	5
Who Must Comply with OFAC Sanctions?	6
Strict Liability Regulations	6
OFAC Requirements and Procedures	7
Reporting Requirements	7
Recordkeeping Requirements	8
License Procedures	8
Consequences of Noncompliance	9
Enforcement Procedures	9
Enforcement Guidelines	9
Enforcement Actions	9
Voluntary Self-Disclosure	9
Sanctions Compliance Best Practices for the Virtual Currency Industry	10
Management Commitment	11
Risk Assessment	12
Case Study: Diagnosing Risky Relationships	12
Internal Controls	13
Case Study: Double-Duty Data	13
Sanctions Screening	16
Remediating the Root Causes of Violations	17
Risk Indicators	17
Testing and Auditing	18
Training	19
OFAC Resources	20
FAQs on Virtual Currency Topics	20
Contact Information	21
Resource Sites	22

66

ORDER

Order granting an exemption from customer identification program requirements implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l), for loans extended by banks (and their subsidiaries) subject to the jurisdiction of the Federal Banking Agencies to all customers to facilitate purchases of property and casualty insurance policies.

Issue Date: October 5, 2020

By ORDER, under the authority set forth in 31 C.F.R. § 1020.220(b) implementing section 326(a) of the USA PATRIOT Act, 31 U.S.C. § 5318(l)(5), the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA), collectively the Federal Banking Agencies (FBAs), with the concurrence of the Financial Crimes Enforcement Network (FinCEN), hereby grant an exemption from the requirements of the customer identification program (CIP) rules implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l),¹ for loans extended by banks² (and their subsidiaries³) subject to the FBAs' jurisdiction to all customers to facilitate purchases of property and casualty insurance policies⁴ (hereinafter referred to as premium finance loans or premium finance lending).

67

Therefore, each FBA, with FinCEN's concurrence, hereby grants by ORDER an exemption from the requirements of the CIP rules implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l), for loans extended by banks (and their subsidiaries) subject to that FBA's jurisdiction to all customers to facilitate purchases of property and casualty insurance policies by the borrower. This ORDER supersedes the previous Order issued on September 27, 2018.

In arriving at the determinations in this ORDER, the FBAs have relied on the determinations made by FinCEN and the accuracy and completeness of the representations made in the Request Letters and the Supplemental Letter. Nothing in this ORDER shall bar, estop, or otherwise prevent the FBAs from taking any action affecting a bank, including the revocation of this ORDER, on the basis of information not known to the FBAs as of the effective date of the ORDER.

Banks engaging in premium finance lending must continue to comply with all other regulatory requirements, including the regulations implementing the BSA that require the filing of suspicious activity reports.²¹

68

For Verification of Attendance for CRCM, <https://probank.cnf.io>



- ▶ Navigate to <https://probank.cnf.io> and tap the session titled "VIRGINIA BANKERS ASSOCIATION - BSA SCHOOL - DAY 2"
- ▶ OR just point your phone's camera at the QR code to join directly

69

Wednesday, February 16
NEW YORK DEPOSIT DOCUMENTATION 9:00am - 4:00pm ▶ Mark Burnside
REAL ESTATE LENDING COMPLIANCE - DAY 1 9:00am - 4:00pm ▶ Andrea Cohen
VIRGINIA BANKERS ASSOCIATION - BSA SCHOOL - DAY 1 9:00am - 4:00pm ▶ Mark W. Cover
COMPLIANCE OFFICER BOOT CAMP - DAY 2 10:00am - 5:00pm ▶ Leah Hamilton
DEPOSIT ACCOUNTS FOR MINORS 2:00pm - 3:30pm ▶ K. Natalie Straus
Thursday, February 17
VIRGINIA BANKERS ASSOCIATION - BSA SCHOOL - DAY 2 9:00am - 4:00pm ▶ Mark W. Cover
ADVANCED TRIO 10:00am - 5:00pm ▶ Mark Burnside
COMPLIANCE OFFICER BOOT CAMP - DAY 1 10:00am - 5:00pm ▶ Leah Hamilton
HELOCs: START TO FINISH 10:00am - 1:00pm ▶ Andrea Cohen

70

ProBank Austin

WFOU-ADMINISTRATOR ASSOCIATION - WEB SCHOOL - QAF 1

Check in To This Session

First Name
Blank

Last Name
Denver

Email Address
mblavin@probank.com

Do You Have CPE Credit?
☐ Yes
☒ No

How Are You Registering?
☐ In Person
☒ Virtual

[Check In Now](#)

[Sign In To My Account](#)

71

ProBank Austin

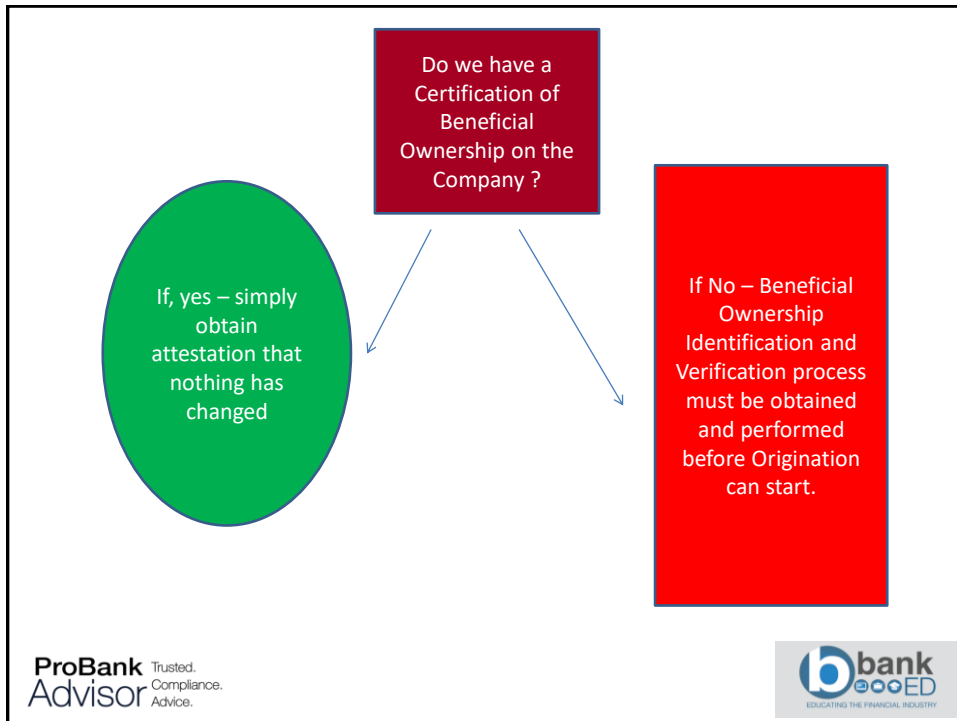
WFOU-ADMINISTRATOR ASSOCIATION - WEB SCHOOL - QAF 1

Check Out [Sign Out](#) | [Check In](#)

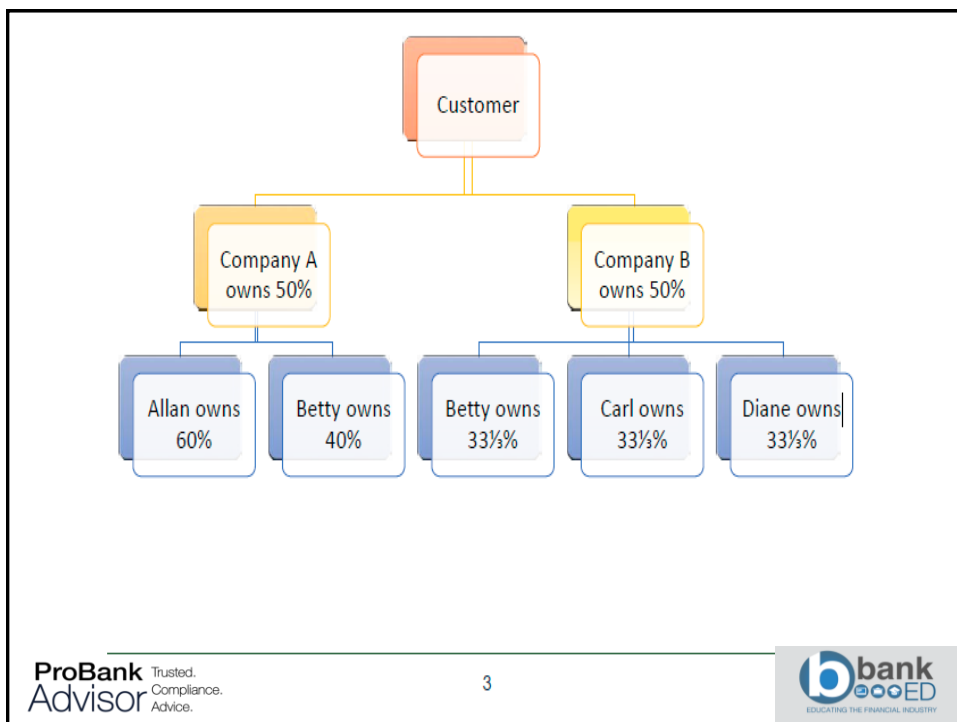
Session ID: [View Session ID](#)

[Sign In To My Account](#)

72



73



74



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](#).

75

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)?

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.

76

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.

77

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.

78

II. ADDITIONAL RECORDKEEPING AND REPORTING REQUIREMENTS

A. Business and Transactions Covered by This Order

1. For purposes of this Order, the “Covered Business” means TITLE INSURANCE COMPANY and any of its subsidiaries and agents.
2. For purposes of this Order, a “Covered Transaction” means a transaction in which:
 - i. Residential real property is purchased by a Legal Entity (as this term is defined in Section III.A of this Order);
 - ii. The purchase price of the residential real property is in the amount of \$300,000 or more in any of the following areas:
 1. The Texas counties of Bexar, Tarrant, or Dallas;
 2. The Florida counties of Miami-Dade, Broward, or Palm Beach;

79

3. The Boroughs of Brooklyn, Queens, Bronx, Staten Island, or Manhattan in New York City, New York;
4. The California counties of San Diego, Los Angeles, San Francisco, San Mateo, or Santa Clara;
5. The City and County of Honolulu in Hawaii;
6. The Nevada county of Clark;
7. The Washington county of King;
8. The Massachusetts counties of Suffolk, or Middlesex; or
9. The Illinois county of Cook;
- iii. Such purchase is made without a bank loan or other similar form of external financing; and
- iv. Such purchase is made, at least in part, using currency or a cashier’s check, a certified check, a traveler’s check, a personal check, a business check, a money order in any form, a funds transfer, or virtual currency.

80

2021 SAR Activity Distribution – 3/4ths (1/1 – 9/30)
1,036,455 // 2,253,718 (+ 15.76 % // + 28.82 %)

1	Transaction(s) Below CTR Threshold	308,734	9.83%
2	Suspicion Concerning the Source of Funds	294,039	9.36%
3	Transaction with No Apparent Economic, Business, or Lawful Purpose	269,045	8.57%
4	Transaction Out of Pattern for Customer(s)	232,634	7.41%
5	Suspicious EFT/Wire Transfers	223,105	7.10%
6	Other Fraud (Type)	174,527	5.56%
7	Suspicious use of multiple transaction locations	167,789	5.34%
8	Check	165,480	5.27%
9	ACH	133,864	4.26%
10	Credit/Debit Card	100,362	3.20%
11	Identity Theft	92,230	2.94%
12	Two or More Individuals Working Together	83,262	2.65%

81

2021 SAR Activity Distribution – 3/4ths (1/1 – 9/30)
1,036,455 // 2,253,718 (+ 15.76 % // + 28.82 %)

13	Suspicious Receipt of Government Payments/Benefits	82,652	2.63%
14	Suspicious Use of Multiple Accounts	81,218	2.59%
15	Other is Suspicious Activities	78,017	2.48%
16	Counterfeit Instrument	63,598	2.03%
17	Suspicious Use of Noncash Monetary Instruments	50,608	1.61%
18	Other Money Laundering	49,093	1.56%
19	Provided Questionable or False Documentation	48,819	1.55%
20	Wire	43,630	1.39%
21	Transaction(s) Involving Foreign High Risk Jurisdiction	41,241	1.31%
22	Consumer Loan (see instructions)	36,364	1.16%
23	Elder Financial Exploitation	31,573	1.01%
24	Account Takeover	31,480	1.00%

82

2021 SAR Activity Distribution – 3/4ths (1/1 – 9/30)
1,036,455 // 2,253,718 (+ 15.76 % // + 28.82 %)

25	Business Loan	28,510	0.91%
	Alters or Cancels Transaction to Avoid CTR		
26	Requirement	24,193	0.77%
27	Forgeries	23,492	0.75%
	Transaction(s) Below BSA Recordkeeping		
28	Threshold	19,957	0.64%
29	Funnel Account	19,618	0.62%
30	Mass-Marketing	15,640	0.50%
	Refused or Avoided Request for		
31	Documentation	12,834	0.41%
32	Against Financial Institution Customer(s)	12,394	0.39%
33	Provided Questionable or False Identification	9,649	0.31%
	Suspicious Inquiry by Customer Regarding Bsa		
34	Reporting or Recordkeeping Requirements	8,728	0.28%
	Exchanges Small Bills for Large Bills or Vice		
35	Versa	5,953	0.19%
	Little or No Concern for Product Performance		
36	Penalties, Fees, or Tax Consequences	5,609	0.18%

83

2021 SAR Activity Distribution – 3/4ths (1/1 – 9/30)
1,036,455 // 2,253,718 (+ 15.76 % // + 28.82 %)

43	Against Financial Institution(s)	3,758	0.12%
46	Other Cyber Event	2,700	0.09%
56	Human Trafficking	1,532	0.05%
60	Healthcare/Public or Private Health Insurance	666	0.02%
68	Ponzi Scheme	230	0.01%
69	Suspected Public/Private Corruption (Domestic)	218	0.01%
70	Human Smuggling	190	0.01%
71	Insider Trading	177	0.01%
72	Known or Suspected Terrorist/Terrorist Organization	142	0.00%
73	Other Terrorist	112	0.00%
74	Pyramid Scheme	103	0.00%

84

2021 SAR Distribution – 3/4ths

1	California	186,264
2	Ohio	105,062
3	New York	101,251
4	Texas	95,942
5	North Carolina	88,251
6	Virginia	75,086
7	Florida	71,196
8	Delaware	52,821
9	Illinois	38,046
10	Georgia	31,901
11	New Jersey	29,507
12	Pennsylvania	28,821
13	South Dakota	27,250
14	Utah	22,966
15	Alabama	22,417
16	Michigan	22,354
17	Tennessee	18,542
18	Massachusetts	18,449
19	Washington	18,078
20	Arizona	17,527

85

2021 SAR Distribution – 3/4ths

21	Maryland	17,229
22	Indiana	16,977
23	Louisiana	15,197
24	Nevada	14,362
25	Oklahoma	13,687
26	Mississippi	13,618
27	Colorado	13,257
28	Wisconsin	12,248
29	Minnesota	11,507
30	South Carolina	10,389
31	Missouri	10,117
32	Connecticut	9,848
33	Oregon	9,502
34	Puerto Rico	9,015
35	Arkansas	7,918
36	Kentucky	7,700
37	Iowa	6,577
38	Hawaii	5,995
39	West Virginia	5,979
40	Kansas	5,733

86

2021 SAR Distribution – 3/4ths

41	New Mexico	5,022
42	Rhode Island	4,068
43	Maine	4,001
44	Nebraska	3,941
45	District of Columbia	3,229
46	New Hampshire	2,992
47	Idaho	2,542
48	Montana	1,998
49	Alaska	1,847
50	North Dakota	1,542
51	Vermont	1,124
52	Wyoming	864
53	Unknown	745
54	Guam	673
55	Virgin Islands	411
56	APO / DPO / FPO	389
57	Northern Mariana Islands	85
58	Palau	30
59	American Samoa	12
60	Micronesia, Federated States	9

87

2021 SAR Activity Distribution “Top 37” Metropolitan Filing Areas

1	New York-Northern New Jersey-Long Island, NY-NJ-PA Metro Area	81,878
2	Charlotte-Gastonia-Rock Hill, NC-SC Metro Area	74,435
3	Los Angeles-Long Beach-Santa Ana, CA Metro Area	71,506
4	San Francisco-Oakland-Fremont, CA Metro Area	59,154
5	Columbus, OH Metro Area	57,741
6	Washington-Arlington-Alexandria, DC-VA-MD-WV Metro Area	42,695
7	Miami-Fort Lauderdale-Pompano Beach, FL Metro Area	36,757
8	Houston-Sugar Land-Baytown, TX Metro Area	32,174
9	Chicago-Joliet-Naperville, IL-IN-WI Metro Area	30,849
10	Dallas-Fort Worth-Arlington, TX Metro Area	27,220
11	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD Metro Area	26,451
12	Sioux Falls, SD Metro Area	26,049

88

2021 SAR Activity Distribution “Top 37” Metropolitan Filing Areas

13	Richmond, VA Metro Area	24,655
14	Atlanta-Sandy Springs-Marietta, GA Metro Area	23,619
15	Riverside-San Bernardino-Ontario, CA Metro Area	17,801
16	Salt Lake City, UT Metro Area	16,875
17	Cincinnati-Middletown, OH-KY-IN Metro Area	14,466
18	Boston-Cambridge-Quincy, MA-NH Metro Area	13,636
19	Phoenix-Mesa-Glendale, AZ Metro Area	13,398
20	Detroit-Warren-Livonia, MI Metro Area	13,089
21	Cleveland-Elyria-Mentor, OH Metro Area	12,560
22	Las Vegas-Paradise, NV Metro Area	12,374
23	San Diego-Carlsbad-San Marcos, CA Metro Area	11,919
24	Birmingham-Hoover, AL Metro Area	10,913

89

2021 SAR Activity Distribution “Top 37” Metropolitan Filing Areas

25	Seattle-Tacoma-Bellevue, WA Metro Area	9,934
26	Orlando-Kissimmee-Sanford, FL Metro Area	9,557
27	San Jose-Sunnyvale-Santa Clara, CA Metro Area	8,625
28	Tampa-St. Petersburg-Clearwater, FL Metro Area	8,419
29	Sacramento--Arden-Arcade--Roseville, CA Metro Area	8,409
30	Minneapolis-St. Paul-Bloomington, MN-WI Metro Area	8,292
31	Baltimore-Towson, MD Metro Area	7,573
32	Denver-Aurora-Broomfield, CO Metro Area	7,561
33	San Juan-Caguas-Guaynabo, PR Metro Area	6,585
34	San Antonio-New Braunfels, TX Metro Area	5,726
35	Seaford, DE Micro Area	5,648
36	Indianapolis-Carmel, IN Metro Area	5,408
37	New Orleans-Metairie-Kenner, LA Metro Area	5,116

90

Instrument/ Payment Types (DFIs) – 2021

1	U.S. Currency	345,505	39.20%
2	Funds Transfer	241,435	27.39%
3	Personal/Business Check	138,930	15.76%
4	Government Payment	57,934	6.57%
5	Other	46,223	5.24%
6	Bank/Cashier's Check	38,646	4.38%
7	Money Orders	10,734	1.22%
8	Foreign Currency	1,700	0.19%
9	Gaming Instruments	235	0.03%
10	Travelers Checks	62	0.01%

91

Product Types (DFIs) – 2021

1	Deposit Account	465,479	62.06%
2	Debit Card	162,033	21.60%
3	Credit Card	53,732	7.16%
4	Other	46,108	6.15%
5	Prepaid Access	13,478	1.80%
6	Residential Mortgage	4,255	0.57%
7	Home Equity Line of Credit	2,421	0.32%
8	Stocks	687	0.09%
9	Home Equity Loan	373	0.05%
10	Forex Transactions	362	0.05%
11	Commercial Paper	238	0.03%
12	Commercial Mortgage	226	0.03%
13	Mutual Fund	197	0.03%
14	Bonds/Notes	145	0.02%
15	Microcap Securities	128	0.02%
16	Insurance/Annuity Products	77	0.01%
17	Options on Securities	71	0.01%
18	Hedge Fund	42	0.01%
19	Security Futures Products	14	0.00%
20	Futures/Options on Futures	11	0.00%
21	Swap, Hybrid, or Other Derivative	5	0.00%

92

2021 SAR Activity Distribution – VA
75,086 (#06 – 3/4ths) + 1.25 %

1	Credit/Debit Card	24,517	11.65%
2	ACH	22,305	10.60%
3	Suspicion Concerning the Source of Funds	13,718	6.52%
4	Other Fraud (Type)	13,490	6.41%
5	Identity Theft	12,623	6.00%
6	Suspicious Receipt of Government Payments/Benefits	12,053	5.73%
7	Provided Questionable or False Documentation	11,743	5.58%
8	Transaction with No Apparent Economic, Business, or Lawful Purpose	11,373	5.40%
9	Transaction(s) Below CTR Threshold	10,970	5.21%
10	Check	10,307	4.90%
11	Suspicious EFT/Wire Transfers	9,945	4.72%
12	Transaction Out of Pattern for Customer(s)	8,737	4.15%

93

2021 SAR Activity Distribution – VA
75,086 (#06 – 3/4ths) + 1.25 %

13	Business Loan	6,476	3.08%
14	Two or More Individuals Working Together	5,247	2.49%
15	Suspicious use of multiple transaction locations	4,930	2.34%
16	Consumer Loan (see instructions)	4,278	2.03%
17	Counterfeit Instrument	2,954	1.40%
18	Elder Financial Exploitation	2,757	1.31%
19	Other Money Laundering	2,705	1.29%
20	Suspicious Use of Multiple Accounts	2,562	1.22%
21	Other Suspicious Activities	2,542	1.21%
22	Wire	2,482	1.18%
23	Account Takeover	2,036	0.97%
24	Suspicious Use of Noncash Monetary Instruments	1,957	0.93%

94

2021 SAR Activity Distribution – VA
75,086 (#06 – 3/4ths) + 1.25 %

25	Transaction(s) Involving Foreign High-Risk Jurisdiction	1,016	0.48%
26	Alters or Cancels Transaction to Avoid CTR Requirement	818	0.39%
27	Funnel Account	772	0.37%
28	Forgeries	762	0.36%
29	Transaction(s) Below BSA Recordkeeping Threshold	583	0.28%
30	Provided Questionable or False Identification	412	0.20%
31	Against Financial Institution Customer(s)	390	0.19%
32	Suspicious Use of Third-Party Transactors (Straw-Man)	236	0.11%
33	Refused or Avoided Request for Documentation	212	0.10%
34	Embezzlement/Theft/Disappearance of Funds	211	0.10%
35	Suspicious Inquiry by Customer Regarding Bsa Reporting or Recordkeeping Requirements	209	0.10%
36	Mass-Marketing	199	0.09%

95

2021 SAR Activity Distribution – VA
75,086 (#06 – 3/4ths) + 1.25 %

43	Human Smuggling	86	0.04%
49	Other Cyber Event	54	0.03%
53	Against Financial Institution(s)	40	0.02%
56	Human Trafficking	33	0.02%
60	Suspected Public/Private Corruption (Foreign)	29	0.01%
65	Healthcare/Public or Private Health Insurance	9	0.00%
67	Known or Suspected Terrorist/Terrorist Organization	5	0.00%
69	Other Terrorist	5	0.00%
70	Suspected Public/Private Corruption (Domestic)	5	0.00%
71	Ponzi Scheme	4	0.00%
72	Pyramid Scheme	4	0.00%

96

2021 SAR Activity Distribution – VA “Top 15” Metropolitan Filing Areas

1	Washington-Arlington-Alexandria, DC-VA-MD-WV Metro Area	42,695
2	Richmond, VA Metro Area	24,655
3	Virginia Beach-Norfolk-Newport News, VA-NC Metro Area	3,732
4	Roanoke, VA Metro Area	801
5	Lynchburg, VA Metro Area	447
6	Staunton-Waynesboro, VA Micro Area	377
7	Harrisonburg, VA Metro Area	313
8	Martinsville, VA Micro Area	302
9	Charlottesville, VA Metro Area	298
10	Danville, VA Metro Area	276
11	Kingsport-Bristol-Bristol, TN-VA Metro Area	207
12	Winchester, VA-WV Metro Area	192
13	Blacksburg-Christiansburg-Radford, VA Metro Area	181
14	Bluefield, WV-VA Micro Area	126
15	Culpeper, VA Micro Area	83

97

2021 SAR Activity Distribution – OH 105,062 (# 2 – 3/4ths) + 4.53%

1	Identity Theft	31,908	9.64%
2	Other Fraud (Type)	31,166	9.42%
3	ACH	23,318	7.05%
4	Suspicious EFT/Wire Transfers	22,995	6.95%
5	Check	20,138	6.08%
6	Transaction with No Apparent Economic, Business, or Lawful Purpose	17,552	5.30%
7	Suspicion Concerning the Source of Funds	15,331	4.63%
8	Provided Questionable or False Documentation	14,731	4.45%
9	Credit/Debit Card	14,417	4.36%
10	Suspicious Receipt of Government Payments/Benefits	13,636	4.12%
11	Transaction Out of Pattern for Customer(s)	12,978	3.92%
12	Counterfeit Instrument	12,643	3.82%

98

2021 SAR Activity Distribution – OH
105,062 (# 2 – 3/4ths) + 4.53%

13	Consumer Loan (see instructions)	11,724	3.54%
14	Account Takeover	10,307	3.11%
15	Transaction(s) Below CTR Threshold	9,676	2.92%
16	Other Other Suspicious Activities	7,640	2.31%
17	Wire	6,595	1.99%
18	Two or More Individuals Working Together	5,693	1.72%
19	Suspicious use of multiple transaction locations	5,247	1.59%
20	Suspicious Use of Noncash Monetary Instruments	4,973	1.50%
21	Suspicious Use of Multiple Accounts	4,277	1.29%
22	Transaction(s) Involving Foreign High-Risk Jurisdiction	4,214	1.27%
23	Business Loan	3,835	1.16%
24	Forgeries	3,531	1.07%

99

2021 SAR Activity Distribution – OH
105,062 (# 2 – 3/4ths) + 4.53%

25	Elder Financial Exploitation	2,882	0.87%
26	Multiple Individuals with Same or Similar Identities	2,414	0.73%
27	Other Money Laundering	2,257	0.68%
28	Against Financial Institution Customer(s)	2,035	0.61%
29	Against Financial Institution(s)	1,891	0.57%
30	Funnel Account	920	0.28%
31	Single Individual with Multiple Identities	799	0.24%
32	Application Fraud	707	0.21%
33	Transaction(s) Below BSA Recordkeeping Threshold	659	0.20%
34	Mass-Marketing	629	0.19%
35	Alters or Cancels Transaction to Avoid CTR Requirement	584	0.18%
36	Refused or Avoided Request for Documentation	574	0.17%

100

2021 SAR Activity Distribution – OH
105,062 (# 2 – 3/4ths) + 4.53%

43	Other Cyber Event	293	0.09%
46	Human Trafficking	248	0.07%
59	Healthcare/Public or Private Health Insurance	42	0.01%
60	Suspected Public/Private Corruption (Foreign)	41	0.01%
61	Known or Suspected Terrorist/Terrorist Organization	40	0.01%
69	Ponzi Scheme	13	0.00%
70	Suspected Public/Private Corruption (Domestic)	12	0.00%
73	Human Smuggling	10	0.00%
76	Other Terrorist	6	0.00%
80	Pyramid Scheme	3	0.00%

101

2021 SAR Activity Distribution – OH
“Top 45” Metropolitan Filing Areas

1	Columbus, OH Metro Area	57,741
2	Cincinnati-Middletown, OH-KY-IN Metro Area	14,466
3	Cleveland-Elyria-Mentor, OH Metro Area	12,560
4	Dayton, OH Metro Area	1,793
5	Toledo, OH Metro Area	1,645
6	Akron, OH Metro Area	1,538
7	Tiffin, OH Micro Area	1,073
8	Canton-Massillon, OH Metro Area	954
9	Youngstown-Warren-Boardman, OH-PA Metro Area	950
10	Lima, OH Metro Area	463
11	Sandusky, OH Metro Area	339
12	New Philadelphia-Dover, OH Micro Area	217
13	Mansfield, OH Metro Area	199
14	Springfield, OH Metro Area	175
15	East Liverpool-Salem, OH Micro Area	143

102

2021 SAR Activity Distribution – OH “Top 45” Metropolitan Filing Areas

16	Portsmouth, OH Micro Area	127
17	Zanesville, OH Micro Area	127
18	Findlay, OH Micro Area	121
19	Wapakoneta, OH Micro Area	108
20	Ashtabula, OH Micro Area	106
21	Wooster, OH Micro Area	106
22	Marion, OH Micro Area	100
23	Mount Vernon, OH Micro Area	92
24	Wheeling, WV-OH Metro Area	91
25	Norwalk, OH Micro Area	89
26	Van Wert, OH Micro Area	86
27	Fremont, OH Micro Area	82
28	Chillicothe, OH Micro Area	81
29	Steubenville-Weirton, OH-WV Metro Area	79
30	Athens, OH Micro Area	78

103

2021 SAR Activity Distribution – OH “Top 45” Metropolitan Filing Areas

31	Celina, OH Micro Area	77
32	Parkersburg-Marietta-Vienna, WV-OH Metro Area	77
33	Bellefontaine, OH Micro Area	69
34	Greenville, OH Micro Area	61
35	Ashland, OH Micro Area	58
36	Defiance, OH Micro Area	58
37	Sidney, OH Micro Area	55
38	Bucyrus, OH Micro Area	50
39	Wilmington, OH Micro Area	48
40	Cambridge, OH Micro Area	42
41	Huntington-Ashland, WV-KY-OH Metro Area	38
42	Washington Court House, OH Micro Area	34
43	Urbana, OH Micro Area	30
44	Coshocton, OH Micro Area	27
45	Point Pleasant, WV-OH Micro Area	16 ⁴

104

2021 SAR Activity Distribution – WV
5,979 (# 39 – 3/4ths) + %

1	ACH	2,926	24.79%
2	Other Fraud (Type)	1,298	11.00%
3	Transaction(s) Below CTR Threshold	1,097	9.30%
4	Suspicious EFT/Wire Transfers	1,094	9.27%
5	Suspicion Concerning the Source of Funds	698	5.91%
6	Transaction Out of Pattern for Customer(s)	694	5.88%
7	Transaction with No Apparent Economic, Business, or Lawful Purpose	582	4.93%
8	Check	471	3.99%
9	Suspicious Receipt of Government Payments/Benefits	332	2.81%
10	Credit/Debit Card	278	2.36%
11	Suspicious use of multiple transaction locations	273	2.31%
12	Other BSA Suspicious Activities	200	1.69%

105

2021 SAR Activity Distribution – WV
5,979 (# 39 – 3/4ths) + %

13	Two or More Individuals Working Together	173	1.47%
14	Suspicious Use of Multiple Accounts	161	1.36%
15	Counterfeit Instrument	145	1.23%
16	Elder Financial Exploitation	144	1.22%
17	Other Money Laundering	117	0.99%
18	Wire	107	0.91%
19	Suspicious Use of Noncash Monetary Instruments	105	0.89%
20	Transaction(s) Below BSA Recordkeeping Threshold	96	0.81%
21	Account Takeover	92	0.78%
22	Identity Theft	88	0.75%
23	Suspicious Inquiry by Customer Regarding Bsa Reporting or Recordkeeping Requirements	48	0.41%
24	Human Trafficking	45	0.38%

106

2021 SAR Activity Distribution – WV
5,979 (# 39 – 3/4ths) + %

25	Funnel Account	40	0.34%
26	Alters or Cancels Transaction to Avoid CTR Requirement	39	0.33%
27	Against Financial Institution Customer(s)	38	0.32%
28	Forgeries	31	0.26%
29	Against Financial Institution(s)	29	0.25%
30	Transaction(s) Involving Foreign High Risk Jurisdiction	27	0.23%
31	Misuse of Position or Self-Dealing	25	0.21%
32	Business Loan	24	0.20%
33	Exchanges Small Bills for Large Bills or Vice Versa	23	0.19%
34	Provided Questionable or False Documentation	23	0.19%
35	Other Structuring	22	0.19%
36	Suspicious Use of Third-Party Transactors (Straw-Man)	19	0.16%

107

2021 SAR Activity Distribution – WV
5,979 (# 39 – 3/4ths) + %

48	Other Cyber Event	7	0.06%
52	Ponzi Scheme	4	0.03%
55	Human Smuggling	3	0.03%
58	Pyramid Scheme	3	0.03%
61	Healthcare/Public or Private Health Insurance	2	0.02%
68	Known or Suspected Terrorist/Terrorist Organization	1	0.01%

108

2021 SAR Activity Distribution – WV “Top 16” Metropolitan Filing Areas

1	Fairmont, WV Micro Area	3,384
2	Charleston, WV Metro Area	385
3	Wheeling, WV-OH Metro Area	366
4	Huntington-Ashland, WV-KY-OH Metro Area	319
5	Morgantown, WV Metro Area	224
6	Clarksburg, WV Micro Area	193
7	Hagerstown-Martinsburg, MD-WV Metro Area	162
8	Beckley, WV Micro Area	144
9	Parkersburg-Marietta-Vienna, WV-OH Metro Area	112
10	Bluefield, WV-VA Micro Area	90
11	Steubenville-Weirton, OH-WV Metro Area	80
12	Oak Hill, WV Micro Area	60
13	Washington-Arlington-Alexandria, DC-VA-MD-WV Metro Area	41
14	Winchester, VA-WV Metro Area	13
15	Point Pleasant, WV-OH Micro Area	10
16	Cumberland, MD-WV Metro Area	8

109

2021 SAR Activity Distribution – DC 3,229 (# 45 – 3/4ths) – 8.21 %

1	Suspicion Concerning the Source of Funds	1,338	10.53%
2	Transaction(s) Below CTR Threshold	1,084	8.53%
3	Suspicious EFT/Wire Transfers	1,062	8.35%
4	Transaction Out of Pattern for Customer(s)	1,040	8.18%
5	Suspicious use of multiple transaction locations	1,032	8.12%
6	Transaction with No Apparent Economic, Business, or Lawful Purpose	937	7.37%
7	Check	834	6.56%
8	Other Fraud (Type)	552	4.34%
9	Two or More Individuals Working Together	461	3.63%
10	Suspicious Use of Multiple Accounts	440	3.46%
11	Suspicious Use of Noncash Monetary Instruments	387	3.04%
12	Identity Theft	355	2.79%

110

2021 SAR Activity Distribution – DC

3,229 (# 45 – 3/4ths) – 8.21 %

13	Counterfeit Instrument	354	2.78%
14	Suspicious Receipt of Government Payments/Benefits	344	2.71%
15	Other BSA Suspicious Activities	318	2.50%
16	Transaction(s) Below BSA Recordkeeping Threshold	282	2.22%
17	ACH	272	2.14%
18	Credit/Debit Card	190	1.49%
19	Transaction(s) Involving Foreign High-Risk Jurisdiction	170	1.34%
20	Other Money Laundering	165	1.30%
21	Provided Questionable or False Documentation	111	0.87%
22	Forgeries	108	0.85%
23	Wire	94	0.74%
24	Funnel Account	85	0.67%

111

2021 SAR Activity Distribution – DC

3,229 (# 45 – 3/4ths) – 8.21 %

25	Elder Financial Exploitation	73	0.57%
26	Account Takeover	61	0.48%
27	Business Loan	55	0.43%
28	Exchanges Small Bills for Large Bills or Vice Versa	48	0.38%
29	Alters or Cancels Transaction to Avoid CTR Requirement	42	0.33%
30	Against Financial Institution Customer(s)	38	0.30%
31	Mass-Marketing	37	0.29%
32	Suspicious Use of Third-Party Transactors (Straw-Man)	31	0.24%
33	Embezzlement/Theft/Disappearance of Funds	28	0.22%
34	Refused or Avoided Request for Documentation	22	0.17%
35	Multiple Individuals with Same or Similar Identities	21	0.17%
36	Suspicious Use of Informal Value Transfer System	20	0.16%

112

2021 SAR Activity Distribution – DC

3,229 (# 45 – 3/4ths) – 8.21 %

46	Human Trafficking	10	0.08%
49	Suspected Public/Private Corruption (Foreign)	8	0.06%
50	Other Cyber Event	7	0.06%
55	Human Smuggling	2	0.02%
57	Other Terrorist	2	0.02%
58	Against Financial Institution(s)	1	0.01%
60	Healthcare/Public or Private Health Insurance	1	0.01%
61	Known or Suspected Terrorist/Terrorist Organization	1	0.01%
65	Ponzi Scheme	1	0.01%

113



FinCEN NOTICE

FIN-2021-NTC4

November 18, 2021

FinCEN Calls Attention to Environmental Crimes and Related Financial Activity

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to call attention to an upward trend in environmental crimes and associated illicit financial activity. FinCEN is highlighting this trend because of: (1) its strong association with corruption and transnational criminal organizations, two of FinCEN's national anti-money laundering and countering the financing of terrorism (AML/CFI) priorities;¹ (2) a need to enhance reporting and analysis of related illicit financial flows;² and (3) environmental crimes' contribution to the climate crisis, including threatening ecosystems, decreasing biodiversity, and increasing carbon dioxide in the atmosphere.³ This Notice provides financial institutions with specific suspicious activity report (SAR) filing instructions and highlights the likelihood of illicit financial activity related to several types of environmental crimes.

Environmental Crimes

Global environmental crimes are estimated by some international organizations to generate hundreds of billions in illicit proceeds annually and now rank as the third largest illicit activity in the world following the trafficking of drugs and counterfeit goods.⁴ The international police

114

FINCEN NOTICE

organization Interpol estimates that total proceeds from environmental crimes are growing at a rate of at least 5% per year.⁵ Furthermore, there is reporting that in conflict zones, environmental crimes, including illegal exploitation and theft of oil, provide an estimated 38% of illicit income to armed groups, more than any other illicit activity, including drug trafficking.⁶

Environmental crimes encompass illegal activity that harm human health, and harm nature and natural resources by damaging environmental quality, including increasing carbon dioxide levels in the atmosphere, driving biodiversity loss, and causing the overexploitation of natural resources.⁷ This category of crimes includes (i) wildlife trafficking, (ii) illegal logging, (iii) illegal fishing, (iv) illegal mining, and (v) waste and hazardous substances trafficking.⁸ These crimes are relatively low risk activities with high rewards because enforcement efforts are limited, demand for the products and services generated by these crimes is high, and criminal penalties are not as severe as for other illicit activities. Environmental crimes frequently involve transnational organized crime and corruption and are often associated with a variety of other crimes including money laundering, bribery, theft, forgery, tax evasion, fraud, human trafficking, and drug trafficking. See appendix for additional information on each type of illicit activity.

115

Suspicious Activity Report Filing Instructions

Financial institutions' SAR filings, in conjunction with effective implementation of their Bank Secrecy Act (BSA) compliance requirements, are crucial to identifying and stopping environmental crimes and related money laundering.

- FinCEN requests that financial institutions reference only this notice in SAR field 2 (Filing Institution Note to FinCEN) using keyword "FIN-2021-NTC4;" this keyword should also be referenced in the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice.⁹
- Financial institutions should also select SAR field 38(z) (Other Suspicious Activities - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and environmental crimes and use the most relevant keyword for suspicious

FINCEN NOTICE

activity such as "wildlife trafficking," "illegal logging," "illegal fishing," "illegal mining," or "waste trafficking." If the suspicious activity involves multiple potential offenses, FinCEN also requests that filers include all relevant keywords in the narrative.

- Financial institutions may consider sharing information on suspected environmental crimes offenses under Section 314(b) for the purposes of identifying and reporting money laundering activity.¹⁰

116

SAR Narrative: FinCEN also requests that filers further detail how the suspicious activity relates to environmental crimes. Filers should provide any available details concerning how the illicit product, plant, or waste was solicited, acquired, stored, transported, financed, and paid for. Filers also should provide all available details (such as names, identifiers, and contact information—including Internet Protocol (IP) and email addresses and phone numbers) regarding: (i) any actual purchasers or sellers of the illicit product, plant, waste or waste disposal services, and their intermediaries or agents; (ii) the volume and dollar amount of the transactions involving an entity that is—or may be functioning as—a supplier of illicit products, plants, waste or waste services; and (iii) any beneficial owner(s) of involved entities (such as shell companies). In the case of illicit waste, filers should provide all available details and specific descriptions of the waste product and any known details about its origin, transport, and destination. If known, filers should provide information about the place(s) where the reported individuals or entities are operating.

For Further Information

Additional illicit finance information, including advisories and notices, can be found on FinCEN's website at <https://www.fincen.gov>, 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.

117

[HOME](#) [ABOUT](#) [RESOURCES](#) [NEWSROOM](#) [CAREERS](#) [ADVISORIES](#) [GLOSSARY](#)

FinCEN Analysis Reveals Upward Trend of SARs Related to Wildlife Trafficking

Contact: Office of Strategic Communications, press@fincen.gov
Immediate Release: December 20, 2021

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today released a [Financial Threat Analysis](#) on wildlife trafficking threat patterns and trend information identified in Bank Secrecy Act (BSA) data. The report aims to further inform efforts to combat wildlife trafficking and the associated movement of illicit proceeds, which are estimated to be between \$7 and \$23 billion per year and account for a quarter of all wildlife trade.

Wildlife trafficking is a major transnational organized crime that fuels corruption, threatens biodiversity, damages fragile ecosystems, and can have a significant negative impact on public health and the economy. It involves the illicit trade of protected animals, animal parts, and derivatives thereof, including procurement, transport, and distribution, in violation of international or domestic law, and money laundering related to this activity. To move, hide, and launder their proceeds, wildlife traffickers exploit weaknesses in financial and non-financial sectors, enabling further wildlife crimes and damaging financial integrity.

"Today's report demonstrates the critical role that financial institutions play in identifying wildlife trafficking and protecting the U.S. financial system from associated illicit finance through compliance with their BSA obligations," said FinCEN Acting Director Himamauli Das.

FinCEN's analysis of wildlife trafficking-related Suspicious Activity Reports (SARs) indicates that wildlife trafficking is affecting the U.S. financial sector. Overall, wildlife trafficking-related SARs filed between January 2018 and October 2021 trended significantly up and SARs filed in 2021 are on track to meet or exceed the amount of SARs filed in 2020 based on current trends.

FinCEN is calling attention to this threat because of: (1) its strong association with corruption and transnational criminal organizations, two of FinCEN's national anti-money laundering and countering the financing of terrorism priorities published in June 2021; (2) a need to enhance reporting and analysis of related illicit financial flows; and, (3) wildlife trafficking's contribution to biodiversity loss, damage to fragile ecosystems, and the increased likelihood of spreading of zoonotic diseases.

This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020, which requires FinCEN to periodically publish threat pattern and trend information derived from SARs, and is another example of FinCEN's increasing focus in this area. In November, FinCEN held a [FinCEN Exchange](#) session on environmental crimes and issued a [Notice](#) to call attention to an upward trend in environmental crimes and associated illicit financial activity.

###

118

FINANCIAL THREAT ANALYSIS

Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in Bank Secrecy Act Data

This report focuses on wildlife trafficking threat patterns and trend information identified in Bank Secrecy Act (BSA) data filed between January 2018 and October 2021.¹ The Financial Crimes Enforcement Network (FinCEN) issued national priorities for anti-money laundering and countering the financing of terrorism policy on June 30, 2021, which included corruption and transnational criminal organization activity as government-wide priorities, and highlighted wildlife trafficking as a transnational criminal organization-related concern. The information contained in this report is intended to provide to the public, including a wide range of businesses and industries, threat pattern and trend information regarding wildlife trafficking. The report also highlights the value of BSA information filed by regulated financial institutions.

Executive Summary: This report seeks to highlight and further inform efforts to combat wildlife trafficking and the associated movement of illicit proceeds, which are estimated to be between \$7 and \$23 billion per year, or approximately one quarter of the amount generated from the legal wildlife trade.² FinCEN is calling attention to this threat³ because of: (1) its strong association with corruption and transnational criminal organizations (TCOs), two of FinCEN's national anti-money laundering and countering the financing of terrorism (AML/CFT) priorities;⁴ (2) a need to enhance reporting and analysis of related illicit financial transactions;⁵ and, (3) wildlife trafficking's

contribution to biodiversity loss,⁶ damage to fragile ecosystems, and the increased likelihood of spreading of zoonotic diseases.⁷

119



FinCEN ADVISORY

FIN-2021-A004

November 8, 2021

Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Detecting and reporting ransomware payments are vital to holding ransomware attackers accountable for their crimes and preventing the laundering of ransomware proceeds.

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: "CYBER FIN-2021-A004" and select SAR field 42 (Cyber Event). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is updating and replacing its October 1, 2020 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments.¹ This updated advisory is in response to the increase of ransomware attacks in recent months against critical U.S. infrastructure, such as the May 2021 ransomware attack that disrupted the operations of Colonial Pipeline, the largest pipeline system for refined oil products in the United States. This attack led to widespread gasoline shortages that affected tens of millions of Americans. Other recent targets include entities in the manufacturing, legal services, insurance, financial services, health care, energy, and food production sectors.

FinCEN issued the original advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. The advisory provided 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. This amended advisory reflects information released by FinCEN in its Financial

Trend Analysis Report issued on October 15, 2021, and is part of the Department of the Treasury's broader efforts to combat ransomware.² In particular, this updated advisory identifies new trends

120

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

121

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.³³

- 1 A financial institution or its customer detects IT enterprise activity that is connected to ransomware cyber indicators or known cyber threat actors. Malicious cyber activity may be evident in system log files, network traffic, or file information.³⁴
- 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 is connected to ransomware variants,³⁵ payments, or related activity. These connections may appear in open sources or commercial or government analyses.
- 4 An irregular 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.

122

122

FINCEN ADVISORY

- 5 A DFIR or CIC customer receives funds from a counterparty 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 customer that has no or limited history of CVC transactions sends a large CVC transaction, particularly when 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 foreign-located CVC exchanger in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.
- 10 A customer receives CVC from an external wallet, and immediately initiates multiple, rapid trades among multiple CVCs, especially AECs, with no apparent related purpose, followed by a transaction off the platform. This may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.
- 11 A customer initiates a transfer of funds involving a mixing service.
- 12 A customer uses an encrypted network (e.g., the onion router) or an unidentified web portal to communicate with the recipient of the CVC transaction.

3

123

FINCEN ADVISORY

Ransomware Payments Require Immediate Attention

It is critical that financial institutions (including CVC exchanges) identify and immediately report any suspicious transactions associated with ransomware attacks. For purposes of meeting a financial institution's SAR obligations, FinCEN and law enforcement consider suspicious transactions involving ransomware attacks to constitute "situations involving violations that require immediate attention."⁴¹ Financial institutions wanting to report suspicious transactions related to recent or ongoing ransomware attacks should contact FinCEN's Financial Institution Hotline at 1-866-556-3974. Financial institutions must subsequently file a SAR using FinCEN's BSA E-filing System, providing as much of the relevant details around the activity as available at that time. Amended SARs should be filed to include additional information related to the same activity that is learned later; completely new activity should be filed in a new "initial" SAR filing.

SAR Filing Instructions

FinCEN requests that financial institutions reference this advisory by including the key term:

"CYBER-FIN-2021-A004"

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.⁴²

124

124

Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021

This Financial Trend Analysis focuses on ransomware pattern and trend information identified in Bank Secrecy Act (BSA) data. This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020 (AMLA) which requires the Financial Crimes Enforcement Network (FinCEN) to periodically publish threat pattern and trend information derived from financial institutions' Suspicious Activity Reports (SARs).¹ FinCEN issued government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) policy on 30 June 2021, which included cybercrime as a government-wide priority. FinCEN highlighted ransomware as a particularly acute cybercrime concern. The information contained in this report is relevant to the public, including a wide range of businesses, industries, and critical infrastructure sectors. The report also highlights the value of BSA information filed by regulated financial institutions.

Executive Summary: This Financial Trend Analysis is in response to the increase in number and severity of ransomware attacks against U.S. critical infrastructure since late 2020. For example, in May 2021, hackers used a ransomware attack to extort a multi-million dollar ransom, which also disrupted the Colonial Pipeline and caused gasoline shortages. Other recent attacks have targeted various sectors, including manufacturing, legal, insurance, health care, energy, education, and the food supply chain in the United States and across the globe. As Treasury Secretary Janet L. Yellen recently noted, "Ransomware and cyber-attacks are victimizing businesses large and small across America and are a direct threat to our economy."²

FinCEN analysis of ransomware-related SARs filed during the first half of 2021 indicates that ransomware is an increasing threat to the U.S. financial sector, businesses, and the public. The number of ransomware-related SARs filed monthly has grown rapidly, with 635 SARs filed and 458 transactions reported between 1 January 2021 and 30 June 2021 ("the review period"), up 30 percent from the total of 487 SARs filed for the entire 2020 calendar year.³ The total value of suspicious activity reported in ransomware-related SARs during the first six months of 2021 was \$590 million, which exceeds the value reported for the entirety of 2020 (\$416 million).

Trends represented in this report illustrate financial institutions' identification and reporting of ransomware events and may not reflect the actual dates associated with ransomware incidents. FinCEN's analysis of ransomware-related SARs highlights average ransomware payment amounts, top ransomware variants, and insights from FinCEN's blockchain analysis:

125



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.²

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. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

This advisory describes the potential sanctions risks associated with making and facilitating ransomware payments and provides information for contacting relevant U.S. government agencies, including OFAC if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.³

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

126



FinCEN NOTICE

FIN-2021-NTC3

September 16, 2021

FinCEN Calls Attention to Online Child Sexual Exploitation Crimes

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to call attention to an increase in online child sexual exploitation (OCSE). This Notice provides financial institutions with specific suspicious activity report (SAR) filing instructions, and highlights some financial trends related to OCSE.

Crimes related to OCSE, including the funding, production, and distribution of child sexual abuse materials (CSAM), have increased during the COVID-19 pandemic, according to multiple law enforcement authorities. This increase in activity is likely due to a confluence of factors, including: (1) increased internet usage by children who are spending more time online, both unsupervised and during traditional school hours; (2) restricted travel during the COVID-19 pandemic resulting in more sex offenders being online; and (3) increased access to and use of technology, including encrypted communications, bulk data transfer, cloud storage, live-streaming, and anonymized transactions.¹ Another trend is the rise in sextortion of minors, who are coerced or exploited into exchanging sexual images via the internet, mobile devices, and social media platforms.² OCSE offenders often groom³ minors to share or post self-generated content online in exchange for money.

FinCEN performed a review of OCSE-related SARs and observed the following trends. Between 2017 and 2020, there was a 147 percent increase in OCSE-related SAR filings, including a 17 percent year-over-year increase in 2020. FinCEN also observed that OCSE offenders are increasingly

127

FINCEN NOTICE

using convertible virtual currency (CVC) (some of which provide anonymity), peer-to-peer mobile applications, the darknet, and anonymization and encryption services to try to avoid detection. CVC in particular is increasingly the payment method of choice for OCSE offenders who make payments to websites that host CSAM.⁴ Finally, FinCEN found that OCSE facilitators attempt to conceal their illicit file sharing and streaming activities by transferring funds via third-party payment processors.⁵

Suspicious Activity Report (SAR) Filing Instructions

SARs, in conjunction with effective implementation of other BSA requirements, are crucial to identify and stop cybercrimes, including OCSE. Financial institutions should provide all pertinent and available information in the SAR narrative and attachments.⁶

- FinCEN requests that financial institutions reference only this notice in SAR field 2 (Filing Institution Note to FinCEN) using the keyword "OCSE-FIN-2021-NTC3"; this keyword should also be referenced in the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice. Financial institutions may highlight additional advisory keywords in the narrative, if applicable.
- Financial institutions should also select SAR Field 38(z) (Other) as the associated suspicious activity type to indicate a connection between the suspicious activity reported and OCSE activity and include the term "OCSE" in the text box. If known, enter the subject's internet-based contact with the financial institution in SAR Field 43 (IP Address and Date).
- If human trafficking or human smuggling are suspected in addition to OCSE activity, financial institutions should also select SAR Field 38(h) (Human Trafficking) or SAR Field 38(g) (Human Smuggling), respectively.⁷
- FinCEN asks that reporting entities use the [Child Sexual Exploitation \(CSE\) terms and definitions in the appendix below](#) when describing suspicious activity, which will assist FinCEN's analysis of the SARs.

128

FINCEN NOTICE

Appendix: CSE Terms and Definitions⁹

Term	Definition
Child Sexual Exploitation ¹⁰	This conduct includes travel in interstate or foreign commerce to engage in illicit sexual conduct with any child under the age of 18; extraterritorial child sexual abuse committed by U.S. citizens and nationals; child sex trafficking; and all other acts involving criminal sexual abuse of children under the age of 18.
Offenses Involving Child Pornography ^{11,12}	The production, advertisement, distribution, receipt, or possession of child pornography, or the livestreaming of child sexual abuse. Production of child pornography includes "sextortion," where offenders use deceit or non-physical forms of coercion, such as blackmail, to acquire child pornography depicting the targeted minors. ¹³ Child pornography is any visual depiction (photo, video, or livestream) showing minors involved in sexually explicit conduct. ¹⁴
Online Child Sexual Exploitation ¹⁵	The use of the internet or mobile phones as a means (1) to engage or attempt to engage in child sexual exploitation; (2) to persuade, induce, entice or coerce a minor to engage in any illegal sexual activity; or (3) to commit an offense involving child sexual abuse material.
Facilitator/ Intermediary ¹⁶	Facilitators and intermediaries are the individuals or entities whose conduct facilitates or aids and abets the commission of the sexual offense against the child.

129



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

130

130

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

131

131

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.

132

132

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.

133

133

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.

134

134

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.

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.

135



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/advisories/bulletins/fact-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.

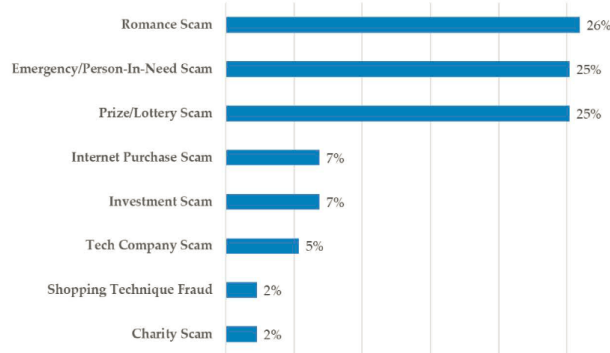
- Total numbers of filings and total suspicious activity amounts increased 20 percent and 30 percent, respectively, each year during the time period.*
- Money Services Business (MSB) reporting indicated elders fell victim to scams in which they sent money overseas, most often to receivers in African 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.

136

136

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.

137

137

Financial institutions can help prevent elder financial exploitation with alerts to trusted contacts

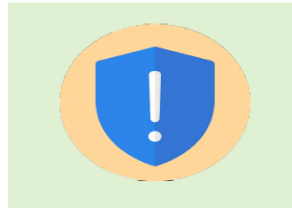
The Consumer Financial Protection Bureau (CFPB) provides voluntary recommendations in this advisory for financial institutions to help them prevent elder financial exploitation with alerts to trusted contacts.

Your institution may already permit, or may someday permit, account holders to designate a trusted contact person for your staff to contact with specific concerns. For example, an account holder may identify a family member or close friend to contact if staff suspects that the account holder if you suspect that the account holder may be at risk of financial exploitation. A trusted contact is an emergency financial contact who can step in to help protect the account holder.

This can be a helpful service for account holders and can also signal to consumers that your institution is taking steps to help protect their assets and prevent financial exploitation. This advisory examines how alerts to a trusted contact can be helpful for your institution and your account holders.

How might alerts to a trusted contact help during a suspicious situation?

Lara, a long-time account holder, listed her adult daughter as a trusted contact and provided written



consent for the financial institution to contact her daughter if there is a concern that Lara might be at risk of financial exploitation.

Today, Lara visits a branch to wire a large sum of money to a new friend overseas for an emergency situation, which is uncharacteristic behavior for Lara. The teller asks some questions about the situation and suspects that Lara may be experiencing a scam.

The teller alerts a supervisor, who speaks with Lara further and expresses concerns about the transaction. If a discussion with Lara does not relieve concerns about the threat, financial institution staff could reach out to Lara's daughter about their concerns and encourage her to intervene.

138

138

FFIEC BANK SECRECY ACT/ANTI-MONEY LAUNDERING INFOBASE

Prompt delivery of introductory, reference, and educational training material on specific topics of interest to field examiners from FFIEC members

View the online [BSA/AML Examination Manual and Procedures](#).

Welcome to the FFIEC Bank Secrecy Act/Anti-Money Laundering InfoBase. The "FFIEC InfoBase" concept was developed by the FFIEC's Task Force on Examiner Education and the Task Force on Supervision to provide field examiners at the financial institution regulatory agencies with an electronic source for training and distributing needed examination information. Financial institutions will also 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 concern to examiners within the FFIEC's member agencies: Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau and the State Liaison Committee. The SLC includes representatives from the Conference of State Bank Supervisors, the American Council of State Savings Supervisors, and the National Association of State Credit Union Supervisors.

139

FFIEC BSA/AML Examination Manual Change History Log

12/1/21

Date	Sections Changed	Change Description
05/11/2018	<ol style="list-style-type: none"> 1. Customer Due Diligence 2. Beneficial Ownership for Legal Entity Customers 	<ul style="list-style-type: none"> • Revised the Customer Due Diligence section • Added a new Beneficial Ownership for Legal Entity Customers section
4/15/2020	<ol style="list-style-type: none"> 1. Table of Contents 2. Scoping and Planning 3. BSA/AML Risk Assessment 4. Assessing the BSA/AML Compliance Program 5. Developing Conclusions and Finalizing the Exam 	<ul style="list-style-type: none"> • Revised all sections titles consistent with the new structure • Added a new Risk-Focused BSA/AML Supervision section and revised content in Developing the BSA/AML Examination Plan section under Scoping and Planning • Revised content in the BSA/AML Risk Assessment section • Added a new introductory section and created individual sections with revised content for BSA/AML Internal Controls, BSA/AML Independent Testing, BSA Compliance Officer, and BSA/AML Training under Assessing the BSA/AML Compliance Program • Revised content in the Developing Conclusions and Finalizing the Exam section
2/25/2021	<ol style="list-style-type: none"> 1. Assessing Compliance with Bank Secrecy Act Regulatory Requirements 2. Customer Identification Program 3. Currency Transaction Reporting 4. Transactions of Exempt Persons 	<ul style="list-style-type: none"> • Added a new introductory section • Revised content in the Customer Identification Program, Currency Transaction Reporting, and Transactions of Exempt Persons sections under Assessing Compliance with BSA Regulatory Requirements
6/21/2021	<ol style="list-style-type: none"> 1. Purchase and Sale of Monetary Instruments Recordkeeping 2. Special Measures 3. Reports of Foreign Financial Accounts 4. International Transportation of Currency or Monetary Instruments Reporting 	<ul style="list-style-type: none"> • Revised content in the Purchase and Sale of Monetary Instruments Recordkeeping, Special Measures, Reports of Foreign Financial Accounts, and International Transportation of Currency or Monetary Instruments Reporting sections under Assessing Compliance with BSA Regulatory Requirements
12/1/2021	<ol style="list-style-type: none"> 1. Introduction – Customers 2. Charities and Nonprofit Organizations 3. Independent Automated Teller Machine Owners or Operators 4. Politically Exposed Persons 	<ul style="list-style-type: none"> • Added a new introductory section • Revised content in Charities and Nonprofit Organizations, Independent Automated Teller Machine Owners or Operators, and Politically Exposed Persons sections under Risks Associated with Money Laundering and Terrorist Financing

140


FFIEC

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

[Home](#) | [Site Index](#) | [Disclaimer](#) | [Privacy Policy](#) | [Accessibility](#)

[About the FFIEC](#)
[Contact Us](#)
[Search](#)
[Press Releases and Announcements](#)
[Enforcement Actions](#)
[What's New](#)
[Consumer Compliance](#)
[Computational Tools](#)
[Reports](#)
[Consumer Help Center](#)
[Financial Institution Info](#)
[Examiner Education](#)
[Supervisory Info](#)
[Cybersecurity Awareness](#)
[Federal Register](#)
[Freedom of Information Act](#)
[EGRPRA \(Economic Growth and Regulatory Paperwork Reduction Act of 1996\)](#)
[Industry Outreach](#)

Press Release

For Immediate Release December 1, 2021

Federal and State Regulators Release Updates to the BSA/AML Examination Manual

The Federal Financial Institutions Examination Council (FFIEC) today released one new section and updates to three sections of the *Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*. Today's updates affect the following sections:

- Introduction - Customers (new)
- Charities and Nonprofit Organizations
- Independent Automated Teller Machine Owners or Operators
- Politically Exposed Persons


The updates should not be interpreted as new requirements or as a new or increased focus on certain areas. Rather, these sections provide information and considerations related to certain customers that may indicate the need for bank policies, procedures, and processes to address potential money laundering, terrorist financing, and other illicit financial activity risks. These sections provide further transparency into the BSA/AML examination process.

The sections also remind examiners that no specific customer type automatically presents a higher risk of money laundering, terrorist financing, or other illicit financial activity. Further, banks that operate in compliance with applicable BSA/AML requirements and reasonably manage and mitigate risks related to the unique characteristics of customer relationships are neither prohibited nor discouraged from providing accounts or services to any specific class or type of customer.

The manual provides instructions to examiners for assessing the adequacy of a bank's or credit union's BSA/AML compliance program and its compliance with BSA regulatory requirements. The manual itself does not establish requirements for banks; such requirements are found in statutes and regulations. FFIEC agencies worked closely with Treasury's Financial Crimes Enforcement Network on today's updates.

Attachments:


141



FFIEC
FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL


[MANUAL](#) | [EXAMINATION PROCEDURES](#) | [REFERENCES](#) | [FFIEC HOME](#)


BSA/AML INFOBASE MANUAL


Quickly access all the sections of the BSA/AML Manual



INTRODUCTION
An introduction to the FFIEC BSA/AML Examination Manual and related concepts.



ASSESSING THE BSA/AML COMPLIANCE PROGRAM
Guidance to examiners on assessing the bank's BSA/AML compliance program.



OFFICE OF FOREIGN ASSETS CONTROL
Guidance to examiners on assessing the bank's compliance with Office of Foreign Assets Control (OFAC) regulations.



SCOPING AND PLANNING
Guidance to examiners on risk-focused supervision and developing the examination plan.


DEVELOPING CONCLUSIONS AND FINALIZING THE EXAM
Guidance to examiners on developing conclusions and finalizing the examination.


PROGRAM STRUCTURES
Guidance to examiners on assessing BSA/AML compliance program structures, management of foreign branches, and parallel banking.


BSA/AML RISK ASSESSMENT
Guidance to examiners on reviewing the bank's BSA/AML risk assessment process.


ASSESSING COMPLIANCE WITH BSA REGULATORY REQUIREMENTS
Guidance to examiners on assessing compliance with other statutory and regulatory BSA requirements.


RISKS ASSOCIATED WITH MONEY LAUNDERING AND TERRORIST FINANCING
Guidance to examiners on money laundering and terrorist financing risks associated with products, services, customers, and geographic locations.

142

Assessing Compliance with BSA Regulatory Requirements

Sections	View	Download	Multiple	Examination Procedures
Introduction (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	<i>Not Applicable</i>
Customer Identification Program (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Customer Due Diligence (2018)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Beneficial Ownership Requirements for Legal Entity Customers (2018)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Suspicious Activity Reporting (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Currency Transaction Reporting (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Transactions of Exempt Persons (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Information Sharing (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Purchase and Sale of Certain Monetary Instruments Recordkeeping (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Funds Transfers Recordkeeping (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Foreign Correspondent Account Recordkeeping, Reporting and Due Diligence (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Private Banking Due Diligence Program (Non-U.S. Persons) (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Special Measures (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Reports of Foreign Financial Accounts (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
International Transportation of Currency or Monetary Instruments Reporting (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online

143

Risks Associated with Money Laundering and Terrorist Financing

Sections	View	Download	Multiple	Examination Procedures
Introduction - Customers (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	<i>Not Applicable</i>
Correspondent Accounts (Domestic) (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Correspondent Accounts (Foreign) (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Bulk Shipments of Currency (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
U.S. Dollar Drafts (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Payable Through Accounts (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Pouch Activities (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Electronic Banking (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Funds Transfers (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Automated Clearing House Transactions (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Prepaid Access (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Third-Party Payment Processors (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Purchase and Sale of Monetary Instruments (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Brokered Deposits (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Independent Automated Teller Machine Owners or Operators (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online

144

Nondeposit Investment Products (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Insurance (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Concentration Accounts (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Lending Activities (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Trade Finance Activities (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Private Banking (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Trust and Asset Management Services (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Nonresident Aliens and Foreign Individuals (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Politically Exposed Persons (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Embassy, Foreign Consulate, and Foreign Mission Accounts (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Non-Bank Financial Institutions (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Professional Service Providers (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Charities and Nonprofit Organizations (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Business Entities (Domestic and Foreign) (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online
Cash-Intensive Businesses (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Online

145

Appendices				
Sections	View	Download	Multiple	Examination Procedures
Appendix 1 – Beneficial Ownership (2018)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix A – BSA Laws and Regulations (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix B – BSA/AML Directives (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix C – BSA/AML References (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix D – Statutory Definition of Financial Institution (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix E – International Organizations (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix F – Money Laundering and Terrorist Financing Red Flags (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix G – Structuring (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix H – Request Letter Items (Core and Expanded) (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix I – Risk Assessment Link to the BSA/AML Compliance Program (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix J – Quantity of Risk Matrix (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix K – Customer Risk Versus Due Diligence and Suspicious Activity Monitoring (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix L – SAR Quality Guidance (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix M – Quantity of Risk Matrix – OFAC Procedures (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix N – Private Banking – Common Structure (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix O – Examiner Tools for Transaction Testing (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix P – BSA Record Retention Requirements (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix Q – Abbreviations (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix R – Enforcement Guidance (2020)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix S – Key Suspicious Activity Monitoring Components (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
Appendix T – BSA E-Filing System (2014)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable

146

146

ACH - SAR “Opportunities”

• RDFI – Examples

- Transaction Volume “Swings” – perhaps isolate to a single client;
- “Unexpected” IAT entry – 9/18/2009;
- Possible tax refund fraud – multiple tax refund credits for different individuals in one account;
- Possible Healthcare Fraud (HCCLAIMPMT);
- Inbound (“Known”) illegal Internet gambling credit(s) for commercial client(s);
- R10 – Consumer advises debit was not authorized – above SAR limits;
- R29 – Corporate client advises debit was not authorized – above SAR limits;
- Federal Reclamation > \$ 5,000 – Suspect is known;
- Garnishment or claims of judgment creditors could launch transactional review.

ProBank Trusted.
Advisor Compliance.
Advice.



147

ACH - SAR “Opportunities”

• ODFI

- Transaction Volume “Swings” – Explanations / Clients
- Originators whose business or occupation does not warrant the volume or nature of ACH activity – E.g. IAT originations that are “inconsistent” – 9/18/2009;
- Large-value ACH transactions frequently initiated through TPSPs/TPSs by Originators that are not clients of the DFI and for which the DFI has no or insufficient CDD information thereon;
- Originators whose origination activity suddenly exceeds projections/credit limits with no reasonable explanation for such;
- Originators (especially TPPPs) generating a high rate or high volume of invalid account returns, unauthorized returns, or other unauthorized transactions;
 - R02 (Acct. Closed) / R03 (No Acct.) / R04 (Invalid Acct.) if volumes exceed “normal”
 - R05 (Corp. Debit posted to consumer acct) / R07 (Authorization Revoked) / R37 (“Double Dip”)
 - R05, R07, R10 (Consumer advises not authorized), R11 (Consumer Advises Entry not in accordance with the authorization), R29 (Corporate Client advises not authorized), & R51 (Ineligible RCK item) ,where return rate exceeds 0.5%.

ProBank Trusted.
Advisor Compliance.
Advice.



148

Staff (All) SAR “Responsibilities”

- **From an operations standpoint, the key is that the team knows:**
 - **What is SAR;**
 - **Who does SAR within;**
 - **How are suspicious transactions to be referred to the SAR coordinator;**
 - **Understand specific Staff – SAR opportunities.**

ProBank Trusted.
Advisor Compliance.
Advice.



149

05/18/21 – HIDTA Update

PUBLISHED DOCUMENT

AGENCY:
Office of National Drug Control Policy (ONDCP).

ACTION:
Notice of six HIDTA designations.

SUMMARY:
The Director of the Office of National Drug Control Policy designated six additional areas as High Intensity Drug Trafficking Areas (HIDTA).. The new areas are (1) Daviess County in Kentucky as part of the Appalachia HIDTA; (2) El Dorado and Placer Counties in California as part of the Central Valley California HIDTA; (3) Madison and St. Clair Counties in Illinois as part of the Midwest HIDTA; and (4) Erie County in Pennsylvania as part of the Ohio HIDTA.

FOR FURTHER INFORMATION CONTACT:
Questions regarding this notice should be directed to Shannon L. Kelly, National HIDTA Director, Office of National Drug Control Policy, Executive Office of the President, Washington, DC 20503; (202) 395-5872.

Dated: May 18, 2021.

DOCUMENT DETAILS

Printed version:
[PDF](#)

Publication Date:
05/24/2021

Agencies:
[Executive Office of the President](#)
[Office of National Drug Control Policy](#)

Document Type:
Notice

Document Citation:
86 FR 27903



Page:
27903 (1 page)

Document Number:
2021-10852


DOCUMENT STATISTICS

Page views:
825
as of 06/28/2021 at 10:15 pm EDT

150

Mark W. Dever, AAP, CAMS
Vice President & Senior Consultant
Education and ProBank Advisor
ProBank Austin
502-479-5246
mdever@probank.com




151

**VIRGINIA BANKERS
ASSOCIATION**

**Thank you for joining us for today's
program.**

**Please visit our website at
www.vabankers.org for upcoming Live-
Streaming Events & Webinars.**



152