

Vendor Opportunities - AML / Risk Management

(NOTE: Not a **FORVIS** 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
- Optima Compass Global Compliance – “AML Compass” – <https://optimacompass.com/aml-technology/>
- “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 Education Services *powered by* **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

1

1

RFC – Indorsement and Payment of Checks Drawn on U.S. Treasury

88 FR 6674 – 6679

02/01/23

Comments Due: 04/03/23

DEPARTMENT OF THE TREASURY

Bureau of the Fiscal Service

31 CFR Part 240

RIN 1530-AA22

Indorsement and Payment of Checks Drawn on the United States Treasury

AGENCY: Bureau of the Fiscal Service,
Treasury.

ACTION: Notice of proposed rulemaking
with request for comment.

SUMMARY: The Bureau of the Fiscal Service (Fiscal Service) at the Department of the Treasury (Treasury) is proposing to amend its regulations governing the payment of checks drawn on the United States Treasury. Specifically, to prevent Treasury checks from being negotiated after cancellation by Treasury or a payment certifying agency—also known as payments over cancellation (POCs)—Fiscal Service is proposing amendments that would require financial institutions use the Treasury Check Verification System (TCVS), or other similar authorized system, to verify that Treasury checks are both authentic and valid. This

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

2

2

RFC – Indorsement and Payment of Checks Drawn on U.S. Treasury

88 FR 6674 – 6679

02/01/23

Comments Due: 04/03/23

SUPPLEMENTARY INFORMATION:

I. Background

Currently, when either Treasury or a payment certifying agency puts a “stop payment” (or “check stop”) on a Treasury check to cancel it, the canceled check may still be negotiated, which leads to a POC. POCs are improper payments that amount to approximately \$98 million each year. Resolving POCs also costs the Federal Government approximately \$1.3 million each year.

Financial institutions often have access to real-time or same-day check verification information to ensure that non-Treasury checks have not been canceled, and soon this will be the case for Treasury checks as well. Fiscal Service’s Treasury Check Verification System (TCVS) provides verification information for Treasury checks, but currently TCVS has a one-day lag. However, Fiscal Service expects to complete enhancements to TCVS that will allow same-day verification by mid-2023.

3

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

3

RFC – Indorsement and Payment of Checks Drawn on U.S. Treasury

88 FR 6674 – 6679

02/01/23

Comments Due: 04/03/23

After enhancements to Treasury’s systems have been implemented and same-day Treasury check verification is functional, Fiscal Service proposes requiring that a financial institution use its check verification system when negotiating a Treasury check if the financial institution is to avoid liability for accepting a Treasury check that has been canceled. Financial institutions will be notified via a communication from the Federal Reserve’s Customer Relations Support Office, **Federal Register** notice, and/or other appropriate means at least 30 days prior to the date that enhanced TCVS will become available for use and this requirement becomes effective.

Under existing rules, financial institutions are required to use “reasonable efforts” to ensure that a Treasury check is authentic (*i.e.*, not counterfeit) and also are responsible if they accept a Treasury check that has been previously negotiated, but they are not required to ensure that a Treasury check has not been canceled. The definition of “reasonable efforts” found in 31 CFR 240.2 does not currently include a requirement to use Treasury’s check verification system to ensure that a Treasury check is valid (*i.e.*, a payable instrument that has not been canceled and meets the criteria for negotiability). Fiscal Service proposes revising the definition of “reasonable efforts” to include this verification process.

4

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

4

Supervisory Highlights Junk Fees Special Edition

Issue 29, Winter 2023

Table of contents

Table of contents	1
1. Introduction	2
2. Supervisory Observations	3
2.1 Deposits.....	3
2.2 Auto Servicing.....	6
2.3 Mortgage Servicing.....	9
2.4 Payday and Small-Dollar Lending	13
2.5 Student Loan Servicing.....	14
3. Supervisory Program Developments	16
3.1 Recent Bureau Supervisory Program Developments.....	16
4. Remedial Actions.....	18
4.1 Public Enforcement Actions.....	18

2.1.1 Unfair Authorize Positive, Settle Negative Overdraft Fees

As described below, Supervision has cited institutions for unfair unanticipated overdraft fees for transactions that authorized against a positive balance, but settled against a negative balance (i.e., APSN overdraft fees). They can occur when financial institutions assess overdraft fees for debit card or ATM transactions where the consumer had a sufficient available balance at the time the financial institution authorized the transaction, but given the delay between authorization and settlement of the transaction the consumer's account balance is insufficient at the time of settlement. This can occur due to intervening authorizations resulting in holds, settlement of other transactions, timing of presentment of the transaction for settlement, and other complex processes relating to transaction order processing practices and other financial institution policies. The Bureau previously discussed this practice in Consumer Financial Protection Circular 2022-06, Unanticipated Overdraft Fee Assessment Practices ("Overdraft Circular").⁷

Supervision has cited unfair acts or practices at institutions that charged consumers APSN overdraft fees. An act or practice is unfair when: (1) it causes or is likely to cause substantial injury to consumers; (2) the injury is not reasonably avoidable by consumers; and (3) the injury is not outweighed by countervailing benefits to consumers or to competition.⁸

While work is ongoing, at this early stage, Supervision has already identified at least tens of millions of dollars of consumer injury and in response to these examination findings, institutions are providing redress to over 170,000 consumers. Supervision found instances in which institutions assessed unfair APSN overdraft fees using the consumer's available balance for fee decisioning, as well as unfair APSN overdraft fees using the consumer's ledger balance for fee decisioning. Consumers could not reasonably avoid the substantial injury, irrespective of account-opening disclosures. As a result of examiner findings, the institutions were directed to cease charging APSN overdraft fees and to conduct lookbacks and issue remediation to consumers who were assessed these fees.

Supervision also issued matters requiring attention to correct problems that occurred when institutions had enacted policies intended to eliminate APSN overdraft fees, but APSN fees were still charged. Specifically, institutions attempted to prevent APSN overdraft fees by not assessing overdraft fees on transactions which authorized positive, as long as the initial authorization hold was still in effect at or shortly before the time of settlement. There were some transactions, however, that settled outside this time period. Examiners found evidence of inadequate compliance management systems where institutions failed to maintain records of transactions sufficient to ensure overdraft fees would not be assessed, or failed to use some other solution to not charge APSN overdraft fees. In response to these findings, the institutions agreed to implement more effective solutions to avoid charging APSN overdraft fees and to issue remediation to the affected consumers.

The Bureau has stated the legal violations surrounding APSN overdraft fees both generally and in the context of specific public enforcement actions will result in hundreds of millions of dollars of redress to consumers.⁹ As discussed in a June 16, 2022 blog post, Supervision has also engaged in a pilot program to collect detailed information about institutions' overdraft practices, including whether institutions charged APSN overdraft fees.¹⁰ A number of banks that had previously reported to Supervision engaging in APSN overdraft fee practices now report that they will stop doing so. Institutions that have reported finalized remediation plans to Supervision state their plans cover time periods starting in 2018 or 2019 up to the point they ceased charging APSN overdraft fees.

2.1.2 Assessing multiple NSF fees for the same transaction

Supervision conducted examinations of institutions to review certain practices related to charging consumers non-sufficient funds (NSF) fees. As described in more detail below, examiners conducted a fact-intensive analysis at various institutions to assess specific types of NSF fees. In some of these examinations, examiners found unfair practices related to the assessment of multiple NSF fees for a single transaction.

Some institutions assess NSF fees when a consumer pays for a transaction with a check or an Automated Clearing House (ACH) transfer and the transaction is presented for payment, but there is not a sufficient balance in the consumer's account to cover the transaction. After declining to pay a transaction, the consumer's account-holding institution will return the transaction to the payee's depository institution due to non-sufficient funds and may assess an NSF fee. The payee may then present the same transaction to the consumer's account-holding institution again for payment. If the consumer's account balance is again insufficient to pay for the transaction, then the consumer's account-holding institution may assess another NSF fee for the transaction and again return the transaction to the payee. Absent restrictions on assessment of NSF fees by the consumer's account-holding institution, this cycle can occur multiple times.

Supervision found that institutions engaged in unfair acts or practices by charging consumers multiple NSF fees when the same transaction was presented multiple times for payment against an insufficient balance in the consumer's accounts, potentially as soon as the next day. The assessment of multiple NSF fees for the same transaction caused substantial monetary harm to consumers, totaling millions of dollars. These injuries were not reasonably avoidable by consumers, regardless of account opening disclosures. And the injuries were not outweighed by countervailing benefits to consumers or competition.

Examiners found that institutions charged several million dollars to tens of thousands of consumers over the course of several years due to their assessment of multiple NSF fees for the same transaction. The institutions agreed to cease charging NSF fees for unpaid transactions entirely and Supervision directed the institutions to refund consumers appropriately. Other regulators have spoken about this practice as well.¹¹

In the course of obtaining information about institutions' overdraft and NSF fee practices, examiners obtained information regarding limitations related to the assessment of NSF fees. Supervision subsequently heard from a number of institutions regarding changes to their NSF fee assessment practices. Virtually all institutions that Supervision has engaged with on this issue reported plans to stop charging NSF fees altogether.

Supervision anticipates engaging in further follow-up work on both multiple NSF fee and APSN overdraft fee issues. In line with the Bureau's statement regarding responsible business conduct, institutions are encouraged to "self-assess [their] compliance with Federal consumer financial law, self-report to the Bureau when [they identify] likely violations, remediate the harm resulting from these likely violations, and cooperate above and beyond what is required by law" with these efforts.¹² As the statement notes, "...the Bureau's Division of Supervision, Enforcement, and Fair Lending makes determinations of whether violations should be resolved through non-public supervisory action or a possible public enforcement action through its Action Review Committee (ARC) process." For those institutions that meaningfully engage in responsible conduct, this "could result in resolving violations non-publicly through the supervisory process."

FDIC FIL 40-2022 – Supervisory Guidance Re-Presentation NSF Fees

The screenshot shows the FDIC website header with navigation links: ABOUT, RESOURCES, ANALYSIS, NEWS, and a search icon. The main heading is "Financial Institution Letter" followed by "Supervisory Guidance on Multiple Re-Presentation NSF Fees". The date is "August 18, 2022" and the file number is "FIL-40-2022". There are social media share buttons for Facebook, Twitter, LinkedIn, and Email. The page is divided into sections: "Contact:" (Division of Depositor and Consumer Protection, Supervisor/Staff/FDIC.org), "Notes:" (links to the FDIC website and a subscription form), "About the FDIC:" (description of the Federal Deposit Insurance Corporation), "Summary:" (overview of the guidance), "Highlights:" (bullet points detailing the guidance's focus on NSF fees, multiple charges, and consumer protection), and "Attachment:".

ProBank Education Services powered by **FORVIS**

13

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

13

CFPB Issues Guidance to Help Banks Avoid Charging Illegal Junk Fees on Deposit Accounts

Agency highlights surprise overdraft and surprise depositor fees

OCT 26, 2022

SHARE & PRINT



87 FR 66935 –
66942
11/07/22

Washington, D.C. - Today, the Consumer Financial Protection Bureau (CFPB) issued guidance about two junk fee practices that are likely unfair and unlawful under existing law. The first, surprise overdraft fees, includes overdraft fees charged when consumers had enough money in their account to cover a debit charge at the time the bank authorizes it. The second is the practice of indiscriminately charging depositor fees to every person who deposits a check that bounces. The penalty is an unexpected shock to depositors who thought they were increasing their funds.

"Americans are willing to pay for legitimate services at a competitive price, but are frustrated when they are hit with junk fees for unexpected or unwanted services that have no value to them," said CFPB Director Rohit Chopra. "We are providing guidance on existing law that will help law-abiding businesses seeking to fairly compete and the families they serve."

Overdraft and depositor fees likely violate the Consumer Financial Protection Act prohibition on unfair practices when consumers cannot reasonably avoid them. Today's [Consumer Financial Protection Circular](#) on surprise overdraft fees and the CFPB's [compliance bulletin on surprise depositor fees](#) lay out when a financial institution's back-end penalties likely break the law.

ProBank Education Services powered by **FORVIS**

14

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

14

CFPB Proposes Rule to Rein in Excessive Credit Card Late Fees

Proposed rule seeks to close loophole exploited by companies to hike fees with inflation

FEB 01, 2023

SHARE & PRINT



WASHINGTON, D.C. – Today, the Consumer Financial Protection Bureau (CFPB) proposed a rule to curb excessive credit card late fees that cost American families about \$12 billion each year. Major credit card issuers continue to profit off late fees that are protected by an expansive immunity provision. Credit card companies have also relied on this provision to hike fees with inflation, even if they face no additional collection costs. The proposed rule would help ensure that over the top late fee amounts are illegal. Based on the CFPB's estimates, the proposal could reduce late fees by as much as \$9 billion per year.

"Over a decade ago, Congress banned excessive credit card late fees, but companies have exploited a regulatory loophole that has allowed them to escape scrutiny for charging an otherwise illegal junk fee," said CFPB Director Rohit Chopra. "Today's proposed rule seeks to save families billions of dollars and ensure the credit card market is fair and competitive."

When someone misses a payment due date, even if they paid a few hours after the deadline, the cardholder may be hit with an exorbitant late fee that far exceeds the credit card company's costs to collect late payments. These excessive late fees may not be needed to deter late payments, nor be justified based on the consumer's conduct in paying late. These late fees also may be on top of other consequences of paying late, such as a lost grace period on paying interest or a lower credit score, depending on how long the missed payment lasts.

Companies currently charge people as much as \$41 for each missed payment, and these fees result in billions of dollars in annual junk fee revenue for credit card companies. The CFPB's proposed changes, which would amend regulations implementing the Credit Card Accountability Responsibility and Disclosure Act of 2009 (CARD Act), would ensure that late fees meet the Act's requirement to be "reasonable and proportional" to the costs incurred

ProBank Education Services

powered by

FORVIS

15

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

15



1700 G Street NW, Washington, D.C. 20552

Circular 2022-04

August 11, 2022

Consumer Financial Protection Circular 2022-04

Insufficient data protection or security for sensitive consumer information

August 11, 2022

Question presented

Can entities violate the prohibition on unfair acts or practices in the Consumer Financial Protection Act (CFPA) when they have insufficient data protection or information security?

Summary answer

Yes. In addition to other federal laws governing data security for financial institutions, including the Safeguards Rules issued under the Gramm-Leach-Bliley Act (GLBA), "covered persons" and "service providers" must comply with the prohibition on unfair acts or practices in the CFPA. Inadequate security for the sensitive consumer information collected, processed, maintained, or stored by the company can constitute an unfair practice in violation of 12 U.S.C. 5536(a)(1)(B). While these requirements often overlap, they are not coextensive.

Acts or practices are unfair when they cause or are likely to cause substantial injury that is not reasonably avoidable or outweighed by countervailing benefits to consumers or competition. Inadequate authentication, password management, or software update policies or practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers, and financial institutions are unlikely to successfully justify weak data security practices based on countervailing benefits to consumers or competition. Inadequate data security can be an unfair practice in the absence of a breach or intrusion.

ProBank Education Services

powered by

FORVIS

16

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

16

87 FR 54346 – 54349 (09/07/22)

Consumers cannot reasonably avoid the harms caused by a firm's data security failures. They typically have no way of knowing whether appropriate security measures are properly implemented, irrespective of disclosures provided. They do not control the creation or implementation of an entity's security measures, including an entity's information security program. And consumers lack the practical means to reasonably avoid harms resulting from data security failures.⁶

Where companies forgo reasonable cost-efficient measures to protect consumer data, like those measures identified below, the Consumer Financial Protection Bureau (CFPB) expects the risk of substantial injury to consumers will outweigh any purported countervailing benefits to consumers or competition. The CFPB is unaware of any instance in which a court applying an unfairness standard has found that the substantial injury caused or likely to have been caused by a company's poor data security practices was outweighed by countervailing benefits to consumers or competition.⁷ Given the harms to consumers from breaches involving sensitive financial information, this is not surprising.

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

Home | Site Index | Disclaimer | Privacy Policy | Accessibility

Press Release

For Immediate Release August 11, 2021

FFIEC Issues Guidance on Authentication and Access to Financial Institution Services and Systems

The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members, today issued guidance that provides financial institutions with examples of effective authentication and access risk management principles and practices for customers, employees, and third parties accessing digital banking services and information systems.

The guidance:

- Highlights the current cybersecurity threat environment including increased remote access by customers and users, and attacks that leverage compromised credentials; and mentions the risks arising from push payment capabilities.
- Recognizes the importance of the financial institution's risk assessment to determine appropriate access and authentication practices to determine the wide range of users accessing financial institution systems and services.
- Supports a financial institution's adoption of layered security and underscores weaknesses in single-factor authentication.
- Discusses how multi-factor authentication or controls of equivalent strength can more effectively mitigate risks.
- Includes examples of authentication controls, and a list of government and industry resources and references to assist financial institutions with authentication and access management.

The new guidance replaces previous documents issued in 2005 and 2011.

Attachment:
[FFIEC Authentication and Access to Financial Institution Services and Systems Guidance \(PDF\)](#)



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

OFFICE OF FOREIGN ASSETS CONTROL

SUPPLEMENTAL GUIDANCE FOR THE PROVISION OF HUMANITARIAN ASSISTANCE

February 27, 2023

The Department of the Treasury’s (Treasury) Office of Foreign Assets Control (OFAC) is issuing this 2023 Fact Sheet to provide guidance on the reach of economic sanctions for persons involved in the conduct of humanitarian-related activities, including: the U.S. government (USG); international organizations and entities (IOs); nongovernmental organizations (NGOs); persons involved in the provision of food, other agricultural commodities, medicine, and medical devices (Ag-Med); and financial institutions and other service providers who support or facilitate transactions for such persons.¹

On December 21, 2022, OFAC amended its regulations to [add or revise](#) general licenses (GLs) across a number of OFAC sanctions programs (the “December 2022 GLs”). These new or revised GLs implement United Nations Security Council Resolution (UNSCR) 2664, which created a humanitarian carveout to the asset freeze measures across United Nations’ sanctions regimes. In line with the Treasury’s [2021 Sanctions Review](#), this action reinforces Treasury’s work to limit the unintended impact of sanctions by providing greater consistency and clarity across U.S. sanctions programs to help legitimate humanitarian assistance and related trade reach at-risk populations through transparent financial channels. This 2023 Fact Sheet supplements OFAC’s 2014 [Guidance Related to the Provision of Humanitarian Assistance by Not-for-Profit Non-Governmental Organizations](#) to reflect the December 2022 GLs.

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.



Compliance Communiqué

Guidance on Authorized Transactions Related to Earthquake Relief Efforts in Syria

FEBRUARY 21, 2023

In response to the devastating earthquakes in Syria on February 6, 2023, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) authorized activity supporting emergency earthquake relief efforts in Syria that would otherwise be prohibited by U.S. sanctions in Syria. Specifically, OFAC issued a broad authorization in the form of a general license, General License [\(GL\) 23](#), to authorize for 180 days certain transactions related to earthquake relief efforts that would otherwise be prohibited by the Syrian Sanctions Regulations. This license supplements broad humanitarian authorizations already in effect under the Syrian Sanctions Regulations for nongovernmental organizations (NGOs), international organizations, and the U.S. government that authorize the provision of disaster relief to Syria.

Specifically, GL 23 expands upon existing humanitarian authorizations to enable foreign governments and private companies to provide support to earthquake relief efforts in Syria and provides additional assurances to financial institutions who process such transactions. This guidance responds to specific questions OFAC received related to earthquake relief efforts in Syria and explains how to provide legitimate humanitarian assistance to the Syrian people in compliance with U.S. sanctions. GL 23 reflects the United States’ commitment to support the people of Syria through their ongoing humanitarian crisis—it is not a change in policy toward the Assad regime. While this authorization alone cannot remedy the many challenges of operating and providing aid in Syria, it can ensure that U.S. sanctions do not inhibit relief following the earthquake disaster.

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

OFFICE OF FOREIGN ASSETS CONTROL

Syrian Sanctions Regulations
31 CFR part 542

GENERAL LICENSE NO. 23

Authorizing Transactions Related to Earthquake Relief Efforts in Syria

(a) Except as provided in paragraph (b) of this general license, all transactions related to earthquake relief efforts in Syria that would otherwise be prohibited by the Syrian Sanctions Regulations, 31 CFR part 542 (SySR), are authorized through 12:01 p.m. eastern daylight time, August 8, 2023.

Note 1 to paragraph (a). The authorization in paragraph (a) of this general license includes the processing or transfer of funds on behalf of third-country persons to or from Syria in support of the transactions authorized by paragraph (a) of this general license. U.S. financial institutions and U.S. registered money transmitters may rely on the originator of a funds transfer with regard to compliance with paragraph (a) of this general license, provided that the financial institution does not know or have reason to know that the funds transfer is not in compliance with paragraph (a) of this general license.

(b) This general license does not authorize:

(1) Any transactions prohibited by section 542.208 of the SySR (prohibiting importation into the United States of petroleum or petroleum products of Syrian origin); or

(2) Any transactions involving any person whose property and interests in property are blocked pursuant to the SySR, other than persons who meet the definition of the term *Government of Syria*, as defined in section 542.305(a) of the SySR, unless separately authorized.

Note 2 to General License 23. Nothing in this general license relieves any person from compliance with any other Federal laws or requirements of other Federal agencies.

FDIC

Federal Deposit Insurance Corporation

Joint Agency Release | February 23, 2023

*Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency*

Agencies Issue Joint Statement on Liquidity Risks Resulting from Crypto-Asset Market Vulnerabilities

Federal bank regulatory agencies today issued a joint statement highlighting liquidity risks to banking organizations associated with certain sources of funding from crypto-asset-related entities and some effective practices to manage those risks.

Recent events in the crypto-asset sector have underscored the potential heightened liquidity risks presented by certain sources of funding from crypto-asset-related entities. The joint statement highlights key liquidity risks and some effective practices to monitor and appropriately manage those risks. The statement reminds banking organizations to apply existing risk management principles; it does not create new risk management principles.

Banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation.

Attachment: [Joint Statement on Liquidity Risks to Banking Organizations Resulting From Crypto-Asset Market Vulnerabilities \(PDF\)](#)

February 23, 2023

Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing this statement on the liquidity risks presented by certain sources of funding from crypto-asset¹-related entities, and some effective practices to manage such risks.

The statement reminds banking organizations to apply existing risk management principles; it does not create new risk management principles.² Banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation.

Liquidity Risks Related to Certain Sources of Funding from Crypto-Asset-Related Entities

This statement highlights key liquidity risks associated with crypto-assets and crypto-asset sector participants that banking organizations should be aware of.³ In particular, certain sources of funding from crypto-asset-related entities may pose heightened liquidity risks to banking organizations due to the unpredictability of the scale and timing of deposit inflows and outflows, including, for example:

23

Effective Risk Management Practices

In light of these heightened risks, it is important for banking organizations that use certain sources of funding from crypto-asset-related entities, such as those described above, to actively monitor the liquidity risks inherent in such funding sources and establish and maintain effective risk management and controls commensurate with the level of liquidity risks from such funding sources. Effective practices for these banking organizations could include, for example:

- Understanding the direct and indirect drivers of potential behavior of deposits from crypto-asset-related entities and the extent to which those deposits are susceptible to unpredictable volatility.
- Assessing potential concentration or interconnectedness across deposits from crypto-asset-related entities and the associated liquidity risks.
- Incorporating the liquidity risks or funding volatility associated with crypto-asset-related deposits into contingency funding planning, including liquidity stress testing and, as appropriate, other asset-liability governance and risk management processes.⁵
- Performing robust due diligence and ongoing monitoring of crypto-asset-related entities that establish deposit accounts, including assessing the representations made by those crypto-asset-related entities to their end customers about such deposit accounts that, if inaccurate, could lead to rapid outflows of such deposits.⁶

In addition, banking organizations are required to comply with applicable laws and regulations.

24

Board of Governors of the Federal Reserve System

The Federal Reserve, the central bank of the United States, provides the nation with a safe, flexible, and stable monetary and financial system.

About the Fed

News & Events

Monetary Policy

Supervision & Regulation

Financial Stability

Payment Systems

Economic Research

Home > News & Events > Press Releases

Press Release

March 15, 2023

Federal Reserve announces July launch for the FedNow Service

For release at 5:00 p.m. EDT

Share 

The Service will Debut with Financial Institutions and the U.S. Treasury on Board

CHICAGO – The Federal Reserve announced that the FedNow Service will start operating in July and provided details on preparations for launch.

The first week of April, the Federal Reserve will begin the formal certification of participants for launch of the service. Early adopters will complete a customer testing and certification program, informed by feedback from the FedNow Pilot Program, to prepare for sending live transactions through the system.

Certification encompasses a comprehensive testing curriculum with defined expectations for operational readiness and network experience. In June, the Federal Reserve and certified participants will conduct production validation activities to confirm readiness for the July launch.

ProBank Education Services

powered by

FORVIS

25

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

25

About the Fed

News & Events

Monetary Policy

Supervision & Regulation

Financial Stability

Payment Systems

Economic Research

"We couldn't be more excited about the forthcoming FedNow launch, which will enable every participating financial institution, the smallest to the largest and from all corners of the country, to offer a modern instant payment solution," said Ken Montgomery, first vice president of the Federal Reserve Bank of Boston and FedNow program executive. "With the launch drawing near, we urge financial institutions and their industry partners to move full steam ahead with preparations to join the FedNow Service."

Many early adopters have declared their intent to begin using the service in July, including a diverse mix of financial institutions of all sizes, the largest processors, and the U.S. Treasury.

In addition to preparing early adopters for the July launch, the Federal Reserve continues to engage a range of financial institutions and service providers to complete the testing and certification program and implement the service throughout 2023 and beyond. Montgomery noted that availability of the service is just the beginning, and growing the network of participating financial institutions will be key to increasing the availability of instant payments for consumers and businesses across the country.

The FedNow Service will launch with a robust set of core clearing and settlement functionality and value-added features. More features and enhancements will be added in future releases to continue supporting safety, resiliency and innovation in the industry as the FedNow network expands in the coming years.

"With the FedNow Service, the Federal Reserve is creating a leading-edge payments system that is resilient, adaptive, and accessible," said Tom Barkin, president of the Federal Reserve Bank of Richmond and FedNow Program executive sponsor. "The launch reflects an important milestone in the journey to help financial institutions serve customer needs for instant payments to better support nearly every aspect of our economy."

About the FedNow Service

The Federal Reserve Banks are developing the FedNow Service to facilitate nationwide reach of instant payment services by financial institutions — regardless of size or geographic location — around the clock, every day of the year. Through financial institutions participating in the FedNow Service, businesses and individuals will be able to send and receive instant payments at any time of day, and recipients will have full access to funds immediately, giving them greater flexibility to manage their money and make time-sensitive payments. Access will be provided through the Federal Reserve's FedLine® network, which serves more than 10,000 financial institutions directly or through their agents. For more information, visit [FedNowExplorer.org](https://www.fednowexplorer.org).

ProBank Education Services

powered by

FORVIS

26

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

26

FedNow^{24/7} INSTANT PAYMENTS™

You are a major part of the ecosystem

The FedNow^{24/7} Service will provide an instant payment platform that financial institutions and other organizations can use to build innovative payment solutions for businesses and consumers. But it will take more than the launch of the service for instant payments to go mainstream. The entire payments ecosystem must work together to create products that deliver the speed and convenience of instant payments throughout the United States.



Where do you fit in?

You may play more than one role.
For example, a payment processor that helps financial institutions connect to the FedNow Service may also provide instant bill presentation services to business end-user clients and may itself be a business end user that would benefit from instant payroll.

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

6 PHASES of the FedNow Service journey

Financial institutions go through several phases to prepare for and ultimately go live with the FedNow^{24/7} Service. While each organization's path to instant payments is unique, this document shows key activities and decisions many take along the way. At each step of your journey, Federal Reserve **relationship managers** are available to assist.



	LEARN	ENGAGE	PREPARE	COMMIT	ONBOARD	GO LIVE
Overview	Learn about instant payments and the FedNow Service	Dig deeper into how instant payments can impact your organization and customers	Start preparing for instant payments and assess your organization's readiness	Decide to adopt the FedNow Service and get ready to onboard	Sign up for the FedNow Service and go through onboarding	Be ready to send and/or receive transactions
Activities and Decision Points	<ul style="list-style-type: none"> Explore educational resources on FedNowExplorer.org Sign up for FedNow News Hear from FedNow Service speakers at industry conferences 	<ul style="list-style-type: none"> Join the FedNow Community Consider instant payment products and services you might offer that clear and settle through the FedNow Service Mobilize a cross-functional internal team to prepare for instant payments, assess readiness and define roles 	<ul style="list-style-type: none"> Review readiness guides and information Contact your Federal Reserve relationship manager to take an assessment Get buy-in from internal team and determine lead times to get ready for instant payments Talk to service providers and vendors Attend FedNow events 	<ul style="list-style-type: none"> Develop a project plan with your assigned onboarding manager Identify core payment systems that will connect to the service Ensure your organization can handle real-time posting and make funds available immediately Determine how you will settle transactions 	<ul style="list-style-type: none"> Discuss your project plan with your assigned onboarding manager Review and sign OC 8 agreements Answer onboarding questions about how you'll connect to the service and settle transactions Gather information Establish connectivity Access and test 	<ul style="list-style-type: none"> Validate production profile Schedule go-live date Publicly announce you're now offering instant payments Enjoy the benefits instant payments bring to you and your customers
Resources	FedNowExplorer.org <ul style="list-style-type: none"> Instant Payments University Welcome Plaza Upcoming Conferences FedNow News Sign Up 	FedNowExplorer.org <ul style="list-style-type: none"> Use Case Arena Preplanning Roadmap Community Sign Up 	FedNowExplorer.org <ul style="list-style-type: none"> Service Readiness Guide Planning Office ISO[®] Education Service Provider Showcase 	FedNowExplorer.org <ul style="list-style-type: none"> Connectivity at a Glance Connectivity Guide FRBServices.org <ul style="list-style-type: none"> Operating Procedures Operating Circular 8 [OC 8] MyStandards <ul style="list-style-type: none"> ISO Specifications and Guides on MyStandards 	Onboarding Tool and Guided Onboarding <ul style="list-style-type: none"> FedNow participants get access to the Onboarding Tool and work with an onboarding manager Early Adopter Hub <ul style="list-style-type: none"> Onboarding and testing resources Technical specifications Recorded webinars 	FRB Services Support Center <ul style="list-style-type: none"> 1-833-FRS-SVCS (377-7827)

For even more resources and information, visit FedNowExplorer.org.

THE FEDERAL RESERVE

The Federal Reserve Financial Services logo, "FedNow," and "FRBServices.org" are service marks of the Federal Reserve Banks. A list of marks related to financial services offered by the Federal Reserve Banks is available at FRBServices.org. "ISO" is a registered service mark of the International Organization for Standardization. © 2023 Federal Reserve Banks.

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

THE **FEDERAL RESERVE**
#Financial Services

FedNowSM
INSTANT PAYMENTS

*The FedNowSM Service
Readiness Guide*
Version: 2/14/23

ProBank Education Services *powered by* **FORVIS**

29

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

29

THE **FEDERAL RESERVE**
#Financial Services

**FedNowSM Service
Operating Procedures**

March 3, 2023
Version 1.2

FedNowSM
INSTANT PAYMENTS

ProBank Education Services *powered by* **FORVIS**

30

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

30

Federal Reserve Banks
Operating Circular No. 8
FUNDS TRANSFERS THROUGH THE FEDNOWSM SERVICE
Effective September 21, 2022

Operating Circular No. 8
Effective September 21, 2022

ProBank Education Services

powered by

FORVIS

31

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

31

Modifications to PSR – 87 FR 75254 – 75267 – 12/08/22

FEDERAL RESERVE SYSTEM [Docket No. OP-1749]

Improvements to the Federal Reserve Policy on Payment System Risk To Increase Access to Intraday Credit, Support the FedNow Service, and Simplify the Federal Reserve Policy on Overnight Overdrafts

AGENCY: Board of Governors of the Federal Reserve System.
ACTION: Notice.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) is adopting changes to part II of the Federal Reserve Policy on Payment System Risk (PSR policy) substantially

as proposed. The changes expand the eligibility of depository institutions to request collateralized intraday credit from the Federal Reserve Banks (Reserve Banks) while reducing administrative steps for requesting collateralized intraday credit. In addition, the Board is adopting changes to the PSR policy that clarify the eligibility standards for accessing uncollateralized intraday credit from Reserve Banks and modify the impact of a holding company's or affiliate's supervisory rating on an institution's eligibility to request uncollateralized intraday credit capacity. The Board is also adopting changes to part II of the PSR policy to support the deployment of the FedNowSM Service (FedNow Service). Finally, the Board is simplifying the Federal Reserve Policy on Overnight Overdrafts (Overnight Overdrafts policy) and incorporating into the PSR policy as part III.

DATES: The FedNow Service-related changes to the PSR policy and the changes related to the Overnight Overdrafts policy will become effective when Reserve Banks begin processing live transactions for FedNow Service participants (expected in 2023). The exact date will be announced on the Board's website. The remaining changes to part II of the PSR policy will become effective February 6, 2023.

ProBank Education Services

powered by

FORVIS

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

32



- Fed360 Home
- Dates to Remember
- In Case You Missed It ▾
- In This Issue ▾
- Article Archives
- Email Notifications
- Email the Editor
- Print ▾
- Share ▾



Reminder: VPN device migration is in progress

FEDLINE SOLUTIONS | March 15, 2023 |

In June 2022, the [Federal Reserve Banks began the Virtual Private Network \(VPN\) Device Migration project](#). The migration requires FedLine Advantage®, FedLine Command® and FedLine Direct® customers to replace their current VPN devices with a more contemporary solution. Specifically, impacted organizations will move from the current Fortinet® FortiGate® 61E model to a Cisco® C1111 model. These changes will improve resiliency and enable access to the FedNowSM Service.

When your VPN device is due for migration, we will instruct an end user authorization contact (EUAC) from your organization to facilitate the migration order, via the Connection Management Center (CMC) within FedLine® Home, in your designated timeframe.

As previously communicated, the Cisco C1111 model **does not allow** for multiple Cisco VPN devices to be connected to FedLine concurrently using the same public IP address. Each Cisco C1111 VPN connection must source from a unique public IP address. If your existing Fortinet VPN devices use the same public IP address, please work with your technical staff and Internet Service Provider (ISP) to set up unique public IP addresses for each new Cisco C1111 device before your VPN device installation date.

We appreciate your organization's willingness to help us maintain reliable and secure access to Federal Reserve Bank Services. Review the [VPN Device Migration Frequently Asked Questions](#) for more information.

Note

"Fortinet" and "FortiGate" are trademarks of Fortinet, Inc.

"Cisco" is a trademark of Cisco Systems, Inc.

FedLine Solutions Resources

FedLine Solutions Resources Home

End User Authorization Contact (EUAC) Support Page for FedLine Web® and FedLine Advantage® EUACs

FedLine Command® Environment and Configuration Change Matrix

FedLine Direct® File Environment and Configuration Change Matrix

FedLine Direct® Message Environment and Configuration Change Matrix

Frequently Asked Questions ▾

VPN Device Migration Frequently Asked Questions

Overview

As part of the Federal Reserve Banks' ongoing efforts to keep pace with evolving industry and customer needs, we have begun the Virtual Private Network (VPN) Device Migration. The migration effort requires all FedLine Advantage® and FedLine Command® customers to replace their current VPN devices with a more contemporary solution. These changes will improve resiliency and enable access to the FedNowSM Service. We are sharing the following information with your organization's End User Authorization Contacts (EUACs) and senior leaders, so you know what to expect for this project.

The setup for the new VPN device will be similar to the setup for the current device and will require changes to your network/firewall settings. Your organization will continue to utilize the Connection Management Center (CMC) to move from the current Fortinet® FortiGate® 61E model to a Cisco® C1111 model. Additionally, device provisioning will move from Sprint® (now T-Mobile®) to a new vendor.

Available via FedLine® Home, the CMC is the Federal Reserve Banks' web-based application that FedLine Advantage EUACs use to place VPN device orders. Please note that a credentialed Technical Contact at your organization can also assist with completing the migration order in the CMC; however, an EUAC must start the order and submit it.

ProBank Education Services

powered by

FORVIS

35

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

35



Action required: Get started on the FedLine® Solutions Security and Resiliency Assurance Program

FEDLINE SOLUTIONS | February 15, 2023 |  

ProBank Education Services

powered by

FORVIS

36

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

36

Your organization is required to complete the FedLine Solutions Security and Resiliency Assurance Program by Dec. 31, 2023. **Attestation materials were recently distributed to all End User Authorization Contacts (EUACs) at impacted organizations.**

If you *did not* receive your materials...

- Please check your junk/spam folders for an email from @adobesign.com.
- Add the @adobesign.com domain to your safe senders list to improve future deliverability.

If you *did* receive your materials...

- Review the quick start guide that is included as part of your organization's attestation packet.
- Identify a primary point of contact to facilitate the Assurance Program process on behalf of your organization.
- Share the attestation materials with your point of contact.

Support and resources

Visit the [resource center](#) for additional assistance. The resource center is designed to be a central hub for key information and supporting materials, including a list of more than 40 [frequently asked questions \(FAQs\)](#).

We appreciate your support and look forward to working with you on this important program.

ProBank Education Services *powered by* **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

3.1 Self-assessment Requirements

Each Institution must at all times comply with the measures, protections and requirements established under the Reserve Bank Program described in Section 1.1 of this Appendix A, the Institution Program described in Section 1.2 of this Appendix A, and any applicable Security Procedures (collectively, the "Security Requirements").

Each Institution and, if applicable, any Service Provider, shall at least annually conduct a self-assessment of its compliance with the Security Requirements ("Self-Assessment"). The Self-Assessment may be calibrated based on an Institution's analysis of the risks it faces. However, the Reserve Banks may in their discretion require that the Self-Assessment be conducted or reviewed by an independent third party, an internal audit function, or an internal compliance function.

3.2 Attestation Requirements

Upon the request of the Reserve Banks which shall not exceed more than once during any consecutive 12-month period, each Institution and, if applicable, any Service Provider, shall attest to having completed a Self-Assessment by submitting an attestation in a form and manner acceptable to the Reserve Banks ("Attestation"). The Attestation sought by the Reserve Banks will generally include the following:

- (i) An acknowledgment of the Institution's responsibility to adhere to the Security Requirements;
- (ii) A confirmation that the Institution has conducted a Self-Assessment within the time period requested by the Reserve Banks;
- (iii) If available, a confirmation that the Self-Assessment was either (i) conducted by an independent third party, (ii) conducted by an independent internal function such as internal audit or compliance, or (iii) to the extent the Self-Assessment was conducted by a non-independent party or function, an independent third party reviewed the work conducted in connection with the Self-Assessment to establish that it was designed and conducted in a manner reasonable sufficient to identify any material noncompliance with the Security Requirements;
- (iv) If available, an acknowledgment that the Institution is responsible for its Service Provider's compliance with the Security Requirements;
- (v) A statement that the Institution has remediation plans in place, including procedures to escalate concerns to the appropriate leaders within the Institution, to promptly address any areas of noncompliance with the Security Requirements; and

Operating Circular No. 5
Effective October 15, 2020

21

ProBank Education Services *powered by* **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

Stay Connected Recent Postings Calendar Publications Site Map A-Z index Careers FAQs Videos Contact Search Advanced

Board of Governors of the Federal Reserve System

The Federal Reserve, the central bank of the United States, provides the nation with a safe, flexible, and stable monetary and financial system.

About the Fed News & Events Monetary Policy Supervision & Regulation Financial Stability Payment Systems Economic Research Data Consumers & Communities

Home > News & Events > Press Releases

Press Release

January 24, 2023

Federal Reserve Board announces it has fined Popular Bank \$2.3 million for processing six Paycheck Protection Program (PPP) loans despite having detected that the loan applications contained significant indications of potential fraud

For release at 11:00 a.m. EST

Share

The Federal Reserve Board on Tuesday announced that it has fined Popular Bank, of New York, New York, \$2.3 million for processing six Paycheck Protection Program (PPP) loans despite having detected that the loan applications contained significant indications of potential fraud and for failing to report the potential fraud in a timely manner. The six loans totaled approximately \$1.1 million.

Under the Coronavirus Aid, Relief, and Economic Security (CARES) Act, Small Business Administration-approved lenders like Popular Bank were allowed to provide PPP loans to qualified small businesses negatively impacted by the COVID-19 pandemic, but were required to follow their anti-money laundering policies. Popular Bank's processing of potentially fraudulent PPP loans and failure to report the potential fraud in a timely manner violated these policies and constituted unsafe or unsound banking practices.

For media inquiries, please email media@frb.gov or call 202-452-2955.

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

39

39



Green Book Chapter 5 Reclamations Update

Wednesday, February 15, 2023

Effective March 1, 2023, the Bureau of the Fiscal Service (Fiscal Service) will no longer accept paper Automated Clearinghouse (ACH) reclamation responses. All responses, with the exception of those ACH reclamations initiated by Defense Finance & Accounting Services (DFAS) and any Treasury-approved exceptions, must be submitted through the Automated Reclamation Processing System (ARPS), located in PAY.gov. This updated requirement is outlined within the [Green Book - Chapter 5: Reclamations](#). If a response is returned to Fiscal Service by U.S. Mail, fax or email, it will be rejected and the financial institution will be liable for any debits associated with that reclamation, due to an untimely response.

As a reminder, by accepting a recurring benefit payment from the government, a Receiving Depository Financial Institution (RDFI) agrees to the provisions of 31 CFR part 210, including the reclamation and debiting of the RDFI's Federal Reserve Bank (FRB) master account for any reclamation for which it is liable. The RDFI also agrees to the liability provisions of the federal reclamation regulations found in 31 CFR part 210, subpart B, and affirms this agreement each time the RDFI accepts and credits an ACH payment on behalf of a depositor. Federal reclamation procedures are outlined in the [Green Book - Chapter 5: Reclamations](#).

If you have any questions about the requirement to use ARPS, please email PFC-Reclamations@fiscal.treasury.gov.

Exceptions: Any exceptions to use of ARPS must be approved on a case-by-case basis by Fiscal Service. Exception requests may be sent to PFC-Reclamations@fiscal.treasury.gov.

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

40

40

Automated Reclamation Processing System (ARPS):

The Bureau of Fiscal Service has developed an electronic version of the current FS-133 process. This process allows financial institutions to submit a response to the Notice of Reclamation (NOR) electronically through the Department of the Treasury's Pay.gov web portal.

How to electronically respond to an ACH Reclamation:

Electronic responses should be made through [Pay.gov](https://www.pay.gov), a web-based application operated by the Department of the Treasury that allows users to submit responses to a Notice of Reclamation. It also allows the Financial Institution to make payments to government agencies by electronic means by authorizing a debit.

1. When the FMS 133, Notice of Reclamation is received, the financial institution will continue to follow its current procedures as stated in the Green Book (Chapter 5, Section 3, Reclamation Procedures)
2. Once the FI is prepared to respond to the Notice of Reclamation; this response will be submitted through the Pay.Gov web portal. This electronic version of the form requires the same information as the paper version.
3. Responding through Pay.gov allows the financial institution to limit liability as well submit full or partial payment(s) via a debit authorization.

Incomplete or Inadequate RDFI Replies

If the RDFI's response is inadequate, the government will send the RDFI a rejection via email, indicating the reason for the disapproval. If no adequate response is received from the RDFI within the allotted timeframe, the government will initiate a debit action for the outstanding amount.

SBA Borrowers: View loan information or make a payment at the [new MySBA site](#).
Dismiss

Pay.gov
Sign In | Create an Account

Browse Payments | See All Agencies | Help | About Us

Information Status
You are signed out

The secure way to pay U.S. Federal Government Agencies

Department of Veterans Affairs
Make a VA Medical Care Copayment
Did you receive a medical bill statement from the U.S. Department of Veterans Affairs?
[Pay it right here](#)

Small Business Administration
Make a SBA 1201 Borrower Payment
Did you receive a payment notice (Form 1201) from the Small Business Administration?
[Pay it right here](#)

Social Security Administration
Repay your Social Security Overpayment
Did you receive an overpayment notice from the Social Security Administration?
[Pay it right here](#)

ProBank Education Services powered by **FORVIS**

SBA Borrowers: View loan information or make a payment at the [new MySBA site](#). [Dismiss](#)

Welcome, mdeverky600 | [My Account](#) | [Sign Out](#)

Pay.gov Fiscal Service Form 133 NOI

[Browse Payments](#) [See All Agencies](#) [Help](#) [About Us](#)

The secure way to pay U.S. Federal Government Agencies

Welcome mdeverky600!

Use the search bar to find a form or scroll down to see our most popular payments and topics! If you would like to see your account information, click the button below.

[Go to My Account](#)

In the My Account Section you can:

- See your Payment Activity
- Use an Access Code
- Update your Password
- Manage Payment Methods and more...

Department of Veterans Affairs
Make a VA Medical Care Copayment
 Did you receive a medical bill statement from the U.S. Department of Veterans Affairs?
[Pay it right here.](#)

Small Business Administration
Make a SBA 1201 Borrower Payment
 Did you receive a payment notice (Form 1201) from the Small Business Administration?
[Pay it right here.](#)

Social Security Administration
Repay your Social Security Overpayment
 Did you receive an overpayment notice from the Social Security Administration?
[Pay it right here.](#)

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

43

43

SBA Borrowers: View loan information or make a payment at the [new MySBA site](#). [Dismiss](#)

Welcome, mdeverky600 | [My Account](#) | [Sign Out](#)

Pay.gov Fiscal Service Form 133 NOI

[Browse Payments](#) [See All Agencies](#) [Help](#) [About Us](#)

Search Results for "Fiscal Service Form 133 NOR"

Forms (978) Agencies (126)

Sort by: Relevance

Fiscal Service Form 133 Notice of Reclamation (NOR)

Description: For Financial Institution Use
Form Number: NOR Form 133
Agency: [Bureau of the Fiscal Service \(BFS\)](#)

[Continue](#)

Bureau of the Fiscal Service - Accounts Receivable

Description: Please use this form to enter a payment for U.S. Savings Bonds or other Treasury security debt. The debt is the result of an overpayment or double payment to you. If you have questions, please contact the Bureau of the Fiscal Service at 304-480-6592.
Form Number: Fiscal Service Accounts Receivable
Agency: [Treasury \(UST\); Bureau of the Fiscal Service; Treasury Securities Services](#)

We're here to help!

- We're Available**
Monday - Friday
8 am - 7 pm Eastern
[Open](#)
- [Send Us A Message](#)
We are experiencing extremely high email and call volume. We will respond to your inquiry as soon as we are able. Thank you for your patience and understanding.
- Call Us Toll Free**
Inside U.S.A. only
800-624-1373
- International Number**
Outside the U.S.A.
+1-216-579-2112

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

44

44

SBA Borrowers: View loan information or make a payment at the [new MySBA site](#)

Dismiss

Welcome, mdeverky600 | My Account | Sign Out

Pay.gov Fiscal Service Form 133 NOX

Browse Payments See All Agencies Help About Us

Fiscal Service Form 133 Notice of Reclamation (NOR)

- 1 Before You Begin
- 2 Complete Agency Form
- 3 Enter Email & Submit
- 4 Confirmation

About this form
For Financial Institution Use

[Preview Form](#) [Cancel](#) [Continue to the Form](#)

This is a secure service provided by United States Department of the Treasury. The information you will enter will remain private. [Please review our privacy policy](#) for more information.

We're here to help! +

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

45

45

FISCAL SERVICE Form 133 Notice of Reclamation (NOR)
(For Financial Institution Use)

1. Enter Reclamation Ticket Number: **1a. Reenter Reclamation Ticket Number:**

2. Total Reclamation Amount: **2a. Debit Authorization Amount:**
(Use "Outstanding Total" from the Notice of Reclamation) (Equal to or less than amount for #2)

IF LESS THAN THE OUTSTANDING TOTAL IS BEING PAID, PROVIDE THE NAMES AND ADDRESSES OF THE ACCOUNT OWNER AND/OR LAST WITHDRAWER ON QUESTION #6.

3. Recipient/beneficiary did not die.

4. Date of death is wrong (If box is checked, provide correct date of death from death certificate.)
Correct Date of Death: (MM/DD/YYYY)

5. Protesting Notice of Reclamation under the 120-Day rule. (If box is checked, it is optional to provide additional notes on question #8.)

6. Provide Account Owner Information and/or Last Withdrawer:

Last Name: First Name:
Address of Last Account Withdrawer
Street Address: Apt. Number:
City Name: State: Zip/Postal Code:
Country:

7. Sole Owner: Yes No (IF NO, PROVIDE ACCOUNT CO-OWNER INFORMATION)

Account Co-Owner Information:
Last Name: First Name:
Street Address: Apt. Number:
City Name: State: Zip/Postal Code:
Country:

8. Notes: (500 Character Limit)

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

46

46



***9. CERTIFICATION NO. 1:**

This certifies that the Notice to Account Owners form was mailed to the owners of the account at the addresses on the records of this financial institution on:

Date: (MM/DD/YYYY)

If a correction has been made to the fact or date of death, this certifies that the date of death entered above is correct and that this financial institution took prudent measures to assure that the person is alive or that the date of death was erroneous.

Digital Signature of FI Representative Completing this Form and CERTIFICATION NO. 1:

DATE SIGNATURE

***10. CERTIFICATION NO. 2:**

In accordance with 31 CFR 210, this certifies that this financial institution received the Notice of Reclamation on:

Date: (MM/DD/YYYY)

And this financial institution first learned of the death on:

Date: (MM/DD/YYYY)

The financial institution had no knowledge of the death or legal incapacity of the recipient or death of the beneficiary at the time any of the payments listed were credited to or withdrawn from the account. An amount equal to the amount remaining in the account, including any additions to the account balance since the receipt of this notice, has been paid to the Government.

Digital Signature of FI Representative Completing this Form and CERTIFICATION NO. 2:

DATE SIGNATURE

***11. Name, Title and Phone Number of FI Representative Completing THIS Form and CERTIFICATION NO. 1 & 2 and Date Completed:**

Last Name: First Name:

Title: Phone Number:

Date: (MM/DD/YYYY)

<https://fedpaymentsimprovement.org/synthetic-identity-fraud-mitigation-toolkit/>

THE FEDERAL RESERVE
Payments Improvement

About | The Community | Strategic Initiatives | News | Resources

Synthetic Identity Fraud Mitigation Toolkit

Synthetic identity fraud is a real problem facing the payments industry and other types of businesses. Furthermore, feedback from the Federal Reserve's ongoing engagement with payments fraud experts and a June 2021 survey reinforces the need for synthetic identity fraud awareness and dialogue about detection and mitigation strategies.

The Fed supports the payments industry in combating synthetic identity fraud by encouraging education, understanding and broad industry collaboration. This fraud mitigation toolkit offers a wide variety of informative resources for financial institutions, businesses and individuals. Through future phases of the toolkit, new resources will be added over time, including in the areas of synthetic identity fraud detection and mitigation.

Why is it Important to Know About Synthetic Identity Fraud?

In the continued progress toward a vision of faster, safer and more efficient payments in the United States, synthetic identity fraud is a high priority for the payments industry and broader U.S. economy because:

- Accounts for substantial financial loss
 - Often miscategorized as a credit loss, accounting for an estimated \$20 billion in losses (Off-site) for U.S. financial institutions in 2020.

Synthetic Identity Fraud Mitigation Toolkit

- Toolkit Module 1: Synthetic Identity Fraud: The Basics
- Toolkit Module 2: How Synthetic Identities Are Used
- Toolkit Module 3: When Synthetics Become a Reality
- Toolkit Module 4: Detecting a Synthetic Identity
- Toolkit Module 5: Validating Identities
- Toolkit Module 6: Identifying Synthetics
- Toolkit Module 7: Technology Enhances Fraud Detection
- Toolkit Module 8: Fraud Data Strategy and Information Sharing
- Toolkit Module 9: Fraud Mitigation Service Providers

ProBank Educ

“In speaking with financial institutions and other payments experts about synthetic identity fraud for a number of years, questions have escalated from ‘What is it?’ and ‘How can I detect it?’ to ‘What can I do about it?’ The Federal Reserve has expanded its Synthetic Identity Fraud Mitigation Toolkit to enhance awareness and understanding of synthetic identity fraud – and to help people and organizations reduce the time they spend to locate service providers and their mitigation offerings for this type of fraud.”

Mike Timoney, vice president of payments improvement

Federal Reserve Financial Services

49

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

49

The latest addition to the toolkit, [Module 9: Fraud Mitigation Service Providers](#), offers a list of synthetic identity fraud mitigation service providers in alphabetical order. Each listing includes the name(s) of the provider's synthetic identity fraud detection and prevention offering(s), a brief description and links to the organization's website and a contact. The Federal Reserve expects to periodically update this list with additional service provider submissions that meet the criteria for inclusion.

Explore the [list of providers](#) and the [full Synthetic Identity Fraud Mitigation Toolkit](#) for insights and downloadable resources on addressing this type of fraud.

Federal Reserve Financial Services (FRFS) is merely the host for the information and providers listed in Module 9 and takes no responsibility for the content or accuracy of any information presented. FRFS does not support or endorse any providers, and the inclusion or exclusion of a provider should in no way imply any recommendation or endorsement by FRFS. None of the providers supplying information in the list have any special or exclusive relationship with FRFS, and no relationship should be implied. For more information, see the [Service Providers Call for Participation](#) and [Rules for Participation](#).

#50

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

50

NATIONAL DEFENSE AUTHORIZATION ACT for FY 2021 // P.L. 116-283

- 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.



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 – “covered” entities (small - < 20 Full-time employees, < \$ 5 Million in Gross Revenue, & operating at a physical office in the USA) will provide Beneficial Ownership information to FinCEN during the process of formation or registration of the company – how this impacts DFIs is unclear until “modification” regulations to Beneficial Ownership requirements are promulgated by Treasury – **Final BOIR Rule Issued 09/30/22**
 - Address inefficiencies in SAR and CTR filing – process, forms and dollar reporting limits;

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.

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

- Greater government resources to address money laundering – FinCEN to establish domestic liaisons as 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



HOME ABOUT ▾ RESOURCES ▾ NEWSROOM ▾ CAREERS ▾ ADVISORIES GLOSSARY

Search

FBAR Due Date FinCEN Combats Ransomware AML Act of 2020 Information COVID-19 Information

Learn more about the Beneficial Ownership Information Reporting Rule – Effective January 1, 2024



FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail

February 27, 2023

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) is issuing an alert to financial institutions on the nationwide surge in check fraud schemes targeting the U.S. Mail. Fraud, including check fraud, is the largest source of illicit proceeds in the United States and is one of the anti-money laundering/countering the financing of terrorism (AML/CFT) National Priorities.

Financial Action Task Force Suspends the Membership of the Russian Federation, and Identifies Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies

March 09, 2023

FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies

January 25, 2023

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)

- Trends in Bank Secrecy Act Data: Financial Activity by Russian Oligarchs in 2022 (December 22, 2022)
- Report on Ransomware Trends in Bank Secrecy Act Data between July 2021-December 2021 (November 1, 2022)
- 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 3, 2022)
- Advance Notice of Proposed Rulemaking (ANPRM) (June 3, 2022)
- News Release (June 30, 2021)
- Report (June 28, 2021)

Corporate Transparency Act || Beneficial Ownership (AML Act Title LXIV (Sections 6401-6403))

- Access and Safeguards Notice of Proposed Rulemaking (NPRM) (December 15, 2022)
- Access and Safeguards NPRM News Release (December 15, 2022)
- Access and Safeguards NPRM Fact Sheet (December 15, 2022)

Reporting Final Rule (September 30, 2022)

- Reporting Final Rule News Release (September 29, 2022)
- Reporting Final Rule Fact Sheet (September 29, 2022)

FinCEN Statement Regarding Beneficial Ownership Information Reporting and Next Steps (February 8, 2022)

- Reporting Notice of Proposed Rulemaking (NPRM) (December 8, 2021)
- Reporting NPRM News Release (December 7, 2021)
- Reporting NPRM Fact Sheet (December 7, 2021)

Reporting Advance Notice of Proposed Rulemaking (ANPRM) (April 5, 2021)

- Reporting ANPRM News Release (April 1, 2021)

Rule Effective January 1, 2024



Beneficial Ownership Information Reporting

ProBank Educ

57

57

Rule Effective January 1, 2024



Beneficial Ownership Information Reporting

A final rule implementing the beneficial ownership information reporting requirements of the Corporate Transparency Act (CTA) was issued in September 2022. These regulations go into effect on January 1, 2024. Beneficial ownership information will not be accepted prior to January 1, 2024.

The Corporate Transparency Act (CTA) establishes uniform 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 CTA authorizes FinCEN to collect that information and disclose it to authorized government authorities and financial institutions, subject to effective safeguards and controls. The CTA and its implementing regulations will provide essential information to law enforcement, national security agencies, and others to help prevent criminals, terrorists, proliferators, and corrupt oligarchs from hiding illicit money or other property in the United States. The CTA is part of the Anti-Money Laundering Act of 2020 (AML Act). More information on the AML Act can be found on the [AML Act page](#).

Beneficial Ownership Information Reporting Requirements

Final Rule (September 30, 2022)
Final Rule News Release (September 29, 2022)
Final Rule Fact Sheet (September 29, 2022)

Beneficial Ownership Information Access and Safeguards

Notice of Proposed Rulemaking (NPRM) (December 15, 2022)
NPRM News Release (December 15, 2022)
NPRM Fact Sheet (December 15, 2022)

Beneficial Ownership Information Collections

Proposed Collection for Beneficial Ownership Information Reports (January 17, 2023)
Proposed Collection for Individual FinCEN Identifiers (January 17, 2023)

ProBank Education Services

powered by

FORVIS

58

58

Beneficial Ownership Information Reporting - Requirements – Final Rule 09/30/22 – 87 FR 59498-59596

- FinCEN has issued the Final Rule requiring certain entities to file with FinCEN, reports that identify two categories (not ingredients within, but categories) of individuals: the beneficial owners of the entity, and individuals who have filed an application with specified governmental authorities to create the entity or register the entity to do business.
- These regulations implement Section 6403 of the Corporate Transparency Act and describe who must file a report, what information must be provided, and when a report is due.
- These Rules are effective: January 01, 2024

Beneficial Ownership Information Reporting Rule Fact Sheet

Reporting Companies

- The rule identifies two types of **reporting companies**: domestic and foreign. A domestic reporting company is a corporation, limited liability company (LLC), or any entity created by the filing of a document with a secretary of state or any similar office under the law of a state or Indian tribe. A foreign reporting company is a corporation, LLC, or other entity formed under the law of a foreign country that is registered to do business in any state or tribal jurisdiction by the filing of a document with a secretary of state or any similar office. Under the rule, and in keeping with the CTA, twenty-three types of entities are exempt from the definition of "reporting company."
- FinCEN expects that these definitions mean that reporting companies will include (subject to the applicability of specific exemptions) limited liability partnerships, limited liability limited partnerships, business trusts, and most limited partnerships, in addition to corporations and LLCs, because such entities are generally created by a filing with a secretary of state or similar office.
- Other types of legal entities, including certain trusts, are 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 in many states the creation of most trusts typically does not involve the filing of such a formation document.

Notable “Differences” in Exemptions

- Large Operating Companies – defined as any entity that:
 - Employees more than 20 full-time employees in the United States;
 - Has an operating presence at a physical office in the United States; and
 - Filed an income tax or information return for the previous year demonstrating > \$5,000,000 in gross receipts or sales as reported on IRS Form 1120, excluding gross receipts or sales from sources outside the United States as determined under federal income tax principles.

Notable “Differences” in Exemptions (cont.)

- Subsidiaries of certain exempt entities – any entity whose ownership interests are controlled or wholly owned directly or indirectly by a large operating company, and other entities described in the Final Rule;
- Inactive Entity – Any entity that was in existence on or before 01/01/20; is not engaged in active business; is not owned by a foreign person, whether directly or indirectly, wholly or partially; has not experienced any change in ownership in the preceding twelve month period; has not sent or received any funds in an amount greater than \$1,000, either directly or through and financial account in which the entity or any affiliate of the entity had an interest, in the preceding twelve month period; and does not otherwise hold any kind or type of assets, whether in the United States or abroad, including any ownership interests in any corporation, LLC, or other similar entity.

Notable “Differences” in Exemptions (cont.)

- Tax-Exempt Entities (e.g., 501(c), and 527(e)(1)) – political organizations organized and operated primarily for the purpose of accepting contributions or making expenditures to influence elections at federal, state, and/or local level, and 4947(a) – a trust described in paragraph one or two of this section);
- Entity assisting a tax-exempt entity – any entity that operates exclusively to provide financial assistance to, or hold governance rights over a tax-exempt entity;
- Money Services Businesses who ARE registered with FinCEN;
- Public Utility.

ProBank Education Services powered by **FORVIS**

63

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

63

“Similarities” in Exemptions

- An issuer of securities registered under Section 12 of the SEC Act of 1934;
- Governmental Authority;
- Bank;
- Credit Union;
- Depository Institution holding company;
- Securities exchange or clearing agency;
- Investment Company or investment advisor;
- Venture capital fund advisor;

ProBank Education Services powered by **FORVIS**

64

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

64

“Similarities” in Exemptions (cont.)

- Insurance Company;
- Commodity Exchange Act registered entity;
- Public accounting firm registered in accordance with Section 102 of Sarbanes-Oxley Act of 2002;
- Financial Market Utility designated by the Financial Stability Oversight Council; and
- Pooled investment vehicle operated or advised by a financial institution regulated by a federal functional regulator

Beneficial Ownership Information Reporting Rule Fact Sheet

Reporting Companies

- The rule identifies two types of **reporting companies**: domestic and foreign. A domestic reporting company is a corporation, limited liability company (LLC), or any entity created by the filing of a document with a secretary of state or any similar office under the law of a state or Indian tribe. A foreign reporting company is a corporation, LLC, or other entity formed under the law of a foreign country that is registered to do business in any state or tribal jurisdiction by the filing of a document with a secretary of state or any similar office. Under the rule, and in keeping with the CTA, twenty-three types of entities are exempt from the definition of “reporting company.”
- FinCEN expects that these definitions mean that reporting companies will include (subject to the applicability of specific exemptions) limited liability partnerships, limited liability limited partnerships, business trusts, and most limited partnerships, in addition to corporations and LLCs, because such entities are generally created by a filing with a secretary of state or similar office.
- Other types of legal entities, including certain trusts, are 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 in many states the creation of most trusts typically does not involve the filing of such a formation document.

Sole Proprietor “Exemption” ?? – 87 FR 59537

The CTA itself provides a reasonably clear principle to apply to the variety of specific scenarios, *i.e.*, that a domestic reporting company is an entity created by the filing of a document with a secretary of state or other similar office. In general, FinCEN believes that sole proprietorships, certain types of trusts, and general partnerships in many, if not most, circumstances are not created through the filing of a document with a secretary of state or similar office. In such cases, the sole proprietorship, trust, or general partnership would not be a reporting company under the final rule. Moreover, where such an entity registers for a business license or similar permit, FinCEN believes that such registration would not generally “create” the entity, and thus the entity would not be created by a filing with a secretary of state or similar office.

ProBank Education Services

powered by

FORVIS

67

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

67

However, the particular context and details of a state’s registration and filing practices may be relevant to determining whether an entity is created by a filing, and based on the range of responses regarding state law corporate formation practices, there may be varying practices that make a categorical rule that includes or exclude specific types of entities impracticable. It is similarly difficult to craft a generally applicable rule for conversions or reorganizations of entities, given the range of possible scenarios for conversions or reorganizations under state law and the variety of outcomes in terms of an entity retaining certain attributes of its predecessor entity. In such cases, the touchstone is whether the successor entity is created by the

filing of a document with a secretary of state or similar office. Given the potential range of relevant facts, FinCEN will consider issuing guidance as necessary to resolve questions on whether entities of particular types in particular circumstances are created by the filing of a document with the relevant authority.

ProBank Education

68

FORVIS is a trademark of FORVIS, LLP, reg.

68

Beneficial Owners

- Under the rule, a **beneficial owner** includes any individual who, directly or indirectly, either (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 rule defines the terms “substantial control” and “ownership interest.” In keeping with the CTA, the rule exempts five types of individuals from the definition of “beneficial owner.”
- In defining the contours of who has **substantial control**, the rule sets forth a range of activities that could constitute substantial control of a reporting company. This list captures anyone who is able to make important decisions on behalf of the entity. FinCEN’s approach is designed to close loopholes that allow corporate structuring that obscures owners or decision-makers. This is crucial to unmasking anonymous shell companies.
- The rule provides standards and mechanisms for determining whether an individual owns or controls 25 percent of the **ownership interests** of a reporting company. Among other things, these standards and mechanisms address how a reporting company should handle a situation in which ownership interests are held in trust.
- These definitions have been drafted to account for the various ownership or control structures reporting companies may adopt. However, for reporting companies that have simple organizational structures it should be a straightforward process to identify and report their beneficial owners. FinCEN expects the majority of reporting companies will have simple ownership structures.

87 FR 59533

iii. Exceptions to Definition of Beneficial Owner

31 U.S.C. 5336(a)(3)(B) includes five exceptions to the definition of beneficial owner, for: a minor child, provided that a parent or guardian’s information is reported; an individual acting as a nominee, intermediary, custodian, or agent on behalf of another individual; an individual acting solely as an employee of a reporting company in specified circumstances; an individual whose only interest in a reporting company is a future interest through a right of inheritance; and a creditor of a reporting company. Proposed 31 CFR 1010.380(d)(4) incorporated the statutory exceptions with minor clarifications and sought comments on whether the proposed rules implementing these statutory exceptions are sufficiently clear, and whether any of these rules require further clarification.

“Substantial” Control vs “Control Prong” – “Any” vs “One-Person”

C. Beneficial Owners

Consistent with the CTA, the final rule defines a “beneficial owner,” with respect to a reporting company, as “any individual who, directly or indirectly, either exercises substantial control over such reporting company or owns or controls at least 25 percent of the ownership interests of such reporting company.”¹⁴⁸ Each reporting company will be required to identify as a beneficial owner any individual who satisfies either of these two components of the definition, unless the individual is subject to an exclusion from the definition of “beneficial owner.” FinCEN expects that a reporting company will always identify at least one beneficial owner under the “substantial control” component, even if all other individuals are subject to an exclusion or fail to satisfy the “ownership interests” component.

87FR59525

ProBank Education Services

powered by

FORVIS

71

“Substantial Control”

87FR59594

(1) *Substantial control*—(i) *Definition of substantial control.* An individual exercises substantial control over a reporting company if the individual:

(A) Serves as a senior officer of the reporting company;

(B) Has authority over the appointment or removal of any senior officer or a majority of the board of directors (or similar body);

(C) Directs, determines, or has substantial influence over important decisions made by the reporting company, including decisions regarding:

(1) The nature, scope, and attributes of the business of the reporting company, including the sale, lease, mortgage, or other transfer of any principal assets of the reporting company;

(2) The reorganization, dissolution, or merger of the reporting company;

(3) Major expenditures or investments, issuances of any equity, incurrence of any significant debt, or approval of the operating budget of the reporting company;

(4) The selection or termination of business lines or ventures, or geographic focus, of the reporting company;

ProBank Education Services

powered by

FORVIS

72

Substantial Control (cont.)

87FR59595

- (5) Compensation schemes and incentive programs for senior officers;
- (6) The entry into or termination, or the fulfillment or non-fulfillment, of significant contracts;
- (7) Amendments of any substantial governance documents of the reporting company, including the articles of incorporation or similar formation documents, bylaws, and significant policies or procedures; or
- (D) Has any other form of substantial control over the reporting company.
 - (i) *Direct or indirect exercise of substantial control.* An individual may directly or indirectly, including as a trustee of a trust or similar arrangement, exercise substantial control over a reporting company through:
 - (A) Board representation;
 - (B) Ownership or control of a majority of the voting power or voting rights of the reporting company;
 - (C) Rights associated with any financing arrangement or interest in a company;
 - (D) Control over one or more intermediary entities that separately or collectively exercise substantial control over a reporting company;
 - (E) Arrangements or financial or business relationships, whether formal or informal, with other individuals or entities acting as nominees; or
 - (F) any other contract, arrangement, understanding, relationship, or otherwise.

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

73

73

In addition, FinCEN has evaluated concerns raised about the scope of the definition of “senior officer” in proposed 31 CFR 1010.380(f)(8) and agrees with commenters that the roles of corporate secretary and treasurer tend to entail ministerial functions with little control of the company. FinCEN has therefore omitted those roles from the definition of “senior officer.” FinCEN considers the role of general counsel to be ordinarily more substantial, and has therefore retained this role as part of the definition of “senior officer.” FinCEN notes that the title of the officer ultimately is not dispositive, as the definition of “senior officer” and other indicators of substantial control make clear. Rather, the underlying question is whether the individual is exercising the authority or performing the functions of a senior officer, or otherwise has authority indicative of substantial

Substantial Control (cont.)

control. The final rule also incorporates changes to the “employee” exception to the definition of “beneficial owner” at proposed 31 CFR 1010.380(d)(4)(iii) to make more clear that persons who are senior officers are not subject to this exception, as discussed in Section III.C.iii.c. below.

87FR59526

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

74

74

Company Applicants

- The rule defines a **company applicant** to be only two persons:
 - the individual who directly files the document that creates the entity, or in the case of a foreign reporting company, the document that first registers the entity to do business in the United States.
 - the individual who is primarily responsible for directing or controlling the filing of the relevant document by another.
- The rule, however, does not require reporting companies existing or registered at the time of the effective date of the rule to identify and report on their company applicants. In addition, reporting companies formed or registered after the effective date of the rule also do not need to update company applicant information.

Timing

- The effective date for the rule is January 1, 2024.
- Reporting companies created or registered before January 1, 2024 will have one year (until January 1, 2025) to file their initial reports, while reporting companies created or registered after January 1, 2024, will have 30 days after receiving notice of their creation or registration to file their initial reports.
- Reporting companies have 30 days to report changes to the information in their previously filed reports and must correct inaccurate information in previously filed reports within 30 days of when the reporting company becomes aware or has reason to know of the inaccuracy of information in earlier reports.

Next Steps

- The BOI reporting rule 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 continues to develop the infrastructure to administer these requirements in accordance with the strict security and confidentiality requirements of the CTA, including the information technology system that will be used to store beneficial ownership information: the Beneficial Ownership Secure System (BOSS).
- Consistent with its obligations under the Paperwork Reduction Act, FinCEN will publish in the Federal Register for public comment the reporting forms that persons will use to comply with their obligations under the BOI reporting rule. FinCEN will publish these forms well in advance of the effective date of the BOI reporting rule.

Next Steps (cont.)

- FinCEN will develop compliance and guidance documents to assist reporting companies in complying with this rule. Some of these materials will be aimed directly at, and made available to, reporting companies themselves. FinCEN will issue a Small Entity Compliance Guide, pursuant to section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996, in order to inform small entities about their responsibilities under the rule. Other materials will be aimed at a wide range of stakeholders that are likely to receive questions about the rule, such as secretaries of state and similar offices. FinCEN also intends to conduct extensive outreach to all stakeholders, including industry associations as well as secretaries of state and similar offices to ensure the effective implementation of the rule.

Prepared Remarks of FinCEN Acting Director Himamauli Das During the ABA/ABA Financial Crimes Enforcement Conference

Implementation of the CTA is an intensive process that requires policy teams, economists, regulatory drafters, IT specialists, and public affairs specialists. We are working hard to complete as much of the CTA implementation work as possible within existing resources and staffing. As we enter 2023, however, we will also need to consider trade-offs in implementing this effort in the absence of additional funding—with the goal of making this program as successful as possible.

87 FR 77404-77456 (12/16/22) – Comments closed 02/14/23

DEPARTMENT OF THE TREASURY
Financial Crimes Enforcement Network
31 CFR Part 1010
RIN 1506-AB59
RIN 1506-AB49

Beneficial Ownership Information Access and Safeguards, and Use of FinCEN Identifiers for Entities

AGENCY: Financial Crimes Enforcement Network (FinCEN), Treasury.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: FinCEN is promulgating proposed regulations regarding access by authorized recipients to beneficial ownership information (BOI) that will be reported to FinCEN pursuant to Section 6403 of the Corporate Transparency Act (CTA), enacted into law as part of the Anti-Money Laundering Act of 2020 (AML Act), which is itself part of the National Defense Authorization Act for Fiscal Year 2021 (NDAA). The proposed regulations would implement the strict protocols on security and confidentiality required by the CTA to protect sensitive personally identifiable information (PII) reported to FinCEN. The NPRM explains the circumstances in which specified recipients would have access to BOI and outlines data protection protocols and oversight mechanisms applicable to each recipient category. The disclosure of BOI to authorized recipients in accordance with appropriate protocols

NPRM Areas for Review

- Disclosures to FIs and Regulatory Agencies for CDD Compliance – 77410;
- BOI Retention and Disclosure Requirements – 77415
- Use of Information – 77417 – 77418
- Security and Confidentiality Requirements – 77421 – 77422
- 30 Specific Questions – 77425 – 77426
- Actual Proposed Regulation – 77453 -- 77457

Request for Comment (77425)

11. FinCEN proposes that FIs be required to obtain the reporting company's consent in order to request the reporting company's BOI from FinCEN. FinCEN invites commenters to indicate what barriers or challenges FIs may face in fulfilling such a requirement, as well as any other considerations.

Request for Comment (77425) (cont.)

12. FinCEN proposes to define “customer due diligence requirements under applicable law” to mean the bureau’s 2016 CDD Rule, as it may be amended or superseded pursuant to the AML Act. The 2016 CDD Rule requires FIs to identify and verify beneficial owners of legal entity customers. Should FinCEN expressly define “customer due diligence requirements under applicable law” as a larger category of requirements that includes more than identifying and verifying beneficial owners of legal entity customers? If so, what other requirements should the phrase encompass? How should the broader definition be worded? It appears to FinCEN that the consequences of a broader definition of this phrase would include making BOI available to more FIs for a wider range of specific compliance purposes, possibly making BOI available to more regulatory agencies for a wider range of specific examination and oversight purposes, and putting greater pressure on the demand for the security and confidentiality of BOI. How does the new balance of those consequences created by a broader definition fulfill the purpose of the CTA?

83

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

83

Request for Comment (77426) (cont.)

Security and Confidentiality Requirements

20. Should FinCEN impose any additional security or confidentiality requirements on authorized recipients of any type? If so, what requirements and why?

84

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

84

Request for Comment (77426) (cont.)

23. FinCEN proposes to require FIs to limit BOI disclosure to FI directors, officers, employees, contractors, and agents within the United States. Would this restriction impose undue hardship on FIs? What are the practical implications and potential costs of this limitation?

24. Are the procedures FIs use to protect non-public customer personal information in compliance with section 501 of Gramm-Leach-Bliley sufficient for the purpose of securing BOI disclosed by FinCEN under the CTA? If not, is there another set of security standards FinCEN should require FIs to apply to BOI?

85

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

85

Request for Comment (77426) (cont.)

25. Are the standards established by section 501 of Gramm-Leach-Bliley, its implementing regulations, and interagency guidance sufficiently clear such that FIs not directly subject to that statute will know how to comply with FinCEN's requirements with respect to establishing and implementing security and confidentiality standards?

26. Do any states impose, and supervise for compliance on, security and confidentiality requirements comparable to those that FFRs are required to impose on FIs under section 501 of Gramm-Leach-Bliley? Please provide examples of such requirements.

86

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

86

Request for Comment (77426) (cont.)

Outreach

29. What specific issues should FinCEN address via public guidance or FAQs? Are there specific recommendations on engagement with stakeholders to ensure that the authorized recipients, and in particular, State, local, and Tribal authorities and small and mid-sized FIs, are aware of requirements for access to the beneficial ownership IT system?

87

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

87

BOIR / CTA Issues for DFIs

- The modification to the current CDD Rule is required to be published by 01/01/25.
- Until the NPRM / Final Rule is published, unknowns include:
 - How will current CDD Rule be “reconciled” to the BOIR Rule;
 - Will DFIs be required to continue to collect and utilize current beneficial ownership information even though covered legal entities will be submitting similar data directly to Treasury;
 - How much, if any, verification will DFIs be expected to perform on the covered legal entity’s compliance with BOIR;
 - Will DFIs be allowed to use the “FinCEN Identifier” in lieu of collecting Beneficial Ownership info;
 - What expectations, if any, will be imposed on DFIs to report discrepancies in the data via SARs;
 - Although FinCEN has promised industry outreach, how much guidance will DFIs be expected to provide to their clients who are covered legal entities.

ProBank Education Services *powered by* **FORVIS**

88

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

88

88FR 2760 – 2764 01/17/23 – Comments Due 03/20/23

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network

Agency Information Collection Activities; Proposed Collection; Comment Request; Beneficial Ownership Information Reports

AGENCY: Financial Crimes Enforcement Network (FinCEN), Treasury.

ACTION: Notice and request for comments.

SUMMARY: FinCEN invites all interested parties to comment on the report that will be used to collect beneficial ownership information, as required by the Beneficial Ownership Information Reporting Requirements final rule that was published on September 30, 2022. The details included in the information collection are listed below. This request for comment is made pursuant to the Paperwork Reduction Act of 1995.

DATES: Written comments are welcome and must be received on or before March 20, 2023.

ProBank Education Services

powered by

FORVIS

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

89

88 FR 2764 – 2766 02/17/23 Comments Due 03/20/23

DEPARTMENT OF THE TREASURY Financial Crimes Enforcement Network Agency Information Collection Activities; Proposed Collection; Comment Request; Individual FinCEN Identifiers

AGENCY: Financial Crimes Enforcement Network (FinCEN), Treasury.
ACTION: Notice and request for comments.

SUMMARY: FinCEN invites all interested parties to comment on the application that will be used to collect information from individuals who seek to obtain a FinCEN identifier, consistent with the Beneficial Ownership Information

Reporting Requirements final rule that was published on September 30, 2022. Obtaining a FinCEN identifier is voluntary; however, individuals who seek to obtain a FinCEN identifier must submit an application and update the information provided on the application as necessary. The details included in the information collection are listed below. This request for comment is made pursuant to the Paperwork Reduction Act of 1995.

DATES: Written comments are welcome and must be received on or before March 20, 2023.

ProBank Education Services

powered by

FORVIS

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

90

90

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 will also 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.

140
Comments

ProBank Education Services
powered by
FORVIS

91

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

91

Modernization of AML/CFT Regulatory Regime

- 86 FR 71201 – 71207
- 26 Questions to “stimulate” thought
- 12/15/21

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.

ProBank Education Services
powered by
FORVIS

92

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

92

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).

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

88 FR 3312 01/19/2023

TABLE 1 OF § 1010.821—PENALTY ADJUSTMENT TABLE

U.S. Code citation	Civil monetary penalty description	Penalties as last amended by statute	Maximum penalty amounts or range of minimum and maximum penalty amounts for penalties assessed on or after 1/19/2022
12 U.S.C. 1829b(j)	Relating to Recordkeeping Violations For Funds Transfers	\$10,000	\$24,793
12 U.S.C. 1955	Willful or Grossly Negligent Recordkeeping Violations	10,000	24,793
31 U.S.C. 5318(k)(3)(C)	Failure to Terminate Correspondent Relationship with Foreign Bank.	10,000	16,771
31 U.S.C. 5321(a)(1)	General Civil Penalty Provision for Willful Violations of Bank Secrecy Act Requirements.	25,000–100,000	67,544–270,180
31 U.S.C. 5321(a)(5)(B)(i)	Foreign Financial Agency Transaction—Non-Willful Violation of Transaction.	10,000	15,611
31 U.S.C. 5321(a)(5)(C)(i)(I)	Foreign Financial Agency Transaction—Willful Violation of Transaction.	100,000	156,107
31 U.S.C. 5321(a)(6)(A)	Negligent Violation by Financial Institution or Non-Financial Trade or Business.	500	1,350
31 U.S.C. 5321(a)(6)(B)	Pattern of Negligent Activity by Financial Institution or Non-Financial Trade or Business.	50,000	105,083
31 U.S.C. 5321(a)(7)	Violation of Certain Due Diligence Requirements, Prohibition on Correspondent Accounts for Shell Banks, and Special Measures.	1,000,000	1,677,030
31 U.S.C. 5330(e)	Civil Penalty for Failure to Register as Money Transmitting Business.	5,000	9,966

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.



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)' 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

ProBank Education Services

powered by

FORVIS

95

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

95

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.

ProBank Education Services

powered by

FORVIS

96

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

96



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.

ProBank Education Services

powered by

FORVIS

97

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

97

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.

ProBank Education Services

powered by

FORVIS

98

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

98

FEDERAL TRADE COMMISSION

A Scammy Snapshot of 2022

(based on reports to Consumer Sentinel)

#FTCTopFrauds
ftc.gov/data
ReportFraud.ftc.gov

REPORT **2.4 million** fraud reports

\$8.8 billion reported lost

The number of reports is down. The amount lost is up. (2021: 2.9 million fraud reports, \$6.1 billion lost)

Top Frauds

- 1 Imposters
- 2 Online shopping
- 3 Prizes, sweepstakes, lotteries
- 4 Investments
- 5 Business and job opportunities

Losses to investment scams more than doubled.

\$1.8 billion (2021) | **\$3.8 billion** (2022)

Losses to business imposters soared.

\$196 million (2020) | **\$453 million** (2021) | **\$660 million** (2022)

Scammers contacting people on social or by phone led to big losses

- \$1.2 billion** total lost
Social media: Highest overall reported losses
- \$1,400** median loss
Phone calls: Highest per person reported losses

ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

CONSUMER SENTINEL NETWORK
DATA BOOK 2022

SNAPSHOT

5.2 MILLION REPORTS

TOP THREE CATEGORIES

- 1 Identity Theft
- 2 Imposter Scams
- 3 Credit Bureaus, Info Furnishers and Report Users

2.4 million fraud reports

26% reported a loss

\$8.8 billion total fraud losses | **\$650** median loss

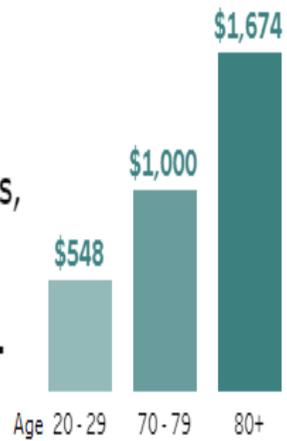
ProBank Education Services powered by **FORVIS**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

Younger people reported losing money to fraud more often than older people.



But when people aged 70+ had a loss, the median loss was much higher.



FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

Imposter Scams



ABOUT
1 in 5
PEOPLE
LOST MONEY

\$2.667 billion
reported lost

\$1,000 median loss

Data as of December 31, 2022

Identity Theft Reports

13% ↑

Credit card new
account fraud

88% ↓

Government
Benefits Applied
For\Received

FEDERAL TRADE COMMISSION • ftc.gov/data

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

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

**Interagency Statement on the Issuance of the Anti-Money Laundering/
Countering the Financing of Terrorism National Priorities**

June 30, 2021

The Anti-Money Laundering Act of 2020 (the "AML Act")¹ requires the Secretary of the Treasury, in consultation with the Attorney General, Federal functional regulators,² relevant State financial regulators, and relevant national security agencies, to establish and make public priorities for anti-money laundering and countering the financing of terrorism policy (AML/CFT Priorities).³ Accordingly, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) published [these](#) first national AML/CFT Priorities today in consultation with the parties as set out in the AML Act. As a result of this publication, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency (collectively, the "federal banking agencies" or "FBAs"), State bank and credit union regulators,⁴ and FinCEN are issuing this statement to provide clarity for banks⁵ on these AML/CFT Priorities.

Today's publication of the AML/CFT Priorities does not create an immediate change to Bank Secrecy Act (BSA) requirements or supervisory expectations for banks. The AML Act requires that, within 180 days of the establishment of the AML/CFT Priorities, FinCEN (in consultation with Federal functional regulators and relevant State financial regulators) shall, as appropriate, promulgate regulations regarding the AML/CFT Priorities.⁶ Although not required by the AML Act, the FBAs plan to revise their BSA regulations, as necessary, to address how the AML/CFT Priorities will be incorporated into banks' BSA requirements.

ProBank Education Services

powered by

FORVIS

103

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

103

Banks are not required to incorporate the AML/CFT Priorities into their risk-based BSA compliance programs until the effective date of the final revised regulations. Nevertheless, in preparation for any new requirements when those final rules are published, banks may wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based BSA compliance programs, such as by assessing the potential related risks associated with the products and services they offer, the customers they serve, and the geographic areas in which they operate.

Finally, the AML Act requires that the review by a bank of the AML/CFT Priorities and the incorporation of those priorities, as appropriate, into its risk-based BSA compliance program, be included as a measure on which a bank is supervised and examined.⁷ This interagency statement confirms that State bank and credit union regulator and FBA examiners will not examine banks for the incorporation of the AML/CFT Priorities into their risk-based BSA programs until the effective date of final revised regulations.

The FBAs, State bank and credit union regulators, and FinCEN recognize the need to provide revised regulations and timely guidance to assist banks in complying with the BSA. In addition, the FBAs and State bank and credit union regulators are committed to working with FinCEN to develop any necessary corresponding guidance and examination procedures for examiners.

ProBank Education Services

powered by

FORVIS

104

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

104

AML “Remaining” Deliverables

- Awaiting Regulations / Changes covering:
 - AML/CFT Priorities;
 - Modifications to BSA FBA Agency Regulations and Exam Procedures.
 - CTA – Beneficial Ownership Information Reporting (BOIR) Rules for Small Businesses;
 - BOIR Final Rule published 09/30/22 – Effective 01/01/2024
 - CTA – Who/How can use the BOIR data Rules;
 - Bene Owner – Modifications to DFI Beneficial Ownership Rules.
 - Modernize, Streamline, and Update the AML/CFT Regime of the United States;
 - Arts and Antiquities inclusions into the BSA “fold”.
- Convertible Virtual Currency “treatment”;
- Results of efficiency studies and “action” items;
- Whistleblower “incentives”

ProBank Education Services powered by **FORVIS**

105

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

105

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.

ProBank Education Services powered by **FORVIS**

106

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

106

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 casher's 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.

FinCEN Announces \$140 Million Civil Money Penalty against USAA Federal Savings Bank for Violations of the Bank Secrecy Act

Contact: Office of Strategic Communications, press@fincen.gov
Immediate Release: March 17, 2022

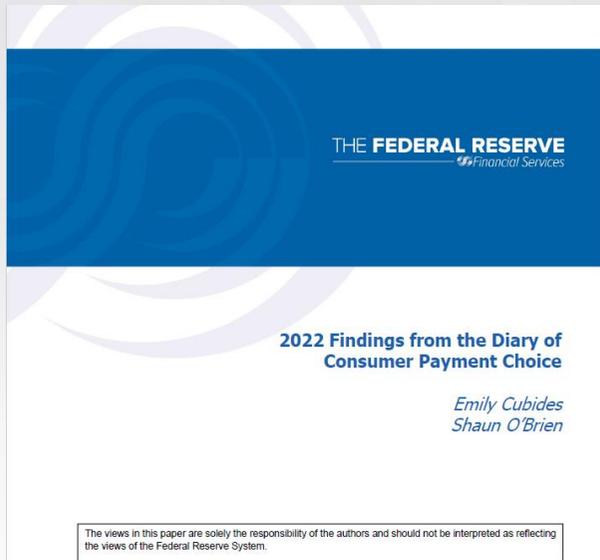
WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today announced that it has assessed a \$140 million [civil money penalty](#) against USAA Federal Savings Bank (USAA FSB) for willful violations of the Bank Secrecy Act (BSA) and its implementing regulations.

Specifically, USAA FSB admitted that it willfully failed to implement and maintain an anti-money laundering (AML) program that met the minimum requirements of the BSA from at least January 2016 through April 2021. USAA FSB also admitted that it willfully failed to accurately and timely report thousands of suspicious transactions to FinCEN involving suspicious financial activity by its customers, including customers using personal accounts for apparent criminal activity.

"As its customer base and revenue grew in recent years, USAA FSB willfully failed to ensure that its compliance program kept pace, resulting in millions of dollars in suspicious transactions flowing through the U.S. financial system without appropriate reporting," said FinCEN's Acting Director Himamauli Das. "USAA FSB also received ample notice and opportunity to remediate its inadequate AML program, but repeatedly failed to do so. Today's action signals that growth and compliance must be paired, and AML program deficiencies, especially deficiencies identified by federal regulators, must be promptly and effectively addressed."

The Office of the Comptroller of the Currency (OCC) assessed a civil penalty of \$60 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 \$60 million civil penalty imposed by the OCC. Taken together, USAA FSB will pay a total of \$140 million to the U.S. Treasury for its violations, with \$80 million representing FinCEN's penalty and \$60 million representing the OCC's penalty.

FinCEN's Office of Enforcement is responsible for investigating serious violations of the BSA. 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 USAA FSB [here](#).



How much do you know about cash?

FED FACTS | June 15, 2022 | [Twitter](#) [LinkedIn](#)

We use cash as part of our daily lives, but how much do you know about its history and features? While cash usage has fluctuated over the past several years, it continues to be a reliable form of payment. Check out these five facts about cash:

- 1. U.S. currency paper is composed of 25% linen and 75% cotton**
Despite its light weight, U.S. currency is quite sturdy. Currency paper is made of a cotton and linen blend with red and blue fibers distributed randomly throughout to make imitation more difficult.
- 2. Each denomination of Federal Reserve notes has its own identifiers and symbols that serve as security features**
While intricate designs make Federal Reserve notes visually appealing, some details add complexity and serve as security features. Each Federal Reserve note, for instance, contains a serial number that provides key information about the note. This unique combination of characters appears twice on the front of the note. Additionally, the Treasury Seal can be found across all denominations.
- 3. The Federal Reserve does not design or print money**
New currency designs are developed by designers at the Bureau of Engraving and Printing (BEP), and the final design is approved by the Secretary of the Treasury. To learn about the process for designing and printing money, visit the BEP's feature on "How Money is Made" ([FED-site](#)).
- 4. The \$5 note has the shortest lifespan.**
The lifespan of Federal Reserve notes varies by denomination. The \$5 note's lifespan is only 4.7 years, followed by the \$10 note at 5.3 years, and \$1 note at 6.6 years. Learn more about [lifespan data \(FED-site\)](#).
- 5. The Federal Reserve Banks review the quality of each note**
When currency is deposited with a Federal Reserve Bank, the quality of each note is evaluated by sophisticated processing equipment. Notes that meet strict quality criteria continue to circulate. The 12 Federal Reserve Banks repurpose banknotes not fit for circulation. The banks shred and reuse money that is too worn or dirty for a number of purposes, such as insulation or compost.

Check out these resources to help you learn more about cash:

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.

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 FD-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



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Enforcement Release: July 21, 2022

OFAC Issues a Finding of Violation to ██████████ for Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has issued a Finding of Violation (FOV) to ██████████ for violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations (WMDPSR). The violations related to ██████████ maintaining accounts for and processing of 34 payments on behalf of two individuals added to OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List") for 14 days post-designation. The violations stemmed from ██████████ misunderstanding of the frequency of its vendor's screening of new names added to the SDN List against its existing customer base. OFAC determined that the appropriate administrative action in this matter was an FOV in lieu of a civil monetary penalty. This FOV reaffirms that financial institutions should take a risk-based approach to sanctions compliance, including when implementing sanctions screening tools, and demonstrates the importance of ensuring the scope and capabilities of outsourced sanctions compliance services are consistent with the financial institution's assessment of its exposure to sanctions risks.

ProBank Education Services

powered by

FORVIS

113

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

113

Description of the Violations

On September 21, 2020, at 12:36 p.m. EDT, OFAC designated and added two individuals to the SDN List ("the blocked persons") pursuant to the WMDPSR. On the same day, between 2:00 p.m. EDT and 5:48 p.m. EDT, ██████████ processed five transactions totaling \$604,000 on behalf of accounts held by the blocked persons. Two of those transactions, totaling \$400,000, were internal book transfers between one of the blocked person's accounts at ██████████. Between September 22, 2020 and October 5, 2020, ██████████ processed 29 additional transactions totaling \$9,879.02 on behalf of the blocked persons. Ninety-eight percent of the value of the post-designation transactions occurred within six hours of designation.

██████████ reported to OFAC that its sanctions screening vendor notified ██████████ that the blocked persons had been added to the SDN list on October 5, 2020, 14 days after their addition. ██████████ then promptly blocked accounts belonging to the blocked persons.

The agreement between ██████████ and its vendor provided for periodic screening of ██████████ customers against the SDN List. Although the vendor conducted daily screenings of new customers and of existing customers with certain account changes (e.g., changes to a customer's name or address), the vendor only screened ██████████ entire existing customer base once a month. ██████████ misunderstood the scope of the contract with its vendor, mistakenly believing that the daily screenings would screen its entire customer base against additions and changes to the SDN List.

ProBank Education Services

powered by

FORVIS

114

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

114

As a result, depending on the timing of additions to the SDN List in relation to the monthly screening, ██████ could be unaware for up to 30 days that it was maintaining an account for a blocked person. In this case, the customers matching two of the September 21, 2020 designations were not discovered until the vendor generated its monthly report on October 5, 2020.

Although ██████ maintained its own process to screen existing customers, this process also screened on a monthly basis only. The first such monthly screening following the subject designations was conducted on October 5, 2021, the same day the vendor flagged the matches for ██████.

As a result of the foregoing, ██████'s maintaining of accounts for and processing 34 transactions on behalf of the blocked persons was in violation of § 544.201 of the WMDPSR.

In an effort to remediate this issue, in November 2020 ██████ implemented a manual process to be notified "of all OFAC list updates" and to manually rescreen the entire customer base whenever there are updates to the SDN List. In addition, in December 2020 the vendor updated the frequency of the screening of the entire account base.

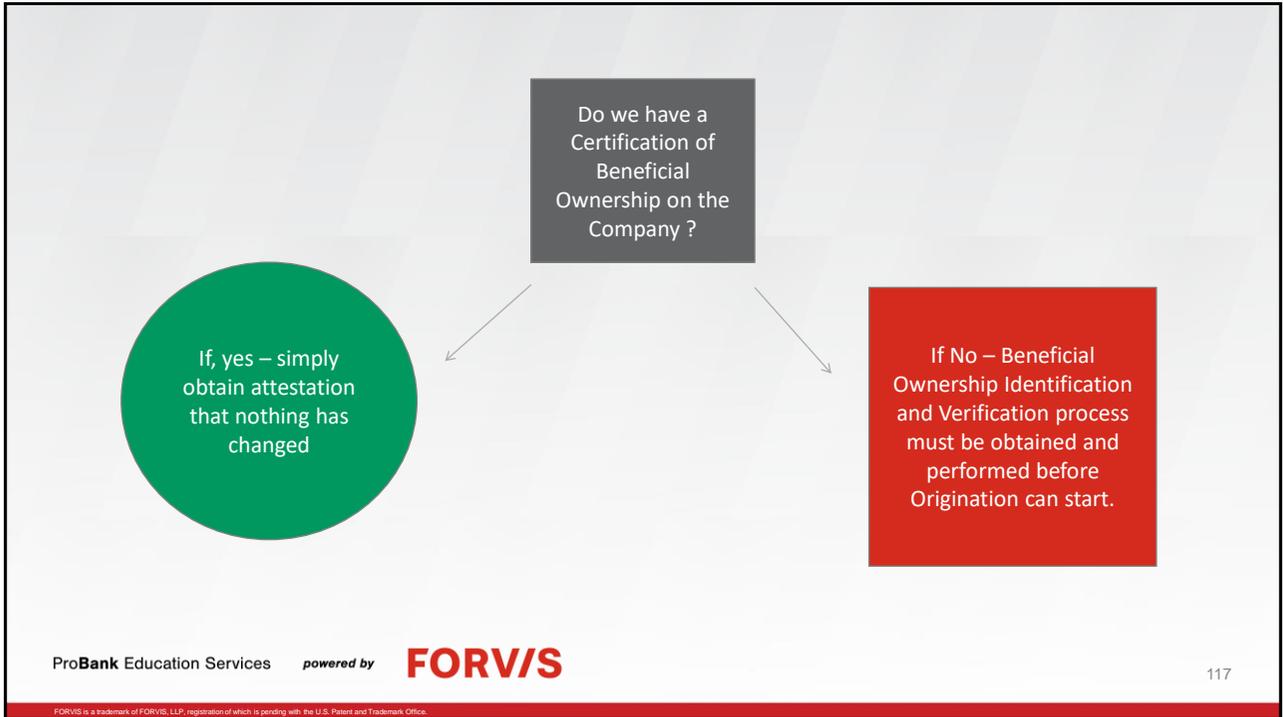
Compliance Considerations

As explained in OFAC's [A Framework for OFAC Compliance Commitments](#), financial institutions should take a risk-based approach when developing their sanctions compliance program, including with respect to screening accounts and transactions for potential violations of OFAC regulations. There is no "one-size-fits all" approach to sanctions screening. Different financial institutions may have different risk tolerances and divergent approaches to sanctions compliance based on an institution's unique risk profile. Accordingly, the frequency with which financial institutions screen and review existing customers and accounts should be based on the financial institution's assessment of its unique sanctions risk. Consistent with that risk-based approach to sanctions compliance, this FOV demonstrates that understanding the scope and capabilities of outsourced sanctions compliance services is critical to ensuring that those services are aligned with the financial institution's expectations for managing its self-assessed sanctions risk.

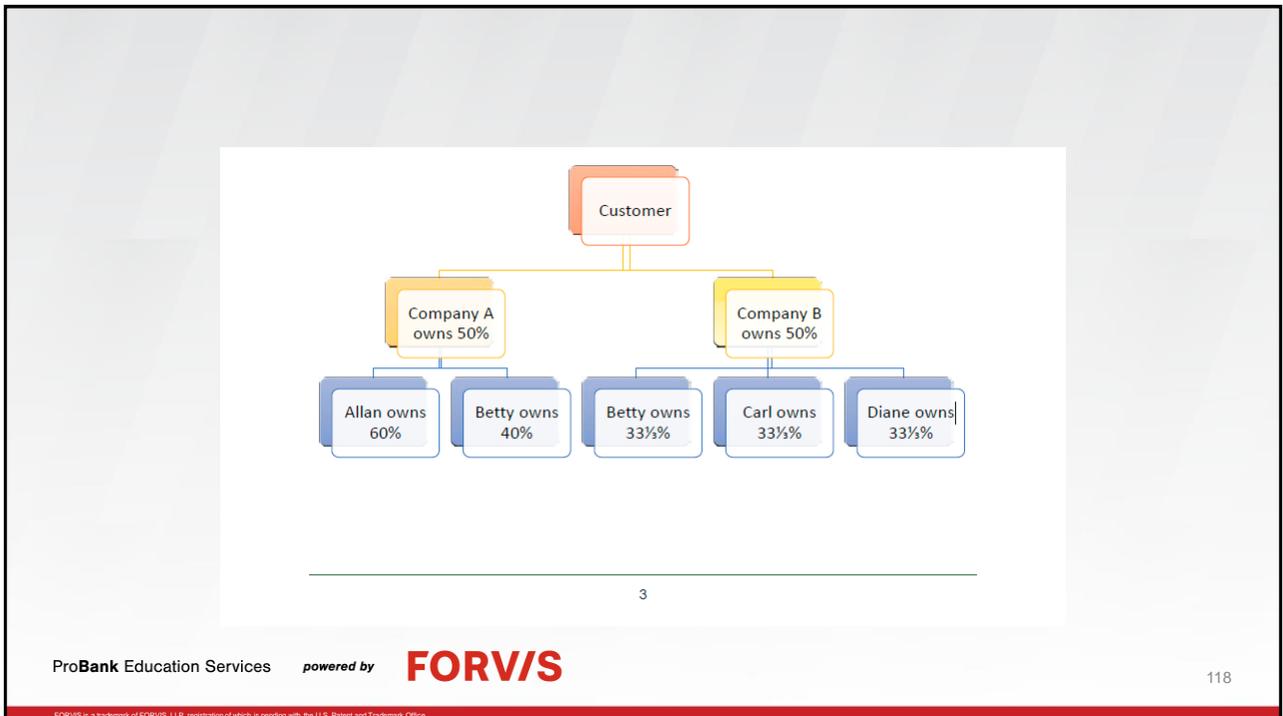
OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published [A Framework for OFAC Compliance Commitments](#) in order to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use goods or services exported from the United States, with OFAC's perspective on the essential components of a sanctions compliance program. The *Framework* also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The *Framework* includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

Information concerning the civil penalties process can be found in the OFAC regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. These references, as well as recent civil penalties and enforcement information, can be found on OFAC's website at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>.



117



118



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](#).

ProBank Education Services

powered by

FORVIS

119

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

119

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.

ProBank Education Services

powered by

FORVIS

120

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

120

II. Customer Risk Profile

Q2: Is it a requirement under the CDD Rule that covered financial institutions:

- use a specific method or categorization to risk rate customers; or
 - automatically categorize as “high risk” products and customer types that are identified in government publications as having characteristics that could potentially expose the institution to risks?
- A. It is not a requirement that covered financial institutions use a specific method or categorization to establish a customer risk profile. Further, covered financial institutions are not required or expected to automatically categorize as “high risk” products or customer types listed in government publications.

Various government publications provide information and discussions on certain products, services, customers, and geographic locations that present unique challenges and exposures regarding illicit financial activity risks. However, even within the same risk category, a spectrum of risks may be identifiable and due diligence measures may vary on a case-by-case basis.

A covered financial institution should have an understanding of the money laundering, terrorist financing, and other financial crime risks of its customers to develop the customer risk profile. Furthermore, the financial institution’s program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the risks of its customers. There are no prescribed risk profile categories, and the number and detail of these categories can vary.

III. Ongoing Monitoring of the Customer Relationship

Q3: Is it a requirement under the CDD Rule that financial institutions update customer information on a specific schedule?

- A. There is no categorical requirement that financial institutions update customer information on a continuous or periodic schedule. The requirement to update customer information is risk based and occurs as a result of normal monitoring. Should the financial institution become aware as a result of its ongoing monitoring of a change in customer information (including beneficial ownership information) that is relevant to assessing the risk posed by the customer, the financial institution must update the customer information accordingly. Additionally, if this customer information is relevant to assessing the risk of a customer relationship, then the financial institution should reassess the customer risk profile/rating and follow established financial institutions policies, procedures, and processes for maintaining or changing the customer risk profile/rating. However, financial institutions, on the basis of risk, may choose to review customer information on a regular or periodic basis.

For Further Information

Questions or comments regarding the contents of this guidance should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

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

Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence

July 6, 2022

The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Financial Crimes Enforcement Network, the National Credit Union Administration, and the Office of the Comptroller of the Currency (collectively, the Agencies) are issuing this joint statement to remind banks¹ of the risk-based approach to assessing customer relationships and conducting customer due diligence (CDD). This statement does not alter existing Bank Secrecy Act/Anti-Money Laundering (BSA/AML) legal or regulatory requirements, nor does it establish new supervisory expectations.

The Agencies recognize that it is important for customers engaged in lawful activities to have access to financial services. Therefore, the Agencies are reinforcing a longstanding position that no customer type presents a single level of uniform risk or a particular risk profile related to money laundering, terrorist financing, or other illicit financial activity.

ProBank Education Services powered by

FORVIS

123

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

123

Banks must apply a risk-based approach to CDD, including when developing the risk profiles of their customers.² More specifically, banks must adopt appropriate risk-based procedures for conducting ongoing CDD that, among other things, enable banks to: (i) understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (ii) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.³

Customer relationships present varying levels of money laundering, terrorist financing, and other illicit financial activity risks. The potential risk to a bank depends on the presence or absence of numerous factors, including facts and circumstances specific to the customer relationship. Not all customers of a particular type automatically represent a uniformly higher risk of money laundering, terrorist financing, or other illicit financial activity.

ProBank Education Services powered by

FORVIS

124

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

124

Banks that operate in compliance with applicable BSA/AML legal and regulatory requirements, and effectively manage and mitigate risks related to the unique characteristics of customer relationships, are neither prohibited nor discouraged from providing banking services to customers of any specific class or type. As a general matter, the Agencies do not direct banks to open, close, or maintain specific accounts. The Agencies continue to encourage banks to manage customer relationships and mitigate risks based on customer relationships, rather than decline to provide banking services to entire categories of customers.⁴

In addition, the Agencies recognize that banks choose whether to enter into or maintain business relationships based on their business objectives and other relevant factors, such as the products and services sought by the customer, the geographic locations where the customer will conduct or transact business, and banks' ability to manage risks effectively.⁵

This statement addresses the Agencies' perspective on assessing customer relationships as well as CDD requirements. It applies to all customer types referenced in the *Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering Examination Manual*,⁶ including, for example, independent automated teller machine owners or operators,⁷ nonresident aliens and foreign individuals, charities and nonprofit organizations, professional service providers, cash intensive businesses, nonbank financial institutions, and customers the bank considers politically exposed persons. This statement also applies to any customer type not specifically addressed in the *FFIEC BSA/AML Examination Manual*.

The *FFIEC BSA/AML Examination Manual*, including sections on certain customer types, provides guidance to examiners for carrying out BSA/AML examinations and assessing a bank's compliance with the BSA; it does not establish requirements for banks. Further, the inclusion of sections on specific customer types provides background information and procedures for examiners related to risks associated with money laundering and terrorist financing; inclusion of these sections is not intended to signal that certain customer types should be considered uniformly higher risk.

Geographic Targeting Order Covering TITLE INSURANCE COMPANY
October 26, 2022

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 \$50,000 or more in the City or County of Baltimore in Maryland, or in the amount of \$300,000 or more in any of the following areas:
 1. The Texas counties of Bexar, Tarrant, Dallas, Harris, Montgomery, or Webb;

ProBank Education Services

powered by

FORVIS

127

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

127

2. The Florida counties of Miami-Dade, Broward, or Palm Beach;
 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 Hawaii counties of Hawaii, Maui, Kauai, or Honolulu, or the City of Honolulu;
 6. The Nevada county of Clark;
 7. The Washington county of King;
 8. The Massachusetts counties of Suffolk or Middlesex;
 9. The Illinois county of Cook;
 10. The Maryland counties of Montgomery, Anne Arundel, Prince George’s, or Howard;
 11. The Virginia counties of Arlington or Fairfax, or the cities of Alexandria, Falls Church, or Fairfax;
 12. The Connecticut county of Fairfield; or
 13. The District of Columbia.
- 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.

ProBank Education Services

powered by

FORVIS

128

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

128

FDIC 2021 National Survey of Unbanked and Underbanked Households – Data collected during June 2021

- Released on 10/25/2022, the survey found:
 - 4.5 % of U.S. households are unbanked (5.9 Million households, down from 7.1 million in 2021,);
 - 14.1% of U.S. households were underbanked, meaning that at least one member of the household had a checking or savings account at a bank or Credit Union, and used at least one money order, check cashing service, international remittance, payday loan, tax refund anticipation loan, or auto-title loan from a non-bank provider.
 - 81.5% of U.S. households were “fully” banked, meaning that at least one member of the household had a checking or savings account at a bank or Credit Union.
 - 95.5% of U.S. households were banked or underbanked.
 - 48.9% of the unbanked households’ # 1 reason for not having a bank account – not enough \$ to meet minimum balance requirements - # 2 – they didn’t trust banks.
 - 33% of the recently banked households reported that ease of receiving government payment contributed to opening the account.

ProBank Education Services

powered by

FORVIS

129

FDIC 2021 National Survey of Unbanked and Underbanked Households – Data collected during June 2021 (cont.)

Figure ES.1 National Estimates, Household Unbanked Rate, 2009–2021 (Percent)

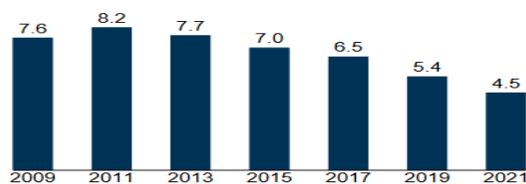


Table 11.1 Underbanked, Fully Banked, and Unbanked Rates by Selected Household Characteristics, 2021
All Households, Row Percent

Characteristics	Underbanked	Fully Banked	Unbanked
All	14.1	81.5	4.5
Family Income			
Less Than \$15,000	19.2	61.0	19.8
\$15,000 to \$30,000	18.9	71.9	9.2
\$30,000 to \$50,000	17.3	78.7	4.0
\$50,000 to \$75,000	14.0	83.9	2.1
At Least \$75,000	9.7	89.7	0.6

ProBank Education Services

powered by

FORVIS

130

2022 SAR Activity Distribution (a/o 02/28/23)

1,827,917 // 3,616,450 (+ 28.12 % // + 17.82%)

1	Check	501,477	9.75%
2	Transaction(s) Below CTR Threshold	439,013	8.54%
3	Suspicion Concerning the Source of Funds	385,111	7.49%
4	Transaction with No Apparent Economic, Business, or Lawful Purpose	365,743	7.11%
5	Transaction Out of Pattern for Customer(s)	310,484	6.04%
6	Suspicious EFT/Wire Transfers	296,804	5.77%
7	Identity Theft	278,121	5.41%
8	Credit/Debit Card	269,694	5.25%
9	Suspicious use of multiple transaction locations	249,482	4.85%
10	Other Fraud (Type)	219,549	4.27%
11	Counterfeit Instrument	213,701	4.16%
12	ACH	183,732	3.57%

ProBank Education Services powered by **FORVIS**

131

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

131

2022 SAR Activity Distribution (a/o 02/28/23)

1,827,917 // 3,616,450 (+ 28.12% // + 17.82%)

13	Other Other Suspicious Activities	157,851	3.07%
14	Two or More Individuals Working Together	141,788	2.76%
15	Suspicious Use of Multiple Accounts	114,064	2.22%
16	Provided Questionable or False Documentation	97,630	1.90%
17	Forgeries	89,735	1.75%
18	Consumer Loan (see instructions)	81,777	1.59%
19	Wire	77,761	1.51%
20	Suspicious Use of Noncash Monetary Instruments	76,181	1.48%
21	Other Money Laundering	73,795	1.44%
22	Account Takeover	61,105	1.19%
23	Elder Financial Exploitation	60,170	1.17%
24	Transaction(s) Involving Foreign High Risk Jurisdiction	50,734	0.99%

ProBank Education Services powered by **FORVIS**

132

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

132

2022 SAR Activity Distribution (a/o 02/28/23)

1,827,917 // 3,616,450 (+ 28.12% // + 17.82%)

25	Suspicious Receipt of Government Payments/Benefits	34,601	0.67%
26	Alters or Cancels Transaction to Avoid CTR Requirement	30,698	0.60%
27	Mass-Marketing	30,629	0.60%
28	Transaction(s) Below BSA Recordkeeping Threshold	26,150	0.51%
29	Against Financial Institution Customer(s)	18,735	0.36%
30	Funnel Account	18,433	0.36%
31	Provided Questionable or False Identification	17,699	0.34%
32	Business Loan	17,603	0.34%
33	Refused or Avoided Request for Documentation	12,889	0.25%
34	Mail	11,830	0.23%
35	Little or No Concern for Product Performance Penalties, Fees, or Tax Consequences	11,814	0.23%
36	Suspicious Inquiry by Customer Regarding BSA Reporting or Recordkeeping Requirements	11,062	0.22%

ProBank Education Services powered by **FORVIS**

133

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

133

2022 SAR Activity Distribution (a/o 02/28/23)

1,827,917 // 3,616,450 (+ 28.12% // + 17.82%)

39	Against Financial Institution(s)	7,188	0.14%
47	Other Cyber Event	4,341	0.08%
48	Unlicensed or Unregistered MSB	3,576	0.07%
54	Human Trafficking	2,069	0.04%
60	Healthcare/Public or Private Health Insurance	977	0.02%
62	Suspected Public/Private Corruption (Foreign)	495	0.01%
66	Ponzi Scheme	390	0.01%
69	Suspected Public/Private Corruption (Domestic)	263	0.01%
70	Human Smuggling	246	0.00%
72	Known or Suspected Terrorist/Terrorist Organization	188	0.00%
73	Other Terrorist	132	0.00%
74	Pyramid Scheme	123	0.00%

ProBank Education Services powered by **FORVIS**

134

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

134

2022 SAR Distribution

By State

1	California	275,518
2	North Carolina	221,382
3	Ohio	189,138
4	New York	166,828
5	Virginia	163,488
6	Texas	143,647
7	Florida	130,804
8	Delaware	112,988
9	Pennsylvania	72,719
10	Illinois	62,409
11	Georgia	59,675
12	New Jersey	57,583
13	Utah	52,426
14	South Dakota	44,829
15	Michigan	33,114
16	Alabama	31,073
17	Massachusetts	28,817
18	Washington	28,609
19	Tennessee	27,403
20	Maryland	27,232

135

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

135

2022 SAR Distribution

By State

21	Arizona	26,196
22	Indiana	23,748
23	Nevada	20,254
24	Louisiana	19,849
25	Wisconsin	18,659
26	Colorado	17,985
27	Minnesota	17,594
28	Oklahoma	15,991
29	South Carolina	15,931
30	Puerto Rico	15,889
31	Mississippi	14,864
32	Connecticut	14,758
33	Missouri	14,512
34	West Virginia	13,314
35	Oregon	12,737
36	Kentucky	12,057
37	Arkansas	9,792
38	Hawaii	8,282
39	Rhode Island	8,145
40	Iowa	7,796

136

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

136

2022 SAR Distribution

By State

41	Kansas	7,686
42	New Mexico	6,351
43	Nebraska	6,137
44	Maine	4,874
45	District of Columbia	4,855
46	New Hampshire	4,019
47	North Dakota	3,832
48	Idaho	3,801
49	Montana	3,245
50	Unknown	3,127
51	Alaska	2,978
52	Vermont	1,822
53	Wyoming	1,108
54	Guam	910
55	Virgin Islands	728
56	APO / DPO / FPO	496
57	Northern Mariana Islands	98
58	Palau	50
59	Micronesia, Federated States	10
60	American Samoa	4
61	Marshall Islands	2

137

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

137

2022 SAR Activity Distribution “Top 48” Metropolitan Filing Areas (out of 1,000+)

1	Charlotte-Gastonia-Rock Hill, NC-SC Metro Area	197,597
2	New York-Northern New Jersey-Long Island, NY-NJ-PA Metro Area	182,188
3	Columbus, OH Metro Area	124,042
4	Washington-Arlington-Alexandria, DC-VA-MD-WV Metro Area	112,437
5	Los Angeles-Long Beach-Santa Ana, CA Metro Area	100,372
6	San Francisco-Oakland-Fremont, CA Metro Area	97,118
7	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD Metro Area	83,592
8	Miami-Fort Lauderdale-Pompano Beach, FL Metro Area	69,907
9	Richmond, VA Metro Area	58,184
10	Chicago-Joliet-Naperville, IL-IN-WI Metro Area	52,558
11	Atlanta-Sandy Springs-Marietta, GA Metro Area	46,332
12	Houston-Sugar Land-Baytown, TX Metro Area	45,539
13	Sioux Falls, SD Metro Area	43,184
14	Dallas-Fort Worth-Arlington, TX Metro Area	40,085
15	Salt Lake City, UT Metro Area	39,087
16	Riverside-San Bernardino-Ontario, CA Metro Area	24,671

ProBank Education Services powered by **FORVIS**

138

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

138

2022 SAR Activity Distribution “Top 48” Metropolitan Filing Areas (out of 1,000+)

17	Cincinnati-Middletown, OH-KY-IN Metro Area	23,809
18	Cleveland-Elyria-Mentor, OH Metro Area	22,462
19	Boston-Cambridge-Quincy, MA-NH Metro Area	21,618
20	Phoenix-Mesa-Glendale, AZ Metro Area	20,193
21	Detroit-Warren-Livonia, MI Metro Area	19,153
22	Las Vegas-Paradise, NV Metro Area	17,579
23	Orlando-Kissimmee-Sanford, FL Metro Area	17,169
24	San Diego-Carlsbad-San Marcos, CA Metro Area	17,089
25	Seattle-Tacoma-Bellevue, WA Metro Area	17,073
26	Birmingham-Hoover, AL Metro Area	16,892
27	Tampa-St. Petersburg-Clearwater, FL Metro Area	15,503
28	Minneapolis-St. Paul-Bloomington, MN-WI Metro Area	13,085
29	San Jose-Sunnyvale-Santa Clara, CA Metro Area	13,027
30	San Juan-Caguas-Guaynabo, PR Metro Area	12,164
31	Baltimore-Towson, MD Metro Area	11,458
32	Denver-Aurora-Broomfield, CO Metro Area	11,010

ProBank Education Services powered by **FORVIS**

139

139

2022 SAR Activity Distribution “Top 48” Metropolitan Filing Areas (out of 1,000+)

33	Sacramento--Arden-Arcade--Roseville, CA Metro Area	9,900
34	Seaford, DE Micro Area	9,502
35	Buffalo-Niagara Falls, NY Metro Area	9,144
36	Fairmont, WV Micro Area	8,905
37	San Antonio-New Braunfels, TX Metro Area	8,550
38	Providence-New Bedford-Fall River, RI-MA Metro Area	8,137
39	New Orleans-Metairie-Kenner, LA Metro Area	8,122
40	Austin-Round Rock-San Marcos, TX Metro Area	7,893
41	Provo-Orem, UT Metro Area	7,813
42	Nashville-Davidson--Murfreesboro--Franklin, TN Metro Area	7,594
43	Memphis, TN-MS-AR Metro Area	7,548
44	Indianapolis-Carmel, IN Metro Area	7,545
45	Portland-Vancouver-Hillsboro, OR-WA Metro Area	7,030
46	Pittsburgh, PA Metro Area	6,989
47	Virginia Beach-Norfolk-Newport News, VA-NC Metro Area	6,576
48	Raleigh-Cary, NC Metro Area	6,336

ProBank Education Services powered by **FORVIS**

140

140

2022 SAR Activity Distribution – VA 163,488 (#05) + 56.94%

1	Credit/Debit Card	76,443	19.59%
2	ACH	43,117	11.05%
3	Identity Theft	40,319	10.33%
4	Provided Questionable or False Documentation	36,685	9.40%
5	Check	29,725	7.62%
6	Suspicion Concerning the Source of Funds	15,926	4.08%
7	Transaction(s) Below CTR Threshold	15,546	3.98%
8	Consumer Loan (see instructions)	14,767	3.78%
9	Transaction with No Apparent Economic, Business, or Lawful Purpose	13,045	3.34%
10	Suspicious EFT/Wire Transfers	10,996	2.82%
11	Transaction Out of Pattern for Customer(s)	10,412	2.67%
12	Other Fraud (Type)	10,219	2.62%

ProBank Education Services powered by **FORVIS**

141

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

141

2022 SAR Activity Distribution – VA 163,488 (#05) + 56.94%

13	Counterfeit Instrument	9,758	2.50%
14	Suspicious use of multiple transaction locations	7,442	1.91%
15	Suspicious Receipt of Government Payments/Benefits	6,237	1.60%
16	Two or More Individuals Working Together	6,158	1.58%
17	Account Takeover	5,546	1.42%
18	Business Loan	4,721	1.21%
19	Wire	4,143	1.06%
20	Elder Financial Exploitation	3,888	1.00%
21	Other Other Suspicious Activities	3,482	0.89%
22	Suspicious Use of Multiple Accounts	3,464	0.89%
23	Other Money Laundering	3,126	0.80%
24	Suspicious Use of Noncash Monetary Instruments	2,489	0.64%

ProBank Education Services powered by **FORVIS**

142

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

142

2022 SAR Activity Distribution – VA 163,488 (#05) + 56.94%

25	Forgeries	2,153	0.55%
26	Provided Questionable or False Identification	1,361	0.35%
27	Funnel Account	1,171	0.30%
28	Alters or Cancels Transaction to Avoid CTR Requirement	897	0.23%
29	Transaction(s) Involving Foreign High-Risk Jurisdiction	870	0.22%
30	Transaction(s) Below BSA Recordkeeping Threshold	754	0.19%
31	Other Structuring	688	0.18%
32	Against Financial Institution Customer(s)	549	0.14%
33	Refused or Avoided Request for Documentation	345	0.09%
34	Suspicious Inquiry by Customer Regarding Bsa Reporting or Recordkeeping Requirements	333	0.09%
35	Mass-Marketing	293	0.08%
36	Mail	275	0.07%

ProBank Education Services powered by **FORVIS**

143

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

143

2022 SAR Activity Distribution – VA 163,488 (#05) + 56.94%

43	Unlicensed or Unregistered MSB	145	0.04%
46	Human Smuggling	107	0.03%
47	Human Trafficking	104	0.03%
48	Against Financial Institution(s)	101	0.03%
55	Other Cyber Event	66	0.02%
62	Suspected Public/Private Corruption (Foreign)	18	0.00%
63	Known or Suspected Terrorist/Terrorist Organization	14	0.00%
66	Ponzi Scheme	10	0.00%
67	Suspected Public/Private Corruption (Domestic)	10	0.00%
69	Healthcare/Public or Private Health Insurance	9	0.00%
71	Pyramid Scheme	6	0.00%
73	Other Terrorist	4	0.00%

ProBank Education Services powered by **FORVIS**

144

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

144

2022 SAR Activity Distribution – VA “Top 15” Metropolitan Filing Areas

1	Washington-Arlington-Alexandria, DC-VA-MD-WV Metro Area	92,386
2	Richmond, VA Metro Area	58,184
3	Virginia Beach-Norfolk-Newport News, VA-NC Metro Area	6,576
4	Roanoke, VA Metro Area	1,117
5	Lynchburg, VA Metro Area	718
6	Charlottesville, VA Metro Area	486
7	Staunton-Waynesboro, VA Micro Area	458
8	Harrisonburg, VA Metro Area	394
9	Danville, VA Metro Area	350
10	Kingsport-Bristol-Bristol, TN-VA Metro Area	329
11	Martinsville, VA Micro Area	300
12	Blacksburg-Christiansburg-Radford, VA Metro Area	296
13	Winchester, VA-WV Metro Area	285
14	Bluefield, WV-VA Micro Area	202
15	Culpeper, VA Micro Area	123

ProBank Education Services powered by **FORVIS**

145

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

145

Current FinCEN SAR Focus Areas - School

- CRE Investments by Sanctioned Russians – 336 / 3-162
- Elder Financial Exploitation – 259 / 3-85
- Environmental Crimes – 309 / 3-135
- Hemp-Related Businesses – 232 / 3-58
- Human Smuggling along the S/W Border – 284 / 3-110
- Human Trafficking – 294 / 3-120
- Kleptocracy – 317 / 3-143
- Mail Theft-Related Check Fraud Schemes – 347 / 3-173
- Marijuana-Related Businesses – 225 / 3-51
- Online Child Sexual Exploitation – 305 / 3-131
- Ransomware – 239 / 3-65

ProBank Education Services powered by **FORVIS**

146

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

146



FinCEN

ALERT

FIN-2023-Alert003

February 27, 2023

FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-MAILTHEFT" and marking the check box for check fraud (SAR Field 34(d)).

In light of a nationwide surge in check fraud schemes targeting the U.S. Mail¹ (hereinafter "mail theft-related check fraud"), the Financial Crimes Enforcement Network (FinCEN) is issuing this alert to financial institutions² to be vigilant in identifying and reporting such activity. Mail theft-related check fraud generally pertains to the fraudulent negotiation of checks stolen from the U.S. Mail. Fraud, including check fraud, is the largest source of illicit proceeds in the United States and represents one of the most significant money laundering threats to the United States, as highlighted in the U.S. Department of the Treasury's most recent National Money Laundering Risk Assessment and

National Strategy for Combatting Terrorist and other Illicit Financing.³ Fraud is also one of the anti-money laundering/countering the financing of terrorism (AML/CFT) National Priorities.⁴

ProBank Education Services

powered by

FORVIS

147

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

147

Emerging Trends in Mail Theft-Related Check Fraud Schemes

Despite the declining use of checks in the United States,⁶ criminals have been increasingly targeting the U.S. Mail since the COVID-19 pandemic to commit check fraud.⁷ The United States Postal Service (USPS) delivers nearly 130 billion pieces of U.S. Mail every year to over 160 million residential and business addresses across the United States.⁸ From March 2020 through February 2021, the USPS received 299,020 mail theft complaints, which was an increase of 161 percent compared with the same period a year earlier.⁹ BSA reporting for check fraud has also increased in the past three years. In 2021, financial institutions filed more than 350,000 SARs to FinCEN to report potential check fraud, a 23 percent increase over the number of check fraud-related SARs filed in 2020. This upward trend continued into 2022, when the number of SARs related to check fraud reached over 680,000, nearly double the previous year's amount of filings.¹⁰

Mail Theft Risks and Vulnerabilities

Criminals committing mail theft-related check fraud generally target the U.S. Mail in order to steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits. Criminals will generally steal all types of checks in the U.S. Mail as part of a mail theft scheme, but business checks may be more valuable because business accounts are often well-funded and it may take longer for the victim to notice the fraud. There have been cases of Postal Service employees stealing checks at USPS sorting and distribution facilities.¹¹ However, according to USPS, mail theft-related check fraud is increasingly committed by non-USPS employees, ranging from individual fraudsters to organized criminal groups comprised of the organizers of the criminal scheme, recruiters, check washers, and money mules.

ProBank Education Services

powered by

FORVIS

148

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

148

Check Washers: Check washing involves the use of chemicals to remove the original ink on a check to replace the payee and often the dollar amount. Fraudsters may also copy and print multiple washed checks for future use or to sell to third-party criminals.¹²

Money Mules: A money mule is a person (whether witting or unwitting) who transfers or moves illicit funds at the direction of or on behalf of another.¹³

These criminals, located throughout the country, target USPS blue collection boxes, unsecured residential mailboxes, and privately owned cluster box units at apartment complexes, planned neighborhoods, and high-density commercial buildings. Mail theft can occur through forced entry or the use of makeshift fishing devices,¹⁴ and increasingly involves the use of authentic or counterfeit USPS master keys, known as Arrow Keys. Arrow Keys open USPS blue collection boxes and cluster box units within a geographic area, and a number of recent cases involve organized criminals violently targeting USPS mail carriers with the intent of stealing Arrow Keys.¹⁵ There have also been cases of corrupt Postal Service employees who unlawfully provide Arrow Keys to criminal actors to facilitate mail theft.¹⁶ Illicit actors may also copy and sell stolen Arrow Keys to third-party fraudsters on the dark web and through encrypted social media platforms in exchange for convertible virtual currency.

Financial Red Flags Relating to Mail Theft-Related Check Fraud

FinCEN, in coordination with USPIS, has identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to mail theft-related check fraud, many of which overlap with red flags for check fraud in general. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious or otherwise indicative of mail theft-related check fraud. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional due diligence where appropriate.

- 1 Non-characteristic large withdrawals on a customer's account via check to a new payee.
- 2 Customer complains of a check or checks stolen from the mail and then deposited into an unknown account.
- 3 Customer complains that a check they mailed was never received by the intended recipient.
- 4 Checks used to withdraw funds from a customer's account appear to be of a noticeably different check stock than check stock used by the issuing bank and check stock used for known, legitimate transactions.
- 5 Existing customer with no history of check deposits has new sudden check deposits and withdrawal or transfer of funds.
- 6 Non-characteristic, sudden, abnormal deposit of checks, often electronically, followed by rapid withdrawal or transfer of funds.
- 7 Examination of suspect checks reveals faded handwriting underneath darker handwriting, giving the appearance that the original handwriting has been overwritten.
- 8 Suspect accounts may have indicators of other suspicious activity, such as pandemic-related fraud.²⁰
- 9 New customer opens an account that is seemingly used only for the deposit of checks followed by frequent withdrawals and transfer of funds.
- 10 A non-customer that is attempting to cash a large check or multiple large checks in-person and, when questioned by the financial institution, provides an explanation that is suspicious or potentially indicative of money mule activity.

SAR Filing Instructions

FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this alert by including the key term “FIN-2023-MAILTHEFT” in SAR field 2 (“Filing Institution Note to FinCEN”), as well as in the narrative, and by selecting **SAR Field 34(d) (check fraud)**. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.

Mail Theft-Related Check Fraud Reporting Hotline for Victims

In addition to filing a SAR, as applicable, financial institutions should refer their customers who may be victims of mail theft-related check fraud to the USPIS at 1-877-876-2455 or <https://www.uspis.gov/report> to report the incident.

USPIS Tips to Prevent Mail Theft

FinCEN recommends as a best practice that financial institutions refer their customers to www.uspis.gov/tips-prevention/mail-theft for tips from the USPIS on how to protect against mail theft.

If customers appear to be a victim of a theft involving USPS money orders, refer them to <https://www.usps.com/shop/money-orders.htm> for guidance on how to replace a lost or stolen money order.

ProBank

151

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

151



FinCEN ADVISORY

FIN-2022-A002

June 15, 2022

Advisory on Elder Financial Exploitation

Amid rampant fraud and abuse targeting older adults, FinCEN urges financial institutions to detect, prevent, and report suspicious financial transactions.

Elder financial exploitation (EFE) is defined as the illegal or improper use of an older adult's funds, property, or assets.¹

SAR Filing Request: FinCEN requests that financial institutions reference the advisory by including “EFE FIN-2022-A002” in SAR field 2 (“Filing Institution Note to FinCEN”), and mark the check box for elder financial exploitation.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to the rising trend of EFE targeting older adults² and to highlight new EFE typologies and red flags since FinCEN issued the first EFE Advisory in 2011.³ FinCEN is also issuing this advisory in support of World Elder Abuse Awareness Day, which has been commemorated on June 15 every year since 2006 and provides an opportunity for communities around the world to promote a better understanding of abuse and neglect of older adults by raising awareness of the related cultural, social, economic, and demographic factors.⁴

According to the U.S. Department of Justice, elder abuse, which includes EFE among other forms of abuse, affects at least 10 percent of older adults each year in the United States,⁵ with millions of older adults losing more than \$3 billion to financial fraud annually as of 2019.⁶ Despite the

ProBank Education Services

powered by

FORVIS

152

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

152

fact that EFE is the most common form of elder abuse, the majority of incidents go unidentified and unreported as victims may choose not to come forward out of fear, embarrassment, or lack of resources.⁷ Older adults are targets for financial exploitation due to their income and accumulated life-long savings, in addition to the possibility that they may face declining cognitive or physical abilities, isolation from family and friends, lack of familiarity or comfort with technology, and reliance on others for their physical well-being, financial management, and social interaction.⁸ The COVID-19 pandemic exacerbated these vulnerabilities for many older adults.⁹ In 2020, over 62,000 suspicious activity reports (SARs) related to EFE were filed, totaling what the Consumer Financial Protection Bureau (CFPB) estimates to be \$3.4 billion in suspicious transactions, an increase from \$2.6 billion in 2019. This is the largest year-to-year increase since 2013.¹⁰ This trend has continued with over 72,000 SARs related to EFE filed in 2021 and, according to the Federal Trade Commission (FTC), older adults now account for 35 percent of the victims associated with filed fraud reports in cases when a consumer provided an age.¹¹

The U.S. government has multiple initiatives in place to counter perpetrators and facilitators of EFE.¹² In support of this whole-of-government approach, FinCEN collaborates with law enforcement, regulatory agencies, and financial institutions to ensure that SARs appropriately identify and report suspicious activity potentially indicative of EFE. Financial institutions are uniquely situated to detect possible financial exploitation through their relationships with older customers. They therefore play a critical role in helping to identify, prevent, and report EFE to law enforcement and their state-based Adult Protective Services,¹³ and any other appropriate first

responder as well as assisting older customers who fall victim to financial exploitation.¹⁴ The information contained in this advisory is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Trends and Typologies of EFE and Associated Payments

EFE schemes generally involve either theft or scams.¹⁵ Perpetrators of elder theft are often known and trusted persons of older adults, while scams, which can disproportionately affect older adults, frequently involve fraudsters, often located outside of the United States, with no known relationship to their victims.¹⁶ Regardless of the relationship, these criminals can place older adults in financially, emotionally, and physically compromising situations, and the resulting loss of income and life-long earnings can be devastating to the financial security, dignity, and quality of life of the victims.¹⁷

Elder Theft

Schemes involving the theft of an older adult's assets, funds, or income by a trusted person.

Elder Scams

Scams involving the transfer of money to a stranger or imposter for a promised benefit or good that the older adult did not receive.

Unfortunately, perpetrators of EFE schemes often do not stop after first exploiting their victims. In both elder theft and scams, older adults are often re-victimized and subject to potentially further financial loss, isolation, and emotional or physical abuse long after the initial exploitation due to the significant illicit gains at stake.¹⁸ Scammers may also sell victims' personally identifiable information (PII) on the black market to other criminals who continue to target the victims using new and emerging scam typologies.¹⁹

Elder Theft

Perpetrators of elder theft are often family members and non-family caregivers who abuse their relationship and position of trust. As identified by FinCEN in 2019 in its analysis of a statistically



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

**Consumer
Protection**

Data Spotlight

FTC reporting back to you

Data Spotlight

Romance scammers' favorite lies exposed

ProBank Education Services

powered by

FORVIS

155

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

155

By: Emma Fletcher | February 9, 2023

Romance scammers tell all sorts of lies to steal your heart and money, and reports to the FTC show those lies are working. Last year's romance scam numbers looked a lot like 2021 all over again, and it's not a pretty picture. In 2022, nearly 70,000 people reported a romance scam, and reported losses hit a staggering \$1.3 billion.^[1] The median reported loss: \$4,400.^[2]

These scammers pay close attention to the information you share, and don't miss a beat becoming your perfect match. You like a thing, so that's their thing, too. You're looking to settle down. They're ready too. But there is one exception – you want to meet in real life, and they can't. Reports show their excuse is often baked right into their fake identity. Claiming to be on a faraway military base is the most popular excuse, but "offshore oil rig worker" is another common (and fake) occupation. In short, there's no end to the lies romance scammers will tell to get your money.

ProBank Education Services

powered by

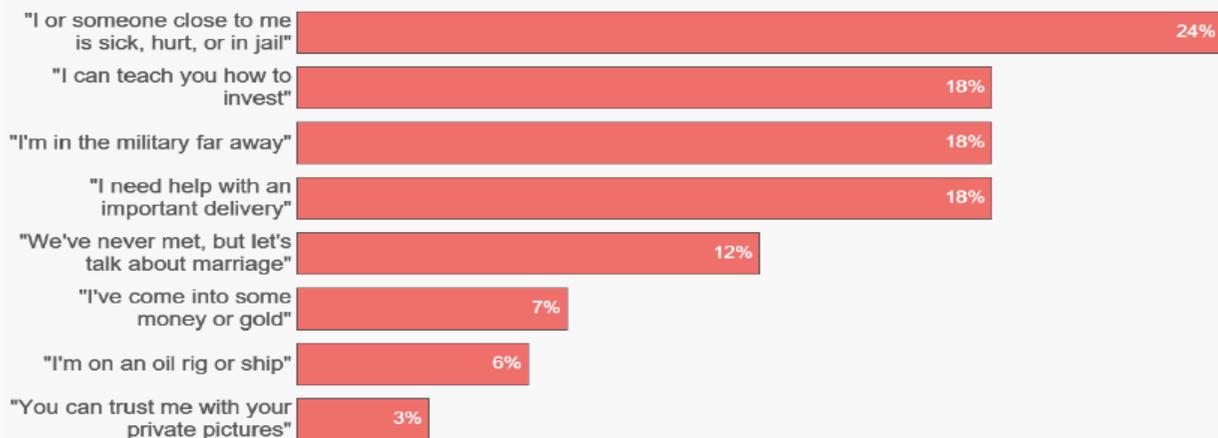
FORVIS

156

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

156

Romance Scammers: Their Favorite Lies by the Numbers



Figures are based on 8,070 2022 romance scam reports that indicated a dollar loss and included a narrative of at least 2,000 characters in length. Lies were identified using keyword analysis of the narratives.

ProBank Education Services powered by **FORVIS**

157

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

157

Reports show romance scammers often use dating apps to target people looking for love. But reports of romance scams that start with unexpected private messages on social media platforms are even more common. In fact, 40% of people who said they lost money to a romance scam last year said the contact started on social media; 19% said it started on a website or app.^[3] Many people reported that the scammer then quickly moved the sweet talk to WhatsApp, Google Chat, or Telegram.^[4]

You may have heard about romance scammers who tell you they're sick, hurt, or in jail – or give you another fake reason to send them money. But did you know that many romance scammers operate by offering to do *you* a favor? They may claim to be a successful cryptocurrency investor who'll teach you how it's done. But any money you "invest" goes straight into their wallet. In another twist, they might say they've shipped you a valuable package (not true), which requires you to send money for "customs" or some other made-up fee. It's all a lie. You send the money, and the package never turns up.

ProBank Education Services powered by **FORVIS**

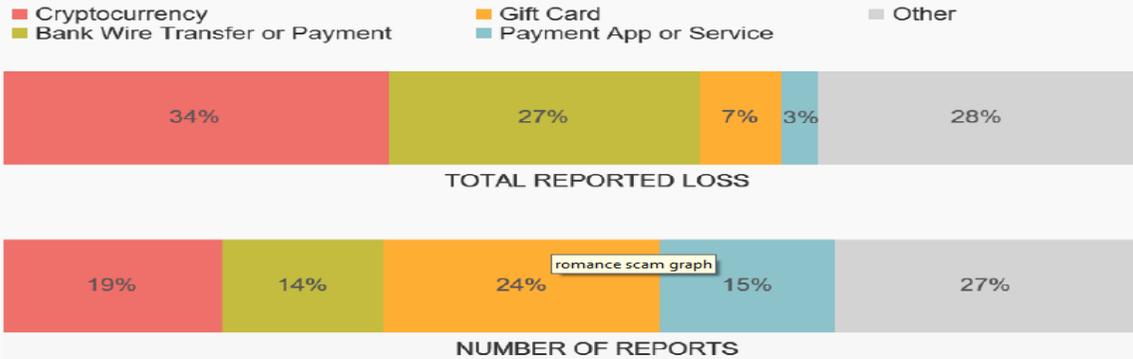
158

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

158

Top payment methods on romance scams in 2022

The largest aggregate reported dollar losses were in cryptocurrency, but more people reported paying with gift cards than any other method.



Figures exclude reports that did not indicate a payment method and reports contributed by MoneyGram and Western Union. The gift card payment method includes cards that hold a specific cash value that can be used for purchases and reload cards such as MoneyPak that are used to add value to these cards.

Reports also show that scammers who convince you to share explicit photos will then threaten to share them with your social media contacts. It's called sextortion, and these reports have increased more than eightfold since 2019. ^[5] People aged 18-29 were over six times as likely to report sextortion than people 30 and over. ^[6] About 58% of 2022 sextortion reports identified social media as the contact method, ^[7] with Instagram and Snapchat topping the list. ^[8]

The way romance scammers take your money is another important piece of the story. People reported sending more money to romance scammers using cryptocurrency and bank wires than any other method: together, they accounted for more than 60% of reported losses to romance scams in 2022. ^[9] While not the costliest payment method, ^[10] gift cards were the most frequently reported – 24% of people who reported losing money to a romance scam in 2022 said it was taken using gift cards. ^[11]

So how can you spot a romance scammer in the act?

- Nobody legit will ever ask you to help—or insist that you invest— by sending cryptocurrency, giving the numbers on a gift card, or by wiring money. Anyone who does is a scammer.
- If someone tells you to send money to receive a package, you can bet it's a scam.
- Talk to friends or family about a new love interest and pay attention if they're concerned.
- Try a reverse image search of profile pictures. If the details don't match up, it's a scam.

Help stop scammers by reporting suspicious profiles or messages to the dating app or social media platform. Then, tell the FTC at [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov). If someone is trying to extort you, [report it to the FBI](https://www.fbi.gov). Learn more at [ftc.gov/romancescams](https://www.ftc.gov/romancescams).

Behavioral Red Flags

Victims of EFE may have limited and irregular contact with others. For some, their only outside contact may involve visiting or communicating with their local financial institution, including at the bank branch, check-cashing counter, or MSB. Therefore, it is critical for customer-facing staff to identify and consider the behavioral red flags when conducting transactions involving their older customers, particularly suspicious behavior that also involves the financial red flags highlighted below. Such information should be incorporated into SAR filings and reported to law enforcement as appropriate. Financial institutions are reminded that behavioral red flags of EFE and the names of staff who witnessed them should be included in the SAR narrative to assist future law enforcement investigations. Behavioral red flags of EFE may include:

- 1 An older customer's account shows sudden and unusual changes in contact information or new connections to emails, phone numbers, or accounts that may originate overseas.
- 2 An older customer with known physical, emotional, and cognitive impairment has unexplainable or unusual account activity.
- 3 An older customer appears distressed, submissive, fearful, anxious to follow others' directions related to their financial accounts, or unable to answer basic questions about account activity.
- 4 An older customer mentions how an online friend or romantic partner is asking them to receive and forward money to one or more individuals on their behalf or open a bank account for a "business opportunity."
- 5 During a transaction, an older customer appears to be taking direction from someone with whom they are speaking on a cell phone, and the older customer seems nervous, leery, or unwilling to hang up.
- 6 An older customer is agitated or frenzied about the need to send money immediately in the face of a purported emergency of a loved one, but the money would be sent to the account of a seemingly unconnected third-party business or individual.
- 7 A caregiver or other individual shows excessive interest in the older customer's finances or assets, does not allow the older customer to speak for himself or herself, or is reluctant to leave the older customer's side during conversations.
- 8 An older customer shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker.
- 9 The financial institution is unable to speak directly with the older customer, despite repeated attempts to contact him or her.
- 10 A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of an older customer without proper documentation.

17 An older customer's financial management changes suddenly, such as through a change of power of attorney, trust, or estate planning vehicles, to a different family member or a new individual, particularly if such changes appear to be done under undue influence, coercion, or forgery or the customer has diminished cognitive abilities and is unable to agree to or understand the consequences of the new arrangement.

18 An older customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

Financial Red Flags

Identification of financial red flags of EFE and the associated payments are critical to detecting, preventing, and reporting suspicious activity potentially indicative of EFE. In addition to the financial red flags set out in DOJ and CFPB notices,⁴⁹ financial red flags of EFE may include:

- 18** Dormant accounts with large balances begin to show constant withdrawals.
- 18** An older customer purchases large numbers of gift cards or prepaid access cards.
- 18** An older customer suddenly begins discussing and buying CVC.
- 18** An older customer sends multiple checks or wire transfers with descriptors in the memo line such as "tech support services," "winnings," or "taxes."
- 18** Uncharacteristic, sudden, abnormally frequent, or significant withdrawals of cash or transfers of assets from an older customer's account.
- 18** An older customer receives and transfers money interstate or abroad to recipients with whom they have no in-person relationship, and the explanation seems suspicious or indicative of a scam or money mule scheme.
- 19** Frequent large withdrawals, including daily maximum currency withdrawals from an ATM.
- 20** Sudden or frequent non-sufficient fund activity.
- 21** Uncharacteristic nonpayment for services, which may indicate a loss of funds or of access to funds.
- 22** Debit transactions that are inconsistent for the older customer.
- 23** Uncharacteristic attempts to wire large sums of money.
- 24** Closing of CDs or accounts without regard to penalties.

SAR Filing Instructions

When filing a SAR, financial institutions should provide all pertinent available information about the activity in the SAR form and narrative. Reporting on how perpetrators of EFE communicate with and target older adults is also useful to law enforcement investigations. FinCEN requests that financial institutions reference this advisory by including the key term below in SAR field 2 ("Filing Institution Note to FinCEN") and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

"EFE FIN-2022-A002"

Financial institutions that suspect EFE activity should also mark the check box for Elder Financial Exploitation (SAR Field 38(d)). FinCEN first added an "Elder Financial Exploitation" checkbox to the SAR Form in 2012 and encourages financial institutions to mark the box when filing an EFE-related SAR. For authorized federal, state, and local law enforcement, the checkbox makes it easier to locate and analyze BSA data related to EFE as detailed above.

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.⁵²

Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this advisory may call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).⁵³

Filers are reminded, as stated in FinCEN's Electronic Filing Instructions, that the narrative section of the report is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators. Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion.⁵⁴ Filers are also encouraged to determine their obligations to report suspected EFE under state law and report suspected EFE to law enforcement and their state-based Adult Protective Services.

FinCEN notes that the tips below are best practices in regard to filing a SAR for suspected EFE and are not regulatory obligations:

- Provide a statement in the narrative documenting the age and location (county/city) of the target or victim. Provide details about the reporting entity's response, e.g., whether accounts were closed, whether the person was warned that transactions appear to involve fraud, if the person was not permitted to conduct new transactions, etc.
- Provide details about the amounts involved and whether any amounts were refunded to the older customer (as of the submission date of the SAR).
- Reference supporting documentation, including any photos or video footage, in the narrative.
- Cross-report the circumstances leading to the filing of EFE SARs directly to local law enforcement if there is any indication that a) a crime may have been committed and/or b) the older adult may still be at risk for victimization by the suspected abuser. Filers should note that the filing of a SAR is not a substitute for any requirement in a given state to report suspected EFE to law enforcement and Adult Protective Services.
- Take advantage of the law enforcement contact field to indicate if the suspicious activity was also reported to law enforcement or Adult Protective Services, as well as the name and phone number of the contact person.
- Provide direct liaisons or points of contact at the reporting entity related to the SAR so investigators can ask questions and request additional documentation in a timely manner.
- Expedite responses to law enforcement requests for supporting documents.⁵⁵

Other U.S. Government EFE Reporting Options

In addition to filing a SAR, financial institutions should refer their older customers who may be a victim of EFE to the DOJ's [National Elder Fraud Hotline](#) at 833-FRAUD-11 or 833-372-8311 for support, resources, and assistance with reporting suspected fraud to the appropriate government agencies. Filers should immediately report any imminent threat or physical danger to their local FBI office or local law enforcement. FinCEN encourages filers to collaborate with other stakeholders in their communities to enhance responses and engage in professional training opportunities, community education prevention, and awareness activities and initiatives.⁶⁴ Filers can find whether there is an existing collaboration on elder fraud prevention and response in their area by contacting Adult Protective Services or their local Area Agency on Aging.⁶⁵

For Further Information

Questions regarding the contents of this advisory should be addressed to the FinCEN Resource Center at frc@fincen.gov.

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.

ProBank Education Services

powered by

FORVIS

167

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

167



FinCEN ADVISORY

FIN-2022-A001

April 14, 2022

Advisory on Kleptocracy and Foreign Public Corruption

FinCEN urges financial institutions to focus efforts on detecting the proceeds of foreign public corruption, a priority for the U.S. government.

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: "**CORRUPTION FIN-2022-A001**" and selecting SAR field 38(m). Additional guidance on filing SARs appears near the end of this advisory.

Corruption includes the abuse of authority or official position to extract personal gain. Corruption corrodes public trust; hobbles effective governance; undercuts development efforts; contributes to national fragility, extremism, and migration; and provides authoritarian leaders a means to undermine democracies worldwide.⁵

Introduction

Last year, President Biden established the fight against corruption as a core national security interest.¹ The proceeds of foreign public corruption travel across national borders and can affect economies and political systems far from the origin of the proceeds.² Foreign public corruption disproportionately harms the most vulnerable in societies, often depriving these populations of critical public services. In the United States, the proceeds of foreign public corruption can distort our markets, taint our financial system, and can erode public trust in government institutions.³ Foreign public corruption can also violate U.S. law.⁴

Kleptocratic regimes and corrupt public officials may engage in bribery, embezzlement, extortion, or the misappropriation of public assets, among other forms of corrupt behavior, to advance their strategic, financial, and personal goals. In doing so, they may exploit the U.S. and international financial systems to launder illicit gains, including through the use of shell companies, offshore financial centers, and professional service providers who enable the movement and laundering

ProBank Education Services

powered by

FORVIS

168

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

168

A **kleptocracy** is a government controlled by officials who use political power to appropriate the wealth of their nation for personal gain, usually at the expense of the governed population.

A **kleptocrat** uses their position and influence to enrich themselves and their networks of corrupt actors.

of illicit wealth, including in the United States and other rule-of-law-based democracies.⁶ These practices harm the competitive landscape of financial markets and often have long-term corrosive effects on good governance, democratic institutions, and human rights standards.⁷

Russia is of particular concern as a kleptocracy because of the nexus between corruption, money laundering, malign influence and armed interventions abroad, and sanctions evasion. Corruption is widespread throughout the Russian government and manifests itself as bribery of officials, misuse of budgetary resources, theft of government property, kickbacks in the procurement process, extortion, and

improper use of official positions to secure personal profits.⁸ Russia's further invasion of Ukraine, for example, highlights foreign public corruption perpetrated by kleptocratic regimes like that of Russian President Vladimir Putin.⁹ Russia's actions in Ukraine are supported and enabled by Russia's elites and oligarchs who control a majority of Russia's economic interests.¹⁰ These individuals have a mutually beneficial relationship with President Putin that allows them to misappropriate assets from the Russian people while helping President Putin maintain his tight control on power.¹¹ Oligarchs are believed to be directly financing off-budget projects that include political malign influence operations and armed interventions abroad.¹² The U.S. government has imposed sanctions on many of these individuals and the businesses and state-owned entities they

control as part of U.S. efforts to hold President Putin and his supporters accountable for Russia's further invasion of Ukraine, and to restrict their access to assets to finance Russia's destabilizing activities globally.¹³

This advisory provides financial institutions with typologies and potential indicators associated with kleptocracy and other forms of foreign public corruption, namely bribery, embezzlement, extortion, and the misappropriation of public assets.

FINCEN ADVISORY

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.⁴¹ Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.⁴² When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML/CFT program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SARs and OFAC Sanctions

Longstanding FinCEN guidance⁴³ provides clarity regarding when a financial institution must satisfy its obligation to file a SAR on a transaction involving a designated person when also filing a blocking report with OFAC. Relatedly, ransomware attacks and payments on which financial institutions file SARs should also be reported to OFAC at OFAC_Feedback@treasury.gov if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment.

SAR Filing Instructions

FinCEN requests that financial institutions reference this alert by including the key term "CORRUPTION FIN-2022-A001" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this alert. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.⁴⁴



FinCEN

ALERT

FIN-2023-Alert002

January 25, 2023

FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies

The Financial Crimes Enforcement Network (FinCEN) is issuing this alert to all financial institutions¹ regarding potential investments in the U.S. commercial real estate (CRE) sector by sanctioned Russian elites, oligarchs, their family members, and the entities through which they act (collectively, “sanctioned Russian elites and their proxies”).² In March 2022, FinCEN issued an alert on the risk of sanctions evasion by sanctioned Russian elites and their proxies involving high-value assets, including both residential and commercial real estate.³ This alert specifically highlights sanctions evasion-related vulnerabilities in the CRE sector and is based on a review of Bank Secrecy Act (BSA) reporting indicating that sanctioned Russian elites and their proxies may exploit them to evade sanctions.⁴

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: “FIN-2023-RUSSIACRE”.

ProBank Educa

171

171

Sanctions Evasion Risks and Vulnerabilities in the Commercial Real Estate Market

FinCEN assesses that sanctioned Russian elites and their proxies are likely attempting to exploit several vulnerabilities in the CRE market in order to evade sanctions. The CRE market presents unique challenges for financial institutions in detecting sanctions evasion. First, CRE transactions routinely involve highly complex financing methods and opaque ownership structures that can make it relatively easy for bad actors to hide illicit funds in CRE investments. For example, CRE transactions nearly always involve private companies or institutional investors as the buyer and/or seller. As such, trusts, shell companies, pooled investment vehicles, or other legal entities are regularly used on both sides of CRE transactions. The standard use of such legal entities in CRE deals is typically due to the high value of the properties (ranging from the low millions of dollars to the billions of dollars) and the need for buyers and sellers to limit their legal, tax, and financial liability. In addition, several layers of legal entities are frequently involved as CRE buyers or sellers, and they may be domiciled in offshore jurisdictions. Further, these legal entities often have a large number of investors behind them and, as a result, it can be difficult for a financial institution to identify all of the beneficial owners. As discussed further below and based on BSA reporting, sanctioned Russian elites and their proxies may seek to further obfuscate their involvement in a CRE transaction by decreasing their percentage of ownership in an investment below the threshold set by a bank’s CDD protocols.

ProBank Educ

172

172

SAR Filing Instructions

FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this alert by including the key term "FIN-2023-RUSSIACRE" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.

Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).²⁹

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.³⁰

ProBank Educ

FORVIS is a trademark of FORVIS

173

173



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/CFT) 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

ProBank Education Services

powered by

FORVIS

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

174

174

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.

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

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.



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.

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

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

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

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.

- 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.

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



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

ProBank Education Services

powered by

FORVIS

183

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

183

Cooperation with OFAC and Law Enforcement

Another factor that OFAC will consider under the Enforcement Guidelines is the reporting of ransomware attacks to appropriate U.S. government agencies and the nature and extent of a subject person's cooperation with OFAC, law enforcement, and other relevant agencies, including whether an apparent violation of U.S. sanctions is voluntarily self-disclosed. In the case of ransomware payments that may have a sanctions nexus, OFAC will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, such as CISA or the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response. OFAC will also consider a company's full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible — to be a significant mitigating factor.

While the resolution of each potential enforcement matter depends on the specific facts and circumstances, OFAC would be more likely to resolve apparent violations involving ransomware attacks with a non-public response (i.e., a No Action Letter or a Cautionary Letter) when the affected party took the mitigating steps described above, particularly reporting the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation.

OFAC Licensing Policy

Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will continue to be reviewed by OFAC on a case-by-case basis with a presumption of denial.

Victims of Ransomware Attacks Should Contact Relevant Government Agencies

OFAC strongly encourages all victims and those involved with addressing ransomware attacks to report the incident to CISA, their local FBI field office, the FBI Internet Crime Complaint Center, or their local U.S. Secret Service office as soon as possible. Victims should also report ransomware attacks and payments to Treasury's OCCIP and contact OFAC if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment. As noted, in doing so victims can receive significant mitigation from OFAC when determining an appropriate enforcement response in the event a sanctions nexus is found in connection with a ransomware payment.

¹ See the U.S. government's website, <https://www.cisa.gov/stopransomware>, for additional guidance.

-5-

ProBank Education Services

powered by

FORVIS

184

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

184

By reporting ransomware attacks as soon as possible, victims may also increase the likelihood of recovering access to their data through other means, such as alternative decryption tools, and in some circumstances may be able to recover some of the ransomware payment. Additionally, reporting ransomware attacks and payments provides critical information needed to track cyber actors, hold them accountable, and prevent or disrupt future attacks.

Contact Information for U.S. Department of Treasury Agencies:

- U.S. Department of the Treasury's Office of Foreign Assets Control
 - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
 - Licensing Division: <https://licensing.ofac.treas.gov/>; (202) 622-2480
- U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
 - OCCIP-Coord@treasury.gov; (202) 622-3600
- U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)
 - FinCEN Regulatory Support Section: fincen.gov

Contact Information for Other Relevant U.S. Government Agencies:

- Federal Bureau of Investigation Cyber Task Force
 - <https://www.ic3.gov/default.aspx>; www.fbi.gov/contact-us/field
- U.S. Secret Service Cyber Fraud Task Force
 - <https://secretsservice.gov/contact-field-offices>
- Cybersecurity and Infrastructure Security Agency
 - <https://us-cert.cisa.gov/forms/report>
- Homeland Security Investigations Field Office
 - <https://www.ice.gov/contact/hsi>

Ransomware Prevention Resources:

- U.S. Government StopRansomWare.gov Website
 - <https://www.cisa.gov/stopransomware>
- CISA Ransomware Guide
 - <https://www.cisa.gov/stopransomware/ransomware-guide>

If you have any questions regarding the scope of any sanctions requirements described in this advisory, please contact OFAC's Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490.



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

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.

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.

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.



FinCEN

ALERT

FIN-2023-Alert001

January 13, 2023

FinCEN Alert on Human Smuggling along the Southwest Border of the United States

The Financial Crimes Enforcement Network (FinCEN) is issuing this alert to better aid financial institutions in the detection of financial activity related to human smuggling along the U.S. southwest border ("SW border").¹ Human smugglers engage in the crime of transporting people across international borders through deliberate evasion of immigration laws, often for financial

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference the alert by including "FIN-2023-HUMANSMUGGLING" in SAR field 2 ("Filing Institution Note to FinCEN") and selecting human smuggling (SAR Field 38(g)). Additional guidance on filing SARs appears near the end of the alert.

benefit.² Human smuggling can endanger lives and have devastating consequences because criminal organizations involved in human smuggling value profit over human life.³ This alert builds upon FinCEN's previous 2014 and 2020 human smuggling and human trafficking advisories,⁴ while providing trends and typologies specifically related to human smuggling occurring along the SW border. This alert also provides red flag indicators to help financial institutions better identify transactions potentially related to human smuggling and reminds financial institutions of their Bank Secrecy Act (BSA) reporting obligations. It further supports ongoing initiatives by the U.S. Government to combat human smuggling and human trafficking.⁵ Human smuggling

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

and human trafficking are also included in FinCEN's anti-money laundering and countering the financing of terrorism priorities (AML/CFT) published in June 2021.⁶

Human Smuggling: Acts or attempts to bring unauthorized persons to or into the United States, transport them within the United States, harbor unauthorized persons, encourage entry of unauthorized persons, or conspire to commit these violations, knowingly or in reckless disregard of illegal status.⁷

Human Trafficking: The recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting a person for the purpose of a commercial sex act (sex trafficking), in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age, or the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery (forced labor).⁸

The information contained in this alert is derived from FinCEN's analysis of BSA data, open-source reporting, and information provided by law enforcement partners.

How Human Smuggling Networks Operate

Smuggling operations along the SW border are typically conducted by networks of smaller groups and organizations that perform different functions along smuggling routes. These networks can be extensive and complex and include individuals who may, among other functions, organize the initial travel arrangements, facilitate lodging, and provide services to guide or facilitate the actual crossing of the SW border. These networks often are associated in some way with transnational criminal organizations (TCO), such as drug cartels that "control" territory through which smuggling operations take place. These associations range from the smuggling networks paying a portion of their illicit gains as a "protection tax" to a TCO for safe passage to more direct involvement by the TCO in the day-to-day operations of the smuggling networks.²³

Human Smuggling and Organized Crime

In November 2020, the United States, in coordination with El Salvador, Guatemala, and Honduras, arrested 36 individuals and issued criminal charges against hundreds of individuals involved in a human smuggling operation controlled by MS-13 and the 18th Street Gang. These TCOs are also suspected of being involved with a number of other crimes, including human trafficking, narcotics trafficking, and murder.²⁴

Human smuggling involves two main phases: solicitation and transportation.²⁵ During the solicitation phase, smugglers advertise their services, for example, by posing as seemingly legitimate businesses such as travel agencies or work recruiters, and build trust with migrants seeking smuggling services. Smugglers acting in a solicitation role will often share the same national origin or related ethnic background as the migrants they smuggle.²⁶ Historically, much of the solicitation was done by word of mouth, but with the rapid development of social media and other technology, smugglers have been able to leverage various platforms to reach a broader audience and potential pool of migrants.²⁷

During the transportation phase, smuggling networks often use social media platforms—particularly those that offer end-to-end encrypted communication—to coordinate along the route.²⁸ Smugglers have also been using social media to recruit third parties to serve as part of the smuggling operation along the SW border. One example involves the recruitment of unaffiliated truck drivers based in the United States to smuggle migrants across the SW border. This is advantageous to the smuggling networks because crossing the SW border presents one of the largest risks of apprehension by law enforcement associated with the journey. By contracting out this portion of the operation to third parties, smuggling networks insulate themselves to a degree because these contracted individuals lack knowledge of the network’s operations or chain-of-command.

Illicit Finance Typologies

As previously reported in FinCEN’s 2014 Advisory, migrants generally pay smugglers in one of three ways: 1) payment in advance, in which the migrant or the migrant’s relatives provide full payment to the smuggler before traveling; 2) partial payment, in which a migrant pays some portion upon departure and the remaining balance is paid in full upon arrival, and 3) payment on arrival, in which the migrant’s relatives pay the full fee to the smuggler after the migrant is successfully smuggled.²⁹ These payments are still primarily conducted in cash, but the use of wire transfers is also common. Migrants who cannot afford full payment might also enter into work agreements with the smugglers to assist along the smuggling route or upon arrival to the United States. However, migrants who cannot afford full payment, are unable to pay any outstanding debt upon arrival in the United States or do not voluntarily enter into work agreements may be vulnerable to human trafficking, to include commercial sex trafficking, forced labor, fraud, kidnapping, and other forms of exploitation, once within the United States.³⁰

The methodologies used by human smuggling networks to launder their illicit gains remain largely the same as previously reported.³¹ Because human smuggling is often tied to larger criminal organizations, these often overlap with money laundering methods used by TCOs.

- *Cash Placement and Layering into the Formal Financial System:* Cash is still the primary method migrants use to pay smugglers.³² Smuggling networks often engage in bulk cash smuggling³³ and, among other money laundering methods, also engage in cash purchases of high-value assets, including real estate and businesses.³⁴ In some cases, smugglers avoid

depositing their cash proceeds into a financial institution and instead use them to finance their living expenses, to purchase luxury items, or to support their drug or gambling habits.³⁵ For example, in 2021, the DOJ indicted members of a human smuggling network alleged to have reaped more than \$200 million from a human smuggling scheme that exploited migrants for labor. This network allegedly laundered the funds through cash purchases of land, homes, vehicles, and businesses; and by funneling millions of dollars through casinos.³⁶

- **Funnel Accounts:** Smuggling fees, often paid by the family members of migrants already settled in the United States and disguised as remittances, are sent to funnel accounts at financial institutions with branches or locations along both sides of the SW border.³⁷ Smuggling networks may seek to establish accounts with financial institutions with a large U.S. presence to allow for easy collection of payments from the families of those being smuggled and who may be located throughout the United States.
- **Alternative Payment Methods:** In addition to payment via cash, human smugglers also use mobile payment applications and other forms of peer-to-peer (P2P) networks to transfer funds. For example, smugglers may use P2P networks to collect payments from migrants to cover the expenses necessary for their travel from the country of origin to their final destination.

Financial Red Flag Indicators of Human Smuggling

FinCEN has identified the following financial red flag indicators to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with human smuggling. Because no single financial red flag indicator is determinative 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.

- 1** Transactions involving multiple wire transfers, cash deposits, or P2P payments from multiple originators from different geographic locations either across (1) the United States, or (2) Mexico and Central America, to one beneficiary located on or around the SW border, with no apparent business purpose.
- 2** Deposits made by multiple individuals in multiple locations into a single account, not affiliated with the account holder's area of residence or work, with no apparent business purpose.
- 3** Currency deposits into U.S. accounts without explanation, followed by rapid wire transfers to countries with high migrant flows (e.g., Mexico, Central America), in a manner that is inconsistent with expected customer activity.

- 4 Frequent exchange of small-denomination for larger-denomination bills by a customer who is not in a cash-intensive industry.
- 5 Multiple customers sending wire transfers to the same beneficiary (who is not a relative, and may be located in the sender's home country), inconsistent with the customer's usual business activity and reported occupation.
- 6 A customer making significantly greater deposits—including cash deposits—than those of peers in similar professions or lines of business.
- 7 A customer making cash deposits that are inconsistent with the customer's line of business.
- 8 Extensive use of cash to purchase assets, such as real estate, and to conduct transactions.

SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.⁴¹ When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this alert by including the key term "**FIN-2023-HUMANSMUGGLING**" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative, and by selecting SAR field 38(g) (human smuggling). Financial institutions that suspect human trafficking activity should also select SAR field 38(h) (human trafficking) and highlight other advisory or alert keywords in the narrative, if applicable.

Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).⁴²

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.⁴³



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(b) (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

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.

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,²⁹ 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.

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.

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
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.

BSA Expectations Regarding Marijuana-Related Businesses FinCEN Guidance 2014-G001 (02/14/14)

- Guidance issued to clarify BSA expectations for DFIs seeking to provide services to marijuana-related businesses. This guidance clarifies “how” (in FinCEN’s mind) DFIs can provide services to marijuana-related businesses consistent with their BSA obligations, and aligns the information provided by DFIs in BSA reports with federal and state law enforcement priorities.
- “The Decision to open, close, or refuse any particular account or relationship should be made by each DFI based on a number of factors specific to that DFI”.
- 3 SAR Filings required under this Guidance:
 - “*Marijuana-Limited*” – identifies the dealer;
 - “*Marijuana-Priority*” – dealer violates one of the “*Cole memo*” priorities;
 - “*Marijuana-Termination*” – when DFI terminates the account relationship with the marijuana dealer.

(It should be noted that both the ABA and ICBA have come out with statements indicating that the FinCEN guidance is not definitive guidance nor indemnification should a DFI opt to service one of these businesses involved in an activity that is still a violation of Federal law).

For Release at 10:00 a.m. ET

December 3, 2019

Agencies Clarify Requirements for Providing Financial Services to Hemp-Related Businesses

WASHINGTON—Four federal agencies in conjunction with the state bank regulators today issued a statement clarifying the legal status of hemp growth and production and the relevant requirements under the Bank Secrecy Act (BSA) for banks providing services to hemp-related businesses.

The statement emphasizes that banks are no longer required to file suspicious activity reports (SAR) for customers solely because they are engaged in the growth or cultivation of hemp in accordance with applicable laws and regulations. For hemp-related customers, banks are expected to follow standard SAR procedures, and file a SAR if indicia of suspicious activity warrants.

This statement provides banks with background information on the legal status of hemp, the U.S. Department of Agriculture's (USDA) interim final rule on the production of hemp, and the BSA considerations when providing banking services to hemp-related businesses.

This statement also indicates that the Financial Crimes Enforcement Network (FinCEN) will issue additional guidance after further reviewing and evaluating the USDA interim final rule.

The statement was issued by the Federal Reserve Board, the Federal Deposit Insurance Corporation, FinCEN, the Office of the Comptroller of the Currency and the Conference of State Bank Supervisors. Banks can contact the USDA, state departments of agriculture, and tribal governments with further questions regarding the Agriculture Improvement Act of 2018 (2018 Farm Bill) and its implementing regulations.

ProBank Education Services

powered by

FORVIS

205

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

205

MANUAL EXAMINATION

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.

ProBank Education Services

powered by

FORVIS

206

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

206

FFIEC
SA AML 1000a

MANUAL EXAMINATION PROCEDURES REFERENCES FFIEC HOME

BSA/AML INFOBASE MANUAL

Quickly access all the sections of the BSA/AML Manual

1 INTRODUCTION

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

[1](#) [2](#)

SCOPING AND PLANNING

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

[1](#) [2](#) [3](#)

BSA/AML RISK ASSESSMENT

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

[1](#) [2](#) [3](#)

ASSESSING THE BSA/AML COMPLIANCE PROGRAM

Guidance to examiners on assessing the bank's BSA/AML compliance program.

[1](#) [2](#) [3](#)

DEVELOPING CONCLUSIONS AND FINALIZING THE EXAM

Guidance to examiners on developing conclusions and finalizing the examination.

[1](#) [2](#) [3](#)

ASSESSING COMPLIANCE WITH BSA REGULATORY REQUIREMENTS

Guidance to examiners on assessing compliance with other statutory and regulatory BSA requirements.

[1](#) [2](#) [3](#)

OFFICE OF FOREIGN ASSETS CONTROL

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

[1](#) [2](#) [3](#)

PROGRAM STRUCTURES

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

[1](#) [2](#) [3](#)

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.

[1](#) [2](#) [3](#)

ProBank Education Services powered by **FORVIS**

207

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

207

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"> Customer Due Diligence 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"> Table of Contents Scoping and Planning BSA/AML Risk Assessment Assessing the BSA/AML Compliance Program 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"> Assessing Compliance with Bank Secrecy Act Regulatory Requirements Customer Identification Program Currency Transaction Reporting 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"> Purchase and Sale of Monetary Instruments Recordkeeping Special Measures Reports of Foreign Financial Accounts 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"> Introduction – Customers Charities and Nonprofit Organizations Independent Automated Teller Machine Owners or Operators 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

ProBank Education Services powered by **FORVIS**

208

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

208

<ul style="list-style-type: none"> Introduction Scoping and Planning BSA/AML Risk Assessment Assessing the BSA/AML Compliance Program Developing Conclusions and Finalizing the Exam Assessing Compliance with BSA Regulatory Requirements Office of Foreign Assets Control Program Structures Risks Associated with Money Laundering and Terrorist Financing Appendices 	Assessing Compliance with BSA Regulatory Requirements				
	Sections	View	Download	Multiple	Examination Procedures
	Introduction (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
	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	
ProBank Education Services powered by FORVIS					
209					

209

	Risks Associated with Money Laundering and Terrorist Financing				
	Sections	View	Download	Multiple	Examination Procedures
	Introduction - Customers (2021)	Online	PDF (.pdf)	<input type="checkbox"/>	Not Applicable
	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	
ProBank Education Services powered by FORVIS					
210					

210

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

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

211

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

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

212

**Pacific National Bank, Miami FL
FinCEN Enforcement Action 2011- 5
OCC Consent Order 2011- 021 (3/24/11)**

- FinCEN and the OCC have assessed a \$7 Million CMP against this \$355 Million Asset DFI, a subsidiary of the Central Bank of Ecuador.
- OCC issued Consent Order in 12/2005 for multiple BSA “failures”, and despite FinCEN notifications, the bank failed to make the necessary corrections.
- The former President & CEO, as well as the Chairman of the Board were personally fined @ \$12,500, and three outside directors were personally fined @ \$ 8,500 for failing to ensure that the bank complied with the 2005 consent order.

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.

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), R 11 (Consumer advises authorized but not correct), R29 (Corporate Client advises not authorized), & R51 (Ineligible RCK item), where return rate exceeds 0.5%.

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.

“Tidbits” from Lexington ‘22

- Regulatory Panel consisting of three federal examiners and one State of KY bank examiner shared their thoughts with attendees in June 2022:
 - 314a – with vacation “season” upon us, make sure staff is covering 314as, not just regular, but any specials that may be released – important to document the scrub “event” and have the BSA Officer sample test just to be sure software is reliable – remember, banks and savings and loans can have up to four points of contact for 314a – both FDIC and FRB;
 - Staffing levels, and levels of expertise – backup and succession planning lacking or non-existent – biggest weakness identified by the OCC, also mentioned by State – State examiner made the point that implementing AML/Risk Management software will NOT reduce staff – what may have been an adequate level of staff in the past may not hold true today;
 - Lack of Independence of the BSA Officer, especially in the smaller community banks – BSA Officer not “doing” the Board reporting (OCC comment) – Board must be “in the loop” as they are ultimately responsible, and personally liable;

“Tidbits” from Lexington ‘22 (cont.)

- CDD – in some cases, documentation lacking supporting assigned risk ratings – not mapping actual vs expected and explaining the differences – OCC called it “elevator analysis” (data without explanation as to why up or down changes occurred) – FRB mentioned that in some cases, the BOIR data was not being entered into the core system and also need to be sure that all activity is being aggregated and monitored – need detailed procedures and adequately trained staff – FDIC noted that it is important to compare like businesses with each other as well;
- Teller systems – FRB finding some teller system controls were “weak” in that they allowed the teller to by-pass CTRs and monetary instrument sales records – ideally the teller system should be able to aggregate appropriate transactions;
- CTRs – State reported some DFIs still filing CTRs late – some CTRs were showing “fake” occupations – retired is not an occupation – retired “what”, or unemployed “what” is the information they are looking for;
- Cyber Event reporting – FDIC wants IP addresses in the narrative, and in 44h – redundancy for some reason;

“Tidbits” from Lexington ’22 (cont.)

- M & A – they all talked about mergers and acquisitions – critically important that you have a strong project plan with clear roles and responsibilities clearly articulated both during and after – very important to identify and resolve issues and track the issues through remediation, and after merger, do a “lessons learned” session to prepare for the next one – post merger, so important to validate the surviving core system is properly feeding AML software - @ acquisition, data mapping missing things or model validation not all encompassing;
- SARs – all mentioned – quality of narratives very important – timing of the filings also very important – OCC really focused on insider SARs – careful that you don’t outgrow your monitoring system as well (OCC);

“Tidbits” from Lexington ’22 (cont.)

- Risk Assessments (All) – at times too focused and stale – OCC would like it more data driven and including trend-line analysis (Quantity, Quality, and aggregate level of direction) – “make sure risk assessment assesses risk” (FRB), and that policies and procedures are updated when risk assessment is updated – new products, services, categories of clients need to be factored into the risk assessments – definite “red-flag” for examiners;
- OFAC – with all the economic sanctions resulting from the war in Ukraine, so important to keep OFAC materials up-to-date – make sure parameters are not too tight, being able to catch different variations of spellings of names;
- AML/Risk Management Software - very important to keep all software updated and patches applied (OCC).

07/27/22 – HIDTA Update

- ☰
- 🗨️
- 📧
- 📁
- 📄
- 📄
- 📄
- 📄
- 📄
- 📄

PUBLISHED DOCUMENT

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

ACTION:
Notice of six High Intensity Drug Trafficking Areas (HIDTA) designations.

SUMMARY:
The Director of the Office of National Drug Control Policy designated six additional areas as High Intensity Drug Trafficking Areas (HIDTA). See **SUPPLEMENTARY INFORMATION** for locations.

FOR FURTHER INFORMATION CONTACT:
Questions regarding this notice should be directed to Shannon Kelly, National HIDTA Director, Office of National Drug Control Policy, Executive Office of the President, Washington, DC 20503; (202) 841-5240.

SUPPLEMENTARY INFORMATION:
The new areas are (1) Butte County in California as part of the Central Valley California HIDTA; (2) Vigo County in Indiana as part of the Indiana HIDTA; (3) Cumberland and Salem Counties in New Jersey as part of the Liberty Mid-Atlantic HIDTA; (4) Schenectady County in New York as part of the New York/New Jersey HIDTA; and (5) Lawrence County in Pennsylvania as part of the Ohio HIDTA.

Authority: 21 U.S.C. 1706(b)(1).

DOCUMENT DETAILS

Printed version:
PDF

Publication Date:
07/27/2022

Agencies:
Executive Office of the President
Office of National Drug Control
Policy

Document Type:
Notice

Document Citation:
87 FR 45135

Page:
45135 (1 page)

Document Number:
2022-16095

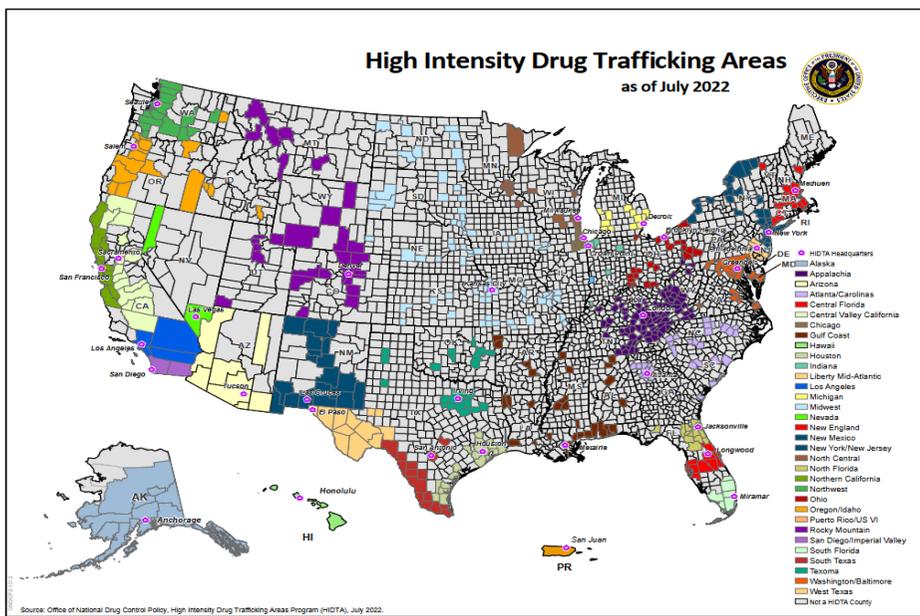
DOCUMENT DETAILS

DOCUMENT STATISTICS

Page views:
205
as of 09/04/2022 at 2:15 pm EDT

DOCUMENT STATISTICS

FORV/S is a trademark of FORV/S, LLP, registration of which is pending with the U.S. Patent and Trademark Office.



FORV/S is a trademark of FORV/S, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

Mark W. Dever, AAP, CAMS
director and ProBank Advisor
ProBank Education Services *powered by*
FORVIS, LLP
502-479-5246
mark.dever@forvis.com



ProBank Education Services *powered by* **FORVIS**

223

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

223

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

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

ProBank Education Services *powered by* **FORVIS**

224

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

224