PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

Majority Staff Report

A FAST AND EASY WAY TO LOSE MONEY:

Insufficient Consumer Protection on the Zelle Network

July 23, 2024 Chairman Richard Blumenthal United States Senate

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Introduction

Millions of Americans moved their lives online during the COVID-19 pandemic, leading to a surge in the use of digital finance services such as online banking and peer-to-peer ("P2P") payments.[1] P2P platforms, which largely operate on mobile phones, allow consumers to transfer money instantly to another person or business.[2] Zelle, a P2P platform owned and operated by Early Warning Services, LLC ("EWS"), which is itself owned by a consortium of large banks, has outpaced competitors like Cash App and Venmo in recent years to become the dominant P2P platform in the United States, making the company an industry leader in digital finance and instant payments.[3] The CEO of EWS has described Zelle as "the digital payments growth engine for the U.S. financial services industry."[4]

Zelle payments are generally instant and irreversible. The speed of P2P payments make them particularly attractive to bad actors.[5] In most cases, by the time a consumer realizes they have been targeted, their money is already gone.[6] Instances in which consumers have been victimized by scams and fraud on Zelle generally fall in two categories: unauthorized transactions, in which a consumer loses control of their account (such as through hacking), and authorized transactions, in which the consumer is somehow tricked into authorizing a payment under false pretenses.[7] Both scams and fraud proliferated on the Zelle Network

---

[1] Polo Rocha, *P2P payments surged during pandemic. So did the complaints about them.*, AMERICAN BANKER (June 22, 2021), https://www.americanbanker.com/news/p2p-payments-surged-during-pandemic-so-did-the-complaints-about-them.

[2] Amber Murakami-Fester and Ruth Sarreal, *What Are Peer-to-Peer Payments?*, NERDWALLET (Feb. 1, 2024), https://www.nerdwallet.com/article/banking/p2p-payment-systems.

[3] Emily Mason, *Despite a Late Start, Bank-Owned Zelle Moves More Money than Venmo and Cash App Combined*, FORBES (Sept. 8, 2022), https://www.forbes.com/sites/emilymason/2022/09/08/despite-a-late-start-bank-owned-zelle-moves-more-money-than-venmo-and-cash-app-combined.

[4] *Zelle Soars with $806 Billion Transaction Volume, up 28% from Prior Year*, ZELLE (Mar. 4, 2024), https://www.zellepay.com/press-releases/zelle-soars-806-billion-transaction-volume-28-prior-year.

[5] *Fraud and instant payments: The basics*, U.S. FED. RESERVE https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html; *Avoid Scams with Peer-to-Peer Payments*, EQUIFAX https://www.equifax.com/personal/education/cybersecurity/articles/-/learn/how-to-avoid-scams-with-payment-apps (last visited July 11, 2024).

[6] *Id.*

[7] *Fraud & Scams Overview*, ZELLE (Apr. 16, 2024), https://www.zellepay.com/safety-education/fraud-scams-overview.

during the pandemic.[8] Federal law requires platforms such as Zelle to reimburse consumers who lose money in unauthorized transactions, what Zelle calls "fraud," but not authorized transactions, what Zelle calls "scams."[9]

Summary of Findings

On June 16, 2023, the Permanent Subcommittee on Investigations ("PSI" or "the Subcommittee") launched an inquiry into EWS, which operates the Zelle Network, and the three largest banks that offer Zelle and co-own EWS: JPMorgan Chase ("JPMorgan"), Bank of America, and Wells Fargo (collectively, the "Three Banks"). Collectively, these banks facilitated 73% of all Zelle payments in 2023.[10] PSI reviewed data and documents related to scams and fraud on the Zelle Network between 2019 to 2023. PSI's inquiry found:

- Despite a legal mandate in the Electronic Fund Transfer Act to reimburse fraud, JPMorgan, Bank of America, and Wells Fargo collectively reimbursed consumers for approximately 38%, or $64 million, of the $166 million worth of fraud disputes at these banks in 2023, leaving over $100 million worth of fraud disputes unreimbursed that year.[11]

    - Consumers who reported scams were infrequently reimbursed by their financial institutions. In 2020, JPMorgan reimbursed three transactions out of 41,390 scam disputes that year, Wells Fargo did not reimburse any of the 25,061 scam disputes, and Bank of America did not track scam data as a separate dispute category until the second half of 2020.[12] In total, these banks rejected scam disputes worth a combined total of approximately $560 million from 2021-2023.[13]

---

[8] Polo Rocha, *P2P payments surged during pandemic. So did the complaints about them.*, AMERICAN BANKER (June 22, 2021), https://www.americanbanker.com/news/p2p-payments-surged-during-pandemic-so-did-the-complaints-about-them.

[9] 15 U.S.C. § 1693f(b); 15 U.S.C. § 1693f(f)(1); *see also*, 12 C.F.R. § 1005. The Electronic Fund Transfer Act is silent regarding authorized payments, but courts have taken the position that financial institutions are not obligated by the statute to reimburse a consumer that took part in authorizing a payment. *See* Background Section IV for further discussion of financial institutions' reimbursement obligations.

[10] Early Warning Services - PSI - Zelle Transaction Percentages, app. C. (on file with EWS) EWS-RR-006-0000001.

[11] These figures were calculated using data produced to PSI by JPMorgan, Wells Fargo, and Bank of America.

[12] *See* Finding 1, Subsection b, for further discussion of these numbers.

[13] These figures were calculated using data produced to PSI by JPMorgan, Wells Fargo, and Bank of America.

- JPMorgan, Bank of America, and Wells Fargo reimbursed claims made by consumers on credit and debit cards at much higher rates than Zelle. From 2019 through 2022, these banks reimbursed 26% of the total dollar value of all Zelle payments disputed for any reason.[14] In contrast, they reimbursed an average of 47% of all credit card disputes and 36% of all debit card disputes during the same period.[15]

- PSI's review of the policies and procedures that JPMorgan, Bank of America, and Wells Fargo use for investigating claims made by consumers disputing Zelle payments found that the policies and procedures allow broad discretion to bank employees reviewing disputes. These policies and procedures allow employees to deny claims based solely on internal documentation in certain instances and offer little transparency to consumers.[16]

- Despite stating on its website that Zelle is intended as a way to send and receive money between "friends, family, and others you trust," commercial usage of Zelle payments has grown significantly, with the number of profiles on Zelle associated with a business growing over 18 times from 2019 to 2023.[17] By comparison, the total processed value of all payments on the Zelle Network grew just over four times in the same time frame.[18]

    - EWS markets Zelle to businesses as a way to accept payments. For example, Zelle introduced integrated QR codes to make it easier for small businesses to accept payment through Zelle and partnered with a national property management company to make it easier for landlords to accept rent payments through Zelle. Despite their apparent efforts to attract commercial payments, EWS, JPMorgan, Bank of America, and Wells Fargo do not offer purchase protections for Zelle payments similar to those available to consumers who use other payment methods, such as credit cards.[19]

---

[14] *Supra*, note 13.

[15] *See* Finding 1, Subsection b, for further discussion of this number.

[16] PSI reviewed policies and procedures related to investigating disputed transactions at JPMorgan, Bank of America, and Wells Fargo.

[17] Letter from Counsel for EWS to the Subcommittee (Feb. 15, 2024); *Zelle Safety 101*, ZELLE, https://www.zellepay.com/pay-it-safe/zeller-safety-101 (last visited Apr. 11, 2024). ("Only send money to those you trust: Zelle® should only be used with friends, family and others you trust"). Note: all letters from respective counsel for EWS, JPMorgan, Bank of America, and Wells Fargo are on file with the Subcommittee.

[18] *Zelle Soars with $806 Billion Transaction Volume, Up 28% From Prior Year*, ZELLE (Mar. 4, 2024), https://www.zellepay.com/press-releases/zelle-soars-806-billion-transaction-volume-28-prior-year; *Gift Giving Helps Zelle® Wrap Up 2019 with Double Digit Growth*, ZELLE (Jan. 28, 2024), https://www.zellepay.com/press-releases/gift-giving-helps-zelle-wrap-2019-double-digit-growth.

[19] *See* Finding 2 for further discussion of the use of Zelle for commercial payments.

- Zelle expanded its reimbursement policy in June 2023, describing the expansion of reimbursement rules as "well above existing legal and regulatory requirements,"[20] but the new policy covers only a small percentage of all scam disputes on the Zelle Network.[21] The policy change resulted in $18.3 million in reimbursed scam claims in the six months following its implementation, amounting to approximately 15-20% of all scam disputes on the Zelle Network within that timeframe.[22]

- EWS oversees governance of the Zelle Network and monitors it for noncompliance with network policies. Six out of seven of the banks that co-own EWS were in violation of Zelle Network policies at least once in the 26-month period reviewed by PSI for having elevated rates of scams and fraud at their institution.[23]

    - In October 2022, Wells Fargo paid a one-time noncompliance fee of $25,000 to EWS and in September 2023, EWS assessed Bank of America a one-time noncompliance fee of $30,000.[24]

- EWS collects voluminous real-time data on the consumers who use Zelle, directly and through the banks that participate in the Zelle Network.[25] EWS uses the data it collects on consumers to develop risk management tools that it sells to financial services companies.[26] EWS operates Zelle at a loss but told PSI that the data-based products it sells are its "profit driver."[27]

    - While banks' obligations to report data to EWS and bank regulators are not the same, JPMorgan, Bank of America, and Wells Fargo appear to share more data on scams and fraud with EWS than with their regulators.[28] The banks told PSI that their meetings with regulators *may* include a discussion of scams and fraud, but the Zelle Network Participation Rules state that banks *must* provide granular data on scams and fraud to EWS on a daily basis.

---

[20] Hannah Lang, *Payments App Zelle Begins Refunds for Imposter Scams After Washington Pressure*, REUTERS (Nov. 13, 2023), https://www.reuters.com/technology/cybersecurity/payments-app-zelle-begins-refunds-imposter-scams-after-washington-pressure-2023-11-13/.

[21] Letter from Counsel for EWS to the Subcommittee (Feb. 15, 2024).

[22] *Id*.

[23] *See* Finding 3, Subsection b, for further discussion of the self-regulation measures of the Zelle Network.

[24] Letter from Counsel for Wells Fargo to the Subcommittee (Jan. 23, 2024); Letter from Counsel for Bank of America to the Subcommittee (Jan. 12, 2024).

[25] *See* Finding 4 for further discussion of EWS's data collection practices.

[26] *Products*, EARLY WARNING (2024), https://www.earlywarning.com/products (last visited July 17, 2024).

[27] Briefing with EWS to the Subcommittee (Nov. 14, 2023).

[28] *See* Finding 4 for further discussion of EWS's data collection practices.

- Between 2019 and 2022, JPMorgan, Bank of America, and Wells Fargo on average reimbursed consumers under 35 at lower rates than older consumers.[29] In 2022, consumers over 65 at these banks were almost twice as likely to be reimbursed for fraud disputes than consumers under 18, with an average of 35% of consumers under 18 reimbursed versus 68% of consumers over 65. Zelle and the banks that offer it provide few controls that could empower parents to protect their minor children, such as the ability to disable Zelle in their child's banking app. These banks appear to have fewer safety protocols in place for minors than for their older customers.[30]

Recommendations

Over the course of PSI's 13-month investigation, the Subcommittee identified multiple opportunities that Congress, regulators, and the companies that participate in the Zelle Network could take to improve consumer protection. Accordingly, this report includes the following recommendations:

1. Congress should amend the Electronic Fund Transfer Act to require financial institutions to reimburse consumers for "fraudulently induced" authorized transactions. Amidst a surge in increasingly sophisticated scams and fraud, such an amendment would offer consumers more robust protection should they fall victim to a scam.

2. The Consumer Financial Protection Bureau ("CFPB") should update Regulation E to require financial institutions to provide greater transparency when responding to disputed transactions by providing further clarity on what constitutes a "reasonable" investigation. This would create a higher standard for dispute investigations, giving banks a minimum set of requirements that they must meet as part of a thorough investigation of disputed claims.

3. Where P2P payments are intended for commercial purposes, payment platforms should be required to provide purchase protections that they provide for other payment methods, such as for credit cards. By extending purchase protections to P2P payments, consumers could engage with small businesses knowing that they are protected by the reimbursement standards offered by other payment methods in commercial transactions.

---

[29] *See* Finding 5 for further discussion of reimbursement rates for various age demographics.

[30] *See* Finding 5, Subsection c, for further discussion of the safety protocols used by the JPMorgan, Bank of America, and Wells Fargo.

4. EWS and banks that offer Zelle should implement a robust framework to share specific and real time information regarding scams and fraud with law enforcement and other financial institutions. This framework would strengthen those institutions' collective defenses to scams and fraud and empower law enforcement to apprehend bad actors.

5. In the face of growing digitization of finance, Congress and the CFPB should further limit the use of consumer financial data collected by payment platforms. Better disclosures and more meaningful limitations on the use of financial data would help protect consumers from unwanted harvesting of their data.

6. EWS should require banks that offer Zelle to allow parents to disable Zelle in their child's online banking app and to notify parents of large transactions initiated by their child. Developing such capabilities would empower parents to monitor the safety of their child's financial decision making.

7. Congress should amend the Electronic Fund Transfer Act to clarify that EWS, and any other financial services companies that play a central role in facilitating electronic fund transfers, are considered a "financial institution" under the statute. Expanding the definition to include these entities would make it more difficult for EWS to avoid responsibility to protect consumers.

FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023

September 2024

Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023

This Financial Trend Analysis focuses on patterns and trends identified in Bank Secrecy Act (BSA) data linked to mail theft-related check fraud. The Financial Crimes Enforcement Network (FinCEN) is issuing this report pursuant to section 6206 of the Anti-Money Laundering Act of 2020, which requires periodic publication of BSA-derived threat pattern and trend information.[1] FinCEN issued government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) on 30 June 2021, which included fraud as a government-wide priority. The United States (U.S.) Department of the Treasury established mail theft-related check fraud as a concern, and FinCEN issued the Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail, FIN-2023-Alert 003, on 27 February 2023 (February 2023 Mail Theft-Related Check Fraud Alert).[2] This Financial Trend Analysis is relevant to the public and a wide range of consumers, businesses, and industries and it highlights the value of BSA information filed by regulated financial institutions, including responses to the February 2023 Mail Theft-Related Check Fraud Alert.

Executive Summary: This Financial Trend Analysis analyzes threat pattern and trend information on mail theft-related check fraud incidents, based on BSA data filed with FinCEN between 27 February and 31 August 2023 (the review period).[3] During the review period, FinCEN received 15,417 BSA reports related to mail theft-related check fraud associated with more than $688 million in transactions, which may include both actual and attempted transactions. Mail theft-related check fraud losses can affect personal savings, checking accounts, business accounts, brokerage accounts and retirement savings, as well as negatively impact financial institutions that typically cover check fraud losses.

Scope and Methodology: FinCEN examined BSA reports that used the February 2023 Mail Theft-Related Check Fraud Alert key term filed during the review period to determine trends. The February 2023 Mail Theft-Related Check Fraud Alert requested financial institutions include the term "FIN-2023-MAILTHEFT" in BSA reporting. The full data set consisted of 15,417 BSA reports filed during this review period, reporting roughly $688 million in mail theft-related check fraud incidents, which may include both completed and attempted

1. William M. (Mac) Thornberry Nat'l Def. Authorization Act for FY 21, Pub. L. No. 116-283, division F, §§ 6001-6511 (2021).
2. *See* Department of the Treasury, "National Money Laundering Risk Assessment" February 2024, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.
3. *See* "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail," FinCEN Alert #FIN-2023-Alert003, 27 February 2023, FinCEN Alert, FIN-2023-Alert003, February 27, 2023.

transactions.[4] [5] These reports may refer to incidents that occurred prior to the review period. FinCEN used a combination of automated and manual review of mail theft-related check fraud BSA reports to identify mail theft-related check fraud activity.

Overview of Key Findings: FinCEN identified three primary outcomes from perpetrators after stealing checks from the U.S. Mail: (1) altering and depositing the checks, (2) using the stolen checks to create counterfeit checks, and (3) fraudulently signing and depositing the checks. The methodologies that criminals use to perpetrate these outcomes can range from unsophisticated to highly organized and complex, often involving the use of advanced counterfeit check technology and chemicals that can remove ink from stolen checks.

- *Banks Filed 88 percent of All Mail Theft-Related Check Fraud Reports*: The largest banks (by asset totals) in the United States submitted 44 percent of the bank filings in the review period. Small-to-medium size banks filed a majority of BSA reports on mail theft-related check fraud.
- *Checks are Most Frequently Altered and then Deposited After They are Stolen from the Mail*: Criminals most frequently alter and then negotiate stolen checks, according to BSA reporting.[6] Their second most frequent use of stolen checks was creating counterfeit checks—where a stolen check is used as a template to produce counterfeits. And the third most common outcome was perpetrators fraudulently signing and depositing checks.[7] Altered checks accounted for approximately 44 percent of the BSA reports, counterfeit accounted for 26 percent, and fraudulently signed checks were 20 percent, according to manual review of BSA reports.
- *Methodologies Range in Sophistication*: The level of sophistication of the check fraud depends on the perpetrator's technological capabilities. Effective alterations and counterfeit checks require some knowledge of the technology and chemicals used to wash checks.[8]
- *Reliance on Avoiding Human Contact*: Many perpetrators utilized methods that avoid human contact, including check deposits via remote deposit capture (RDC) or at automated teller machines (ATMs) and opening accounts online rather than in person.

4. Amounts associated with these BSA reports may include attempted transactions and payments that were unpaid. This figure also includes BSA reports that describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity. These suspicious activity amounts may also include duplicates, counting of both inbound and outbound transactions, transfers between accounts, typos, and errors as submitted by filers. Additionally, to reduce outliers, FinCEN excluded amounts over $1 billion, which caused the loss of two BSA reports.
5. For the purposes of this report, FinCEN omitted filings pertaining to August 2023 incidents filed after the review period.
6. Check negotiation refers to a transfer of ownership of a check or the process of changing a check into money. It can also include endorsing a check and depositing it, cashing it, or signing it over to another party for further negotiation.
7. These figures represent the number of times a methodology was identified for individual check deposits reported in BSA data. BSA reports indicated multiple check deposits in one report that may detail different methodologies. As such, the numbers for each methodology will be higher than the total number of BSA reports reviewed.
8. Check washing is when criminals treat a stolen check with chemicals or compounds that remove the ink from a check and then replace the erased information.

- *Mail Theft-Related Check Fraud is a Nationwide Problem*: The BSA reporting included subjects or branch activity in every U.S. state as well as Washington, D.C., and Puerto Rico.

What is Mail Theft-Related Check Fraud?

Mail theft-related check fraud is the fraudulent negotiation of checks stolen from the U.S. Mail.[9] Criminals may steal different types of checks and attempt to use them for their own benefit. Once stolen, there are several ways they use the checks, including altering payees and/or amounts, using the stolen check to create counterfeit checks, fraudulently signing the check, and selling the check or its identifying information on dark web marketplaces or encrypted social media platforms, according to BSA reporting. Generally, mail theft-related check fraud is the combination of two crimes: mail theft and check fraud.

The United States Postal Inspection Service (USPIS) received 299,020 mail theft complaints between March 2020 and February 2021, a 161 percent increase compared with the previous 12 months.[10] Additionally, the United States Postal Service (USPS) reported 38,500 high volume mail theft incidents from mail receptables (including blue USPS collection boxes) from October 2021-October 2022 and over 25,000 such incidents in the first half of Fiscal Year 2023.[11] While mail theft often consists of mail being stolen from USPS mailboxes or personal mailboxes, USPIS reported 412 mail carriers were robbed on duty between October 2021-October 2022 and 305 were robbed in the first half of Fiscal Year 2023.[12] Incidents of mail theft spiked after the onset of the COVID-19 pandemic, as many individuals and businesses received financial assistance via the U.S. Mail.[13]

Check fraud refers to any use of paper or digital checks to fraudulently obtain funds. As noted above, this fraud can take many forms, including alterations, counterfeiting, and perpetrators signing checks not belonging to them, among others. FinCEN received over 680,000 BSA filings related to check fraud in 2022, which is nearly double the filings received related to check fraud in the previous year.[14] Those filings cover check fraud as a whole and are not indicative of mail theft-related check fraud, specifically.

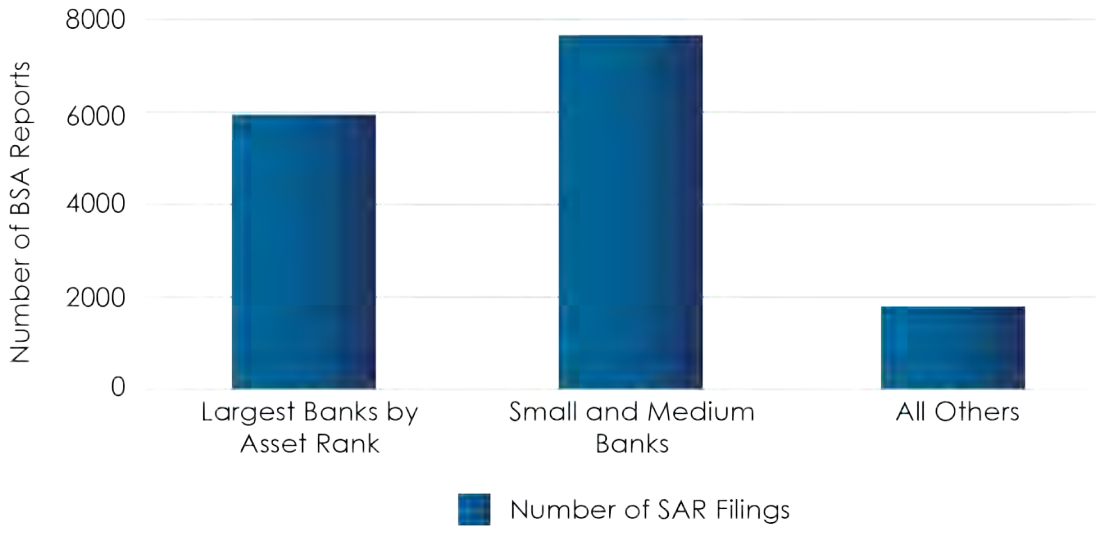
9. *See* FinCEN *supra* note 3.
10. *See* "U.S. Postal Inspection Service Pandemic Response to Mail Fraud and Mail Theft," U.S. Postal Service Office of the Inspector General Report #20-305-R21, 20 May 2021, https://www.uspsoig.gov/sites/default/files/reports/2023-01/20-305-R21.pdf.
11. *See* USPS, "Postal Inspection Service Roll Out Expanded Crime Prevention Measures to Crack Down on Mail Theft, Enhance Employee Safety, and Strengthen Consumer Protections," 12 May 2023, https://about.usps.com/newsroom/national-releases/2023/0512-usps-postal-inspection-service-roll-out-expanded-measures-to-crack-down-on-mail-theft.htm.
12. *See id*.
13. *See* USPS *supra* note 10.
14. *See* FinCEN *supra* note 3.

Banks Filed Vast Majority of Mail Theft-Related Check Fraud BSA Reports

Financial institutions filed 15,417 BSA reports with the February 2023 Mail Theft-Related Check Fraud Alert key term during the review period. This period covers the first six months after FinCEN issued its alert to use the key term in BSA filings on 27 February 2023. A total of 841 financial institutions—consisting primarily of banks, credit unions, and securities/futures firms—filed BSA reports indicating the mail theft-related check fraud alert term. The number of filings each month were relatively consistent during the review period, ranging from a low of 2,307 received in July 2023, to a high of 2,918 received in August 2023.

Banks filed 13,618 of the total mail theft-related check fraud BSA reports, accounting for 88 percent of the filings during the review period. The largest U.S. banks by asset size, according to rankings by the Federal Reserve, filed 44 percent of the BSA reports from banks.[15] In total, 635 unique banks filed BSA reports indicating mail theft-related check fraud, which included 31 banks that filed more than 100 BSA reports during the review period. Financial institutions that filed BSA reports in this dataset included instances when clients were victimized and when clients deposited or attempted to deposit stolen or counterfeit checks.

BSA Report Filings by Filer Type



While credit unions and securities/futures firms also issue and negotiate checks, these financial institutions combined only filed 1,767 BSA reports—or 11.5 percent of the total—during the review period. Securities/futures firms filed 885 BSA reports, and credit unions filed 882 BSA reports. In total, 32 different securities/futures firms and 165 different credit unions filed mail theft-related check fraud BSA reports.

15. *See* "Insured U.S-Chartered Commercial Banks that have Consolidated Assets of $300 Million or More, Ranked by Consolidated Assets as of March 31, 2023," Federal Reserve Statistical Release, United States Federal Reserve Board, https://www.federalreserve.gov/releases/lbr/current/.

Money services businesses (MSBs) filed three mail theft-related check fraud BSA reports. While this may represent a relatively low number of BSA reports, check casher MSBs are not required to file Suspicious Activity Reports, although they may do so voluntarily. Check cashers, however, are required to register with FinCEN as an MSB, maintain an anti-money laundering program, and meet other recordkeeping and reporting obligations under the BSA.[16]

The average activity amount reported per BSA report for mail theft-related check fraud was $44,774, while the median amount was $14,215. This included 41 BSA reports that had no amount reported, 41 others that reported $0, and one that reported $1.[17] Additionally, numerous BSA filings reported the entire amount of a check that was attempted to be negotiated, even though the transaction never occurred.

Stolen Checks are Most Frequently Altered Before Negotiation

Stolen checks are most frequently altered and then deposited or cashed, according to BSA reporting. The payee line was the most frequently altered section, followed by the amount, which is typically made higher than the intended amount. Perpetrators also forged signatures and altered issuer information, which often requires washing the checks first. If a stolen check is not altered or directly deposited, criminals may use it as a template to create counterfeit checks, which was the second most frequently observed behavior. If counterfeit checks are not identified during the negotiation process, losses resulting from that initial stolen check can be significantly higher.

- Some perpetrators do not alter any information on the check and simply sign the back and attempt to negotiate it, though this occurred least frequently. In some instances, perpetrators forged the intended recipient's signature and other times they simply signed their own name or applied an indecipherable signature and attempted to deposit it.
- Other times, perpetrators opened a new account at a financial institution that had either the same name as the intended recipient or a nearly identical name and deposited the check. These new accounts were typically opened online with fraudulent or stolen identification information, according to BSA filings.

Check Manipulation Methodologies Range in Sophistication

BSA reporting indicated several methodologies used to alter, counterfeit, or fraudulently sign checks that ranged in sophistication, demonstrating that perpetrators' capabilities are expansive. Some opted for speed and ease, while others took extra effort to disguise their activity and increase the likelihood of successful negotiation. More organized check cashing rings often appeared

16. *See* 31 CFR 1022.320. Check cashers are required to file Currency Transaction Reports (CTRs) and other applicable BSA forms.
17. The $0 reports and those with no amount reported were left in the dataset of this report because of how different filers reported their amounts. If no money was transferred, some filers reported the suspicious activity amount as $0 while others included the amount that was intended to be transferred. There were also BSA reports that included both successful and unsuccessful transactions as part of the suspicious activity amount.

to combine methodologies to maximize their chances of success.[18] The levels of sophistication identified below were broken into three general categories (unsophisticated, moderately sophisticated, and sophisticated) based on which methods take the most time, expertise, and precision to successfully execute. While some methods are relatively simple, others that are more difficult require check washing chemicals and technological expertise. Below is a brief description of identified methodologies—categorized by level of sophistication—which all occurred after a check was stolen from the mail:

Unsophisticated Methodologies

- **Fraudulently endorsing a check without modifying any information on the check**: This involved someone signing their name on the back of a stolen check and attempting to deposit it.
- **Altering the payee or dollar amount without washing the check**: Some perpetrators crossed out the payee and added their own name or changed certain letters or numbers to change the payee and/or amount. Others used white out to alter the information.
- **Third-party payments[19] with no check modifications**: Instead of modifying a check, criminals attempted making it appear as though the intended payee signed it over to them and attempted negotiating the check.

Moderately Sophisticated Methodologies

- **Check washing**: Perpetrators wash check information using available chemicals to remove original ink and replace it with new information.
- **Selling information from a stolen check online**: Some criminals attempted monetizing the check beyond its original amount by selling the check on dark web marketplaces or online forums, according to BSA reports and open-source research.[20]
- **Using compromised check information to create counterfeit checks**: Criminals took stolen checks and used them as a framework to create counterfeit checks with the victim's banking information. Some criminals used more sophisticated technology to make high-quality counterfeit checks.
- **Stealing newly ordered checks from the mail**: Some criminals stole newly ordered blank checks from the mail, forged the rightful account holder's signature, and then issued the checks to themselves or others.

18. *See* United States Attorney's Office, Northern District of Georgia Press Release, "Fifteen Defendants Sentenced in Stolen U.S. Treasury Check Ring," 18 December 2018, https://www.justice.gov/usao-ndga/pr/fifteen-defendants-sentenced-stolen-us-treasury-check-ring; State of California Department of Justice Press Release, "Attorney General Bonta Announces 56 Arrests in $5 Million Postal Theft and Fraud Operation," 7 October 2022, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-56-arrests-5-million-postal-theft-and-fraud.
19. A third-party check is a check in which the original payee has both endorsed the check and assigned it to a new payee, allowing that person to deposit or cash it. Financial institutions are not required to accept third party checks.
20. *See* Ron Lieber, "Stolen Checks are for Sale Online. We Called Some of the Victims," *The New York Times*, 20 December 2023, https://www.nytimes.com/2023/12/09/business/stolen-checks-telegram.html.

Sophisticated Methodologies

- **New account fraud**: New account fraud involved criminals opening new accounts, typically online, specifically designed to negotiate stolen checks.[21] This most frequently occurred when stolen checks were made out to businesses. Some criminals opened accounts either in the name of the payee or a name that is nearly identical. The company that opened the account may not actually exist and may use a fraudulent address during the account opening process. Perpetrators may open these accounts using compromised identifying information or synthetic IDs comprising of information from several people.
- **Mail theft-related check fraud as part of a larger scam, mostly romance and employment scams**: In these cases, scammers engaged victims in a scam and convinced them to negotiate a check and then send the funds elsewhere, using the victims as money mules to move stolen funds.
- **Insider involvement**: Sophisticated operations have enlisted insider assistance at financial institutions or the USPS.[22] In one case, federal prosecutors charged a USPS employee with stealing more than $1.6 million in checks from the U.S. mail, altering the checks, and depositing them into his own account.[23]

Perpetrators Try to Avoid Interaction with Bank Personnel

BSA reporting reflects that perpetrators appear to prefer depositing checks via methods that avoid in-person contact with depository institution personnel.[24] This eliminates a hurdle to negotiating the checks in person, as bank officials could potentially detect the fraudulent check or become suspicious of the person depositing the check, which could hinder the scheme.

- Deposits at ATMs or via RDC were the preferred method of deposit, according to BSA reports. While both allow depositors to avoid bank personnel, RDC ensures that no one from the receiving bank physically handles the check. Financial institutions noted that poorly made counterfeit checks are often made using incorrect check stock, and security features according to BSA reporting and open-source information.[25]
- Perpetrators of new account fraud often opened their accounts online, using fraudulent identifying information or a money mule to open the account, according to BSA reporting.

21. New account fraud refers to fraud in newly opened accounts shortly after opening. Often, these accounts appear to be opened solely to facilitate fraud or process fraud-related payments.
22. *See* United States Attorney's Office, Central District of California Press Release, "Orange County Man Pleads Guilty to $1.2 Million Check Fraud Scheme He Promoted on Social Media," 25 May 2023, https://www.justice.gov/usao-cdca/pr/orange-county-man-pleads-guilty-12-million-check-fraud-scheme-he-promoted-social-media.
23. *See* United States Attorney's Office, District of Columbia Press Release, "Former Postal Worker Charged with Stealing Checks from the U.S. Mail," 22 September 2023, https://www.justice.gov/usao-dc/pr/former-postal-worker-charged-stealing-checks-us-mail.
24. For this report, depository institutions consist of both banks and credit unions.
25. *See* Georgia Department of Banking and Finance, "Check Fraud/Counterfeit Checks," https://dbf.georgia.gov/check-fraud-counterfeit-checks.

Mail Theft-Related Check Fraud Affects Communities Across the United States

Financial institutions reported transactional activity or BSA filing subjects linked to every U.S. state, Washington, D.C., and Puerto Rico. While every state has been affected, populous states with large urban areas have reported more incidents. See below for additional information regarding locations of subjects identified in BSA reports. Based on a review of the BSA reports within the dataset, filers completed this field where subject location could be identified. However, the subject may not be known or their information may not be available and/or reported in all instances.

Top Five States by BSA Report Subjects (Count and per 100,000 Residents by Subject State)

Count of Subjects per State	BSA Report Subjects per 100,000 Residents
New York: 1,702	Alabama: 13.992
California: 1,458	Georgia: 10.838
Florida: 1,423	Washington, D.C.: 9.572
Georgia: 1,161	New York: 8.425
Texas: 1,007	New Jersey: 7.579

See below for additional information regarding locations of check deposit and cashing activity. As with the subject information, filers completed this field where a branch location could be identified, but this information is not always available and/or reported, including where the reported activity was conducted entirely online:

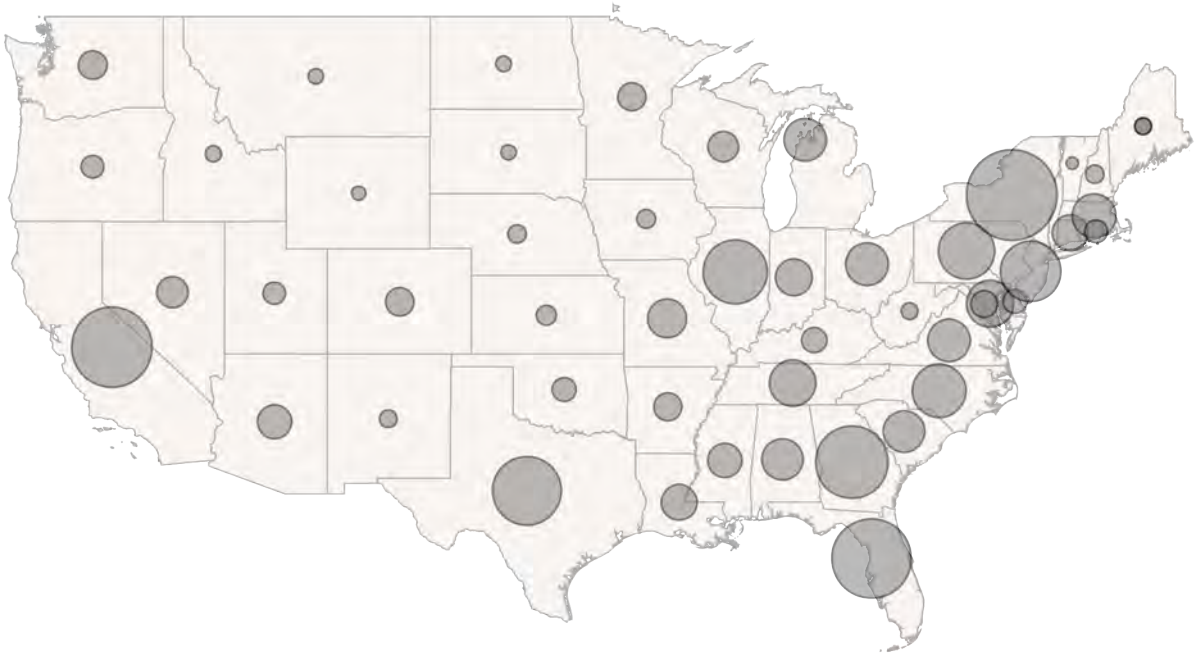
Top Five States by Branch Location Activity (Branch Location BSA Report Count and Branch Location Count per 100,000 Residents)

Branch Location Count	Branch Location Counts per 100,000 Residents
New York: 1,037	Washington, D.C.: 6.816
California: 745	New York: 5.133
Florida: 466	New Jersey: 4.285
New Jersey: 398	Maryland: 3.610
Illinois: 375	Delaware: 3.536

The information in this report is based on mail theft-related check fraud information obtained from analysis of BSA data, and open-source publications, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at frc@fincen.gov.

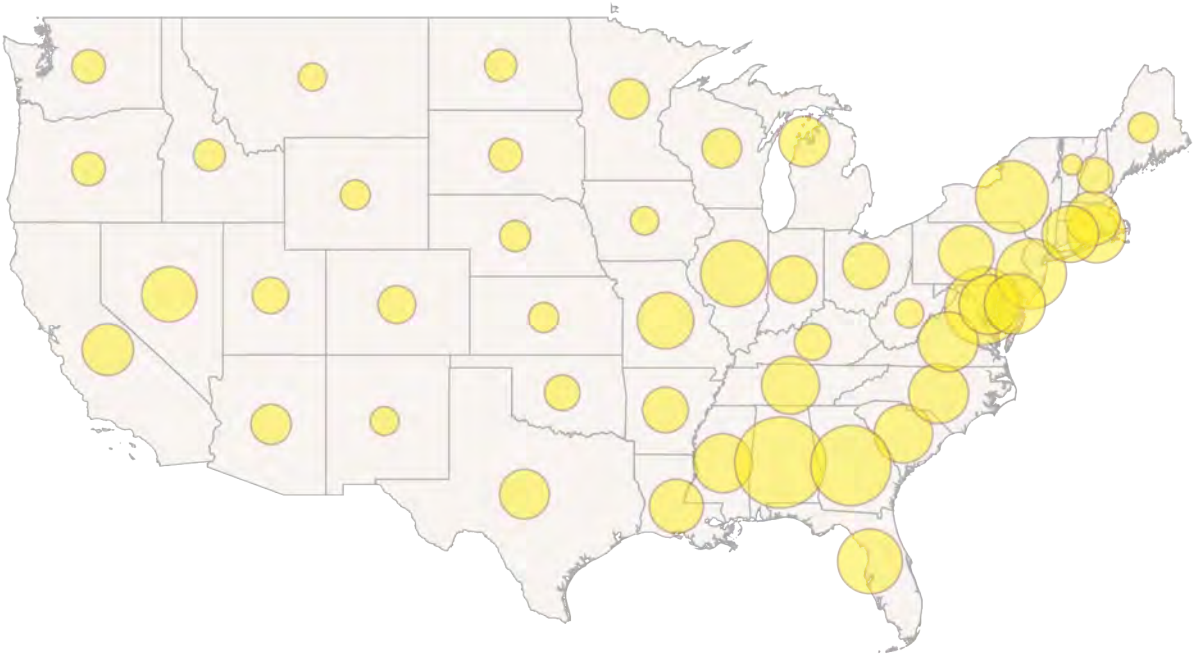
Appendix A: BSA Report Subjects and Branch Location Activity by State

Map 1: States by Count of BSA Report Subjects



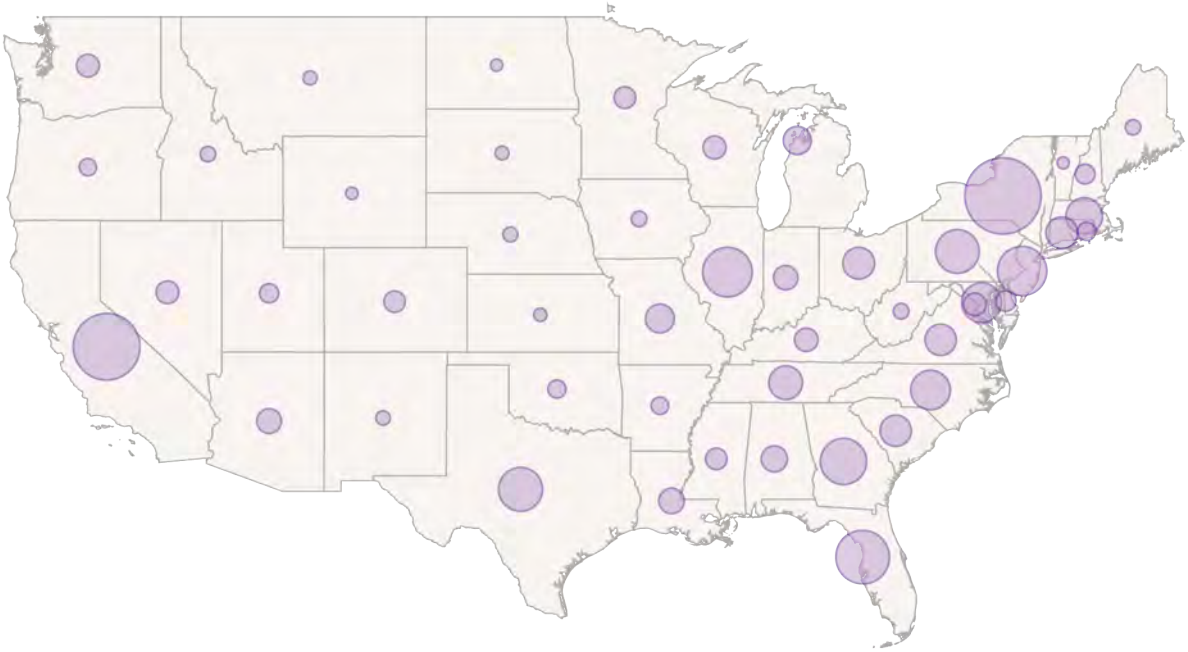
State	Subjects Count	State	Subjects Count	State	Subjects Count
AK	7	KY	69	NY	1,702
AL	703	LA	189	OH	336
AR	87	MA	308	OK	61
AZ	163	MD	345	OR	55
CA	1,458	ME	13	PA	585
CO	100	MI	372	RI	58
CT	175	MN	109	SC	265
DC	66	MO	287	SD	11
DE	56	MS	156	TN	347
FL	1,423	MT	8	TX	1,007
GA	1,161	NC	565	UT	51
HI	7	ND	9	VA	469
IA	24	NE	20	VT	2
ID	20	NH	21	WA	96
IL	894	NJ	704	WI	119
IN	204	NM	17	WV	16
KS	25	NV	144	WY	5

Map 2: BSA Report Subjects per 100,000 Residents by State



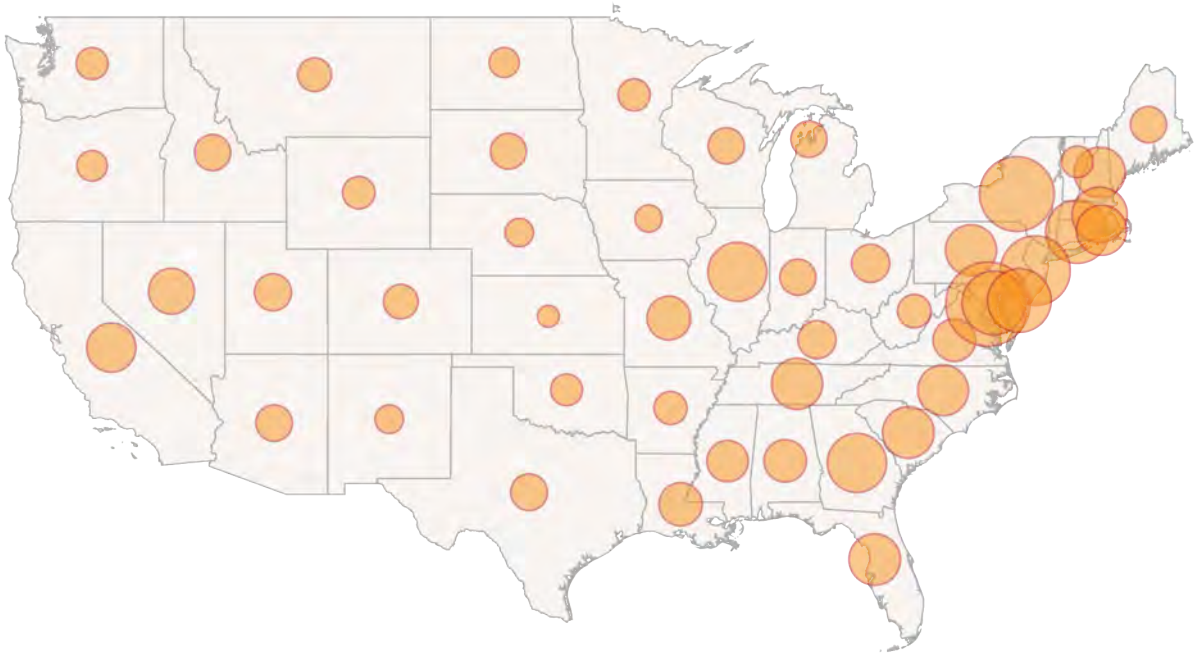
State	Subjects Per 100,000	State	Subjects Per 100,000	State	Subjects Per 100,000
AK	0.954	KY	1.531	NY	8.425
AL	13.992	LA	4.058	OH	2.848
AR	2.889	MA	4.381	OK	1.541
AZ	2.279	MD	5.585	OR	1.298
CA	3.688	ME	0.954	PA	4.499
CO	1.732	MI	3.691	RI	5.285
CT	4.853	MN	1.910	SC	5.177
DC	9.572	MO	4.663	SD	1.241
DE	5.657	MS	5.268	TN	5.021
FL	6.607	MT	0.738	TX	3.455
GA	10.838	NC	5.412	UT	1.559
HI	0.481	ND	1.155	VA	5.434
IA	0.752	NE	1.020	VT	0.311
ID	1.087	NH	1.524	WA	1.246
IL	6.978	NJ	7.579	WI	2.019
IN	3.006	NM	0.803	WV	0.892
KS	0.851	NV	4.638	WY	0.867

Map 3: Branch Location Activity by BSA Report Count



State	Branch Count	State	Branch Count	State	Branch Count
AK	25	KY	46	NY	1,037
AL	68	LA	68	OH	126
AR	21	MA	181	OK	25
AZ	63	MD	223	OR	24
CA	745	ME	11	PA	281
CO	43	MI	93	RI	23
CT	126	MN	37	SC	111
DC	47	MO	89	SD	8
DE	35	MS	38	TN	147
FL	466	MT	8	TX	272
GA	322	NC	220	UT	29
HI	1	ND	4	VA	126
IA	12	NE	10	VT	4
ID	16	NH	30	WA	47
IL	375	NJ	398	WI	51
IN	61	NM	10	WV	13
KS	6	NV	49	WY	4

Map 4: BSA Report Branch Location Activity per 100,000 Residents



State	Branches Per 100,000	State	Branches Per 100,000	State	Branches Per 100,000
AK	3.409	KY	1.021	NY	5.133
AL	1.353	LA	1.460	OH	1.068
AR	0.697	MA	2.575	OK	0.631
AZ	0.881	MD	3.610	OR	0.566
CA	1.884	ME	0.807	PA	2.161
CO	0.745	MI	0.923	RI	2.096
CT	3.494	MN	0.648	SC	2.169
DC	6.816	MO	1.446	SD	0.902
DE	3.536	MS	1.283	TN	2.127
FL	2.164	MT	0.738	TX	0.933
GA	3.006	NC	2.107	UT	0.886
HI	0.069	ND	0.513	VA	1.460
IA	0.376	NE	0.510	VT	0.622
ID	0.870	NH	2.178	WA	0.610
IL	2.927	NJ	4.285	WI	0.865
IN	0.899	NM	0.472	WV	0.725
KS	0.204	NV	1.578	WY	0.693

Fact Sheet: FinCEN Issues Final Rule to Increase Transparency in Residential Real Estate Transfers

In August 2024, the Financial Crimes Enforcement Network (FinCEN) announced a final rule that is designed to combat and deter money laundering by increasing transparency in the U.S. residential real estate sector. The rule requires, on a nationwide basis, certain persons involved in real estate closings and settlements to report information to FinCEN about specified transfers of residential real estate that are a high risk for illicit finance. The final rule will take effect on December 1, 2025, and, consistent with any applicable requirements of the Paperwork Reduction Act, FinCEN will provide a separate opportunity for the public to comment on the form of the report mandated by the rule.

Illicit actors often favor non-financed transfers (including "all-cash" sales) of residential real estate to avoid scrutiny from financial institutions that have anti-money laundering and countering the financing of terrorism (AML/CFT) program and Suspicious Activity Report (SAR) filing requirements under the Bank Secrecy Act. Illicit actors also often hold residential real estate in the name of a legal entity or trust, in an effort to obscure their identities and their ownership interests in the property. Transfers that are both non-financed and involve a transferee that is a legal entity or trust are of higher risk for money laundering and make the proceeds of crime and their owners more difficult to track and identify. The reporting of these transfers will help curtail the anonymous laundering of illicit proceeds through the purchase of residential real property which threatens U.S. economic and national security.

Building on FinCEN's long-running Residential Real Estate Geographic Targeting Orders (GTOs)—which required title insurance companies to file reports identifying the beneficial owners of legal entities that make certain non-financed purchases of residential real estate in select jurisdictions in the United States—this rule will address the demonstrated need for increased transparency and work to deter illicit use of the U.S. residential real estate market.

The final rule reflects FinCEN's consideration of the comments it received in response to the notice of proposed rulemaking that was published in February 2024. Commenters included a broad array of individuals, businesses, and organizations, including trade associations, transparency groups, law enforcement representatives, and other interested parties. In response to the commenters and in order to reduce potential compliance burden, FinCEN made several amendments to the proposed rule, such as the adoption of a reasonable reliance standard with respect to information provided by others. Additionally, in order to provide flexibility for real estate professionals in complying with the rule, the rule continues to contain a "cascade" system for determining which professional has primary filing responsibility, but with a with a flexible option for industry professionals to designate compliance responsibilities. FinCEN believes that the requirements set out in the rule reflect the appropriate balance between ensuring that reports

filed under the rule have a high degree of usefulness to law enforcement and minimizing the compliance burden incurred by businesses, including small businesses.

The following provides a general overview of the key elements of the rule (for example, when a report is required to be filed, who must file, and when) and related administrative details. Please refer to the actual text of the final rule for further details, including important definitions.

Overview of the Final Rule

The final rule requires "reporting persons" performing specified closing or settlement functions in certain reportable transfers of residential real property to report specified information to FinCEN about the transfer. As explained in greater detail below, this includes information about the parties to the transfer and the property itself.

Reportable Transfers of Residential Real Property

Transfers are reportable when they meet the following criteria: (1) the property is residential real property; (2) the transfer is non-financed; (3) the property is transferred to a legal entity or trust, and (4) an exemption does not apply.

Transfers meeting the rule's requirements must be reported regardless of purchase price or the value of the property. Gift transfers are thus subject to the rule.

However, transfers made directly to an individual are not covered by this rule.

Definition of Residential Real Property

The rule applies only to residential real property located in the United States. Reportable property includes single-family houses, townhouses, condominiums, and cooperatives, including condominiums and cooperatives in large buildings containing many such units, as well as entire apartment buildings designed for occupancy by one to four families. The rule also requires reporting on transfers of land, such as vacant or unimproved land, on which the transferee intends to build a structure designed for occupancy by one to four families. Furthermore, a transfer of property may be reportable even if the property is mixed use, such as a single-family residence that is located above a commercial enterprise.

Definition of Non-Financed Transfer

For a transfer to be reportable, it must be non-financed, meaning that it does not involve an extension of credit to all transferees that is both (1) secured by the transferred property and (2) extended by a financial institution subject to an AML program and Suspicious Activity Report (SAR) obligations. Transfers that are financed only by a lender without an obligation to maintain an AML program and file SARs, such as a non-bank private lender, are treated as non-financed transfers that potentially must be reported.

Definitions of Transferee Entity and Transfer Trust

A transfer of residential real property must be reported if at least one of the new owners of residential real property is a "transferee entity" or "transferee trust." These categories include legal vehicles commonly used to own property, such as limited liability companies, corporations, partnerships, and trusts. Both domestic and foreign entities and trusts are covered by the reporting requirement.

Certain definitional exemptions apply for highly regulated types of legal entities and trusts that are less likely to be used by illicit actors to launder money through residential real property.

Exemptions from Reporting

Exemptions are provided for certain common, lower-risk transfers. A reportable transfer does not include:

- a transfer of an easement;
- a transfer resulting from the death of an individual, whether pursuant to the terms of a decedent's will or the terms of a trust, the operation of law, or by contractual provision;
- a transfer incident to divorce or dissolution of a marriage or civil union;
- a transfer to a bankruptcy estate;
- a transfer supervised by a court in the United States;
- a transfer made for no consideration by an individual, either alone or with their spouse, to a trust of which that individual, their spouse, or both of them, are the settlor or grantor;
- a transfer to a qualified intermediary for purposes of a like-kind exchange under Section 1031 of the Internal Revenue Code; and
- a transfer for which there is no reporting person.

Determination of Reporting Persons

FinCEN expects that the obligation to file reports will generally rest with settlement agents, title insurance agents, escrow agents, and attorneys. There is only one reporting person for any given reportable transfer.

The reporting person is determined by one of the following ways:

1. Reporting cascade: The reporting cascade consists of a list of seven different functions that a real estate professional may perform in a transfer of residential real property, with the reporting obligation for any such transfer applying to the professional that performed a function that appears highest on the list. For example, the first function on the list is the professional listed as the agent on the closing or settlement statement. If no such professional is involved in the transfer, then the reporting obligation applies to any professional that performed the second function on the list (*i.e.*, the professional that prepared the closing or settlement statement), and so on down the list.

2. Real estate professionals decide: Designed to provide flexibility to the industry and reduce potential burden, the real estate professionals that perform the functions described in the cascading list may enter into a written agreement with each other to designate the professional that will file the report for the transfer.

Required Information

The final rule requires that a reporting person provide information about the transfer of residential real property identifying the following:

- The reporting person;
- The legal entity (transferee entity) or trust (transferee trust) receiving ownership of the property;
- The beneficial owners of the transferee entity or transferee trust;
- Certain individuals signing documents on behalf of the transferee entity or transferee trust during the reportable transfer;
- The transferor (*e.g.,* the seller);
- The residential real property being transferred; and
- Total consideration and certain information about any payments made.

Beneficial owners of transferee entities: To be a beneficial owner of a transferee entity, an individual must, either directly or indirectly, exercise "substantial control" over the transferee entity, or own or control at least 25 percent of the transferee entity's ownership interests. This definition is consistent with the definition of a beneficial owner in FinCEN's Beneficial Ownership Information Reporting Rule. See https://fincen.gov/boi.

Beneficial owners of transferee trusts: The beneficial owner of a transferee trust is any individual who is a trustee or otherwise has authority to dispose of transferee trust assets; is a beneficiary who is the sole permissible recipient of income and principal from the transferee trust or who has the right to demand a distribution of, or to withdraw, substantially all of the assets of the transferee trust; is a grantor or settlor of a revocable trust; or is the beneficial owner of an entity or trust that holds one of these aforementioned positions in the trust.

Reasonable Reliance on Information Provided by Others

When determining whether a transfer is reportable and when collecting required information, reporting persons may rely on information provided by any other person, but only if the reporting person does not have knowledge of facts that would reasonably call into question the reliability of the information.

With regard to the beneficial ownership information of transferee entities or transferee trusts, this reasonable reliance standard is slightly more limited. In these situations, the reasonable reliance standard applies only to information provided by the transferee or the transferee's representative and only if the person providing the information certifies the accuracy of the information in writing to the best of their knowledge.

Filing Real Estate Reports and Keeping Records

A report must be filed by the later date of either: (1) the final day of the month following the month in which the reportable transfer occurred; or (2) 30 calendar days after the date of closing.

The reporting person is not required to retain a copy of the report. However, they must keep for five years a copy of any certification, signed by the transferee or a transferee's representative, certifying that the transferee's beneficial ownership information, as well as a copy of any designation agreement signed. Other parties to the designation agreement similarly need to keep copies of the agreement.

Next Steps

The effective date of this rule is December 1, 2025. FinCEN will publish a notice regarding the form of the report at a later date, consistent with any applicable requirements of the Paperwork Reduction Act.

FinCEN Reminds Financial Institutions to Remain Vigilant to Suspicious Transactions Associated with Synthetic Opioids

Immediate Release: August 26, 2024

WASHINGTON—During Overdose Awareness Week (https://www.whitehouse.gov/briefing-room/presidential-actions/2024/08/23/a-proclamation-on-overdose-awareness-week-2024/) as the nation honors and remembers loved ones lost to the drug overdose epidemic, the Financial Crimes Enforcement Network (FinCEN) reminds financial institutions to monitor for and report suspicious transactional activity related to the illicit fentanyl supply chain and the trafficking of illicit fentanyl and other synthetic opioids. FinCEN continues its efforts to marshal resources and expertise to combat the trafficking of illicit fentanyl through its participation in the Department of the Treasury's Counter-Fentanyl Strike Force (https://home.treasury.gov/news/press-releases/jy1946).

FinCEN has previously published the following resources on the trafficking of fentanyl, fentanyl analogues, and other synthetic opioids and the precursor chemicals and associated manufacturing equipment needed to synthesize these deadly drugs:

- Supplemental Advisory on the Procurement of Precursor Chemicals and Manufacturing Equipment Used for the Synthesis of Illicit Fentanyl and Other Synthetic Opioids (https://www.fincen.gov/sites/default/files/advisory/2024-06-20/FinCEN-Supplemental-Advisory-on-Fentanyl-508C.pdf) (June 2024)
- Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids (https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl Advisory FINAL 508.pdf) (August 2019)

FinCEN continues to work with law enforcement and the private sector to combat the opioid crisis. FinCEN is convening information exchange sessions to bring together the public and private sectors for discussions on ways to deepen collaboration against financial crime threats that devastate communities and undermine the integrity of the global financial system.

This past spring, FinCEN partnered with IRS Criminal Investigation (CI) to launch its "Promoting Regional Outreach to Educate Communities on the Threat of Fentanyl" (PROTECT) series of FinCEN Exchange (https://www.fincen.gov/resources/financial-crime-enforcement-network-exchange) events that are being held in U.S. cities that are highly impacted by the opioid epidemic as part of Treasury Department's Counter-Fentanyl Strike Force (https://home.treasury.gov/news/press-releases/jy1946). To date, PROTECT events have been held in Boston, Massachusetts; Tucson, Arizona; Miami, Florida; and just this month, FinCEN and CI hosted two additional PROTECT events in Portland, Oregon and Denver, Colorado. The Portland event, held on August 13, included a threat briefing from government officials on fentanyl and drug trafficking organizations. The Denver event, held on August 20, included region-specific insight from the Rocky Mountain High Intensity Drug Trafficking Area teams on money laundering trends.

*****

FinCEN Exchange is a voluntary public-private partnership that convenes relevant stakeholders, including law enforcement agencies and financial institutions. FinCEN Exchange aims to protect our national security and our citizens from harm by combatting money laundering and its related crimes, including terrorism, through public-private dialogue that encourages, enables, and acknowledges industry focus on high-value and high-impact activities. FinCEN Exchange began in 2017 and was codified as part of the Anti-Money Laundering Act of 2020.

"Promoting Regional Outreach to Educate Communities on the Threat of Fentanyl" (or PROTECT) is a series of ten FinCEN Exchange sessions that will be held through the remainder of 2024 in U.S. cities that are highly impacted by the opioid epidemic as part of the Treasury Department's Counter-Fentanyl Strike Force (https://home.treasury.gov/news/press-releases/jy1946), which is in partnership with IRS Criminal Investigation. The series is specifically designed to work with regional and local banks that are deeply connected to their communities and offer unique perspectives on the opioid crisis and will focus on how law enforcement can best support their efforts to monitor activity that may be tied to the illicit trafficking of fentanyl. At these exchanges, federal officials brief on information critical to tracking these illicit financial flows, including typologies and red-flag indicators of fentanyl-related activity, and discuss what types of information are particularly valuable when financial institutions report suspicious activity. The PROTECT series was launched in collaboration with other government partners, including the Drug Enforcement Administration, Homeland Security Investigations, Customs and Border Protection, the U.S. Secret Service, the Federal Bureau of Investigation, the Department of Justice Money Laundering and Asset Recovery Section, various U.S. Attorney's Offices, and local law enforcement agencies.

###

OFAC Consolidated Frequently Asked Questions

Search FAQs

Search FAQs

Basic Information on OFAC and Sanctions

1. What is OFAC and what does it do?

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions against targeted foreign jurisdictions and regimes, as well as individuals and entities engaging in harmful activity, such as terrorists, international narcotics traffickers, weapons of mass destruction proliferators, and other malign actors, in response to threats to the national security, foreign policy, or economy of the United States. OFAC sanctions take various forms, from blocking the property of specific individuals and entities to broadly prohibiting transactions involving an entire country or geographic region, such as through a trade embargo or prohibitions related to particular sectors of a country's economy.

Read more about OFAC's history on the About OFAC page on OFAC's website.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

3. What kinds of prohibitions does OFAC impose?

Contact OFAC

Each OFAC sanctions program is based on different foreign policy and national security goals, so the prohibitions imposed may vary between programs. Many sanctions programs require blocking the property and interests in property of specific individuals and entities and prohibit dealing in such blocked property. (For more information, see FAQ 9.) OFAC sanctions prohibitions may also take many other forms that do not require blocking but prohibit U.S. persons from engaging in certain trade or financial transactions and other dealings unless authorized by OFAC or exempted by statute. Non-U.S. persons are also subject to certain OFAC prohibitions. For example, non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions. For information on specific prohibitions, authorizations, or exemptions under a particular OFAC sanctions program, please see the relevant OFAC implementing regulations and the Sanctions Programs and Country Information page on OFAC's website.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

4. Are there exceptions to sanctions prohibitions? Are exceptions the same across sanctions programs?

Yes. There may be exceptions to sanctions prohibitions. Exceptions may take the form of authorizations, such as general licenses and specific licenses, or exemptions.

OFAC issues general licenses in most of its sanctions programs to authorize certain transactions that would otherwise be prohibited, such as transactions related to humanitarian activities or official business of the U.S. government. General licenses are self-executing, meaning they allow persons to engage in certain transactions involving the United States or U.S. persons without needing to apply for a specific license provided the transactions meet certain terms and conditions as described in the general license.

OFAC may also issue specific licenses on a case-by-case basis. In contrast to general licenses, which authorize certain transactions for all persons who meet the conditions described in the license, specific licenses only authorize the licensee(s) to engage in certain transactions that would otherwise be prohibited. For guidance on how to request and apply for a specific license, please see 31 CFR § 501.801 and the License Application page on OFAC's website.

Exceptions may also take the form of exemptions, meaning certain types of transactions are exempt from sanctions and therefore not prohibited. For

example, in certain sanctions programs transactions involving personal communications, humanitarian donations, information or informational materials, and travel are exempt from relevant prohibitions.

Most OFAC sanctions programs have certain exceptions, but exceptions may vary in type and scope across different sanctions programs. For information on the authorizations or exemptions under a particular OFAC sanctions program, please see the relevant OFAC implementing regulations and the Sanctions Programs and Country Information page on OFAC's website.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

6. Where can I find specific details about a particular sanctions program?

References to relevant statutes, executive orders, regulations, guidance, general licenses, and sanctions actions for each sanctions program may be found in the Sanctions Programs and Country Information page on OFAC's website. The OFAC Legal Library page on OFAC's website also contains links to the relevant legal authorities, including statutes, executive orders, and the Code of Federal Regulations, where specific OFAC sanctions regulations can be found.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

7. If I want to engage in a transaction or activity prohibited by OFAC, how can I do so? Can I rely on a general or specific license to engage in a transaction involving a sanctioned jurisdiction or person?

OFAC issues general licenses to authorize certain transactions that would otherwise be prohibited pursuant to a particular sanctions program. These general licenses are self-executing, meaning they allow persons to engage in certain transactions involving the United States or U.S. persons without needing to apply for a specific license, provided the transactions meet certain terms and conditions as described in the general license. In addition, some categories of activities, such as personal communications and transactions ordinarily incident to travel, may be exempt from sanctions in certain programs. Subject to sanctions program-specific considerations, non-U.S. persons do not generally risk being sanctioned for

engaging in or facilitating transactions for which a U.S. person would not require a specific license.

If you seek to engage in a prohibited transaction involving a U.S. person or blocked property and there is no applicable general license or exemption, you may apply for a specific license from OFAC by submitting a license application. OFAC may grant, on a case-by-case basis, a specific license to authorize a person to engage in a transaction, or series of transactions, that otherwise would be prohibited by sanctions. For guidance on how to request and apply for a specific license, please see 31 CFR § 501.801 and the License Application page on OFAC's website.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

9. What does OFAC mean when it refers to "blocked" property? How does OFAC define "property"?

"Blocking" refers to freezing assets or other property. Blocking immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regard to the property.

OFAC authorities may require U.S. persons to block all property and interests in property of certain persons, known as "blocked persons." When this is the case, any property and interests in property of a blocked person that are within the United States or within the possession or control of a U.S. person must be blocked (i.e., "frozen")—not seized—and may not be transferred, withdrawn, or otherwise dealt in. Title to the blocked property remains with the blocked person, but the exercise of powers and privileges normally associated with ownership is prohibited without authorization from OFAC.

In addition, parties must report blocked property to OFAC within 10 business days of the property becoming blocked. Blocked persons include persons that appear on OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List), foreign governments subject to blocking, and persons blocked pursuant to OFAC's "50 Percent Rule." For further information, see FAQ 401 and OFAC guidance on the "50 Percent Rule."

The term "property," as defined in various OFAC regulations, includes financial property (e.g., money, checks, savings accounts, stocks, bonds, debt, or any other financial instruments), real, tangible, and intangible assets (e.g., goods, merchandise, ships, land contracts, and real estate), and any other property or interests therein present, future, or contingent. For information on how OFAC defines property in a particular sanctions program, please see the relevant OFAC

implementing regulations and the Sanctions Programs and Country Information page on OFAC's website.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

10. What jurisdictions or countries are sanctioned by the United States?

OFAC implements, administers, and enforces U.S. sanctions across many jurisdictions. Some of these sanctions are comprehensive in nature and broadly prohibit most transactions involving the particular jurisdiction and may also include blocking restrictions on the government of such jurisdiction. These jurisdictions include both countries and certain geographic regions.

Other sanctions programs impose targeted sanctions on specific persons in relation to a particular jurisdiction or activity. For example, persons appearing on OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List) are blocked pursuant to OFAC regulations and authorities. U.S. persons are prohibited from engaging in transactions involving blocked persons wherever blocked persons are located, and all property of blocked persons within U.S. jurisdiction must also be blocked. For example, a person may be designated for engaging in malign activity, such as narcotics trafficking or terrorism. The names, and often aliases, of such designated persons are added to the SDN List, along with other identifying information. With limited exceptions, entities owned by a person on the SDN List (defined as a direct or indirect ownership interest of 50 percent or more) are also blocked, regardless of whether that entity is separately named on the SDN List. For further information, see FAQ 401 and OFAC guidance on the "50 Percent Rule."

Aside from the SDN List, OFAC publishes and maintains other sanctions lists that have different prohibitions associated with them. For example, OFAC's Sectoral Sanctions Identification (SSI) List identifies persons operating in certain sectors that are subject to restrictions other than blocking. Note that the SSI List is not part of the SDN List; however, persons on the SSI List may also appear on the SDN List.

Sanctions programs may change frequently. It is important to check OFAC's website on a regular basis to ensure that you have the most up-to-date information on OFAC prohibitions across sanctions programs, including OFAC's various sanctions lists. OFAC's Sanctions List Search tool can be used to search both the SDN List and all other OFAC sanctions lists. The OFAC Basics videos series

provides further information on how to use OFAC's Sanctions List Search tool. Please see the Sanctions Programs and Country Information page on OFAC's website for information on specific OFAC sanctions programs.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

11. Who must comply with OFAC sanctions?

All U.S. persons must comply with OFAC sanctions, including all U.S. citizens and permanent residents regardless of where they are located, all individuals and entities within the United States, and all U.S. incorporated entities and their foreign branches. Terms such as "U.S. person" and "person subject to U.S. jurisdiction" are defined in the implementing regulations for a particular sanctions program in 31 CFR chapter V. (*See e.g.,* 31 CFR § 560.314 (Iranian Transactions and Sanctions Regulations (ITSR)); 31 CFR § 598.318 (Foreign Narcotics Kingpin Sanctions Regulations). In the case of certain programs, foreign subsidiaries owned or controlled by U.S. persons also must comply. (*See e.g.,* 31 CFR § 560.215 (ITSR); 31 CFR § 510.214 (North Korea Sanctions Regulations)). Non-U.S. persons are also subject to certain sanctions prohibitions. For example, non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions. Certain programs also require foreign persons reexporting certain goods, technology, or services from the United States to comply with U.S. sanctions, even if no U.S. persons are involved in the reexport.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

12. How much are the penalties for violating OFAC sanctions regulations?

Violations of OFAC-administered sanctions programs may result in civil and, in some cases, criminal penalties. Penalties for violations can be substantial. Civil penalties vary by sanctions program, and the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended by the Federal Civil Penalty Inflation Adjustment Act Improvements Act of 2015, requires OFAC to adjust civil monetary penalty amounts annually. For current penalty amounts, see Appendix A to 31 CFR part 501—Economic Sanctions Enforcement Guidelines. For a list of select OFAC enforcement actions, organized by year, please see the Civil Penalties and Enforcement Information page on OFAC's website.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

13. How can I report a possible violation of U.S. sanctions to OFAC? Will I receive "amnesty" if I report a possible violation to OFAC or if my failure to comply with U.S. sanctions was inadvertent?

OFAC encourages anyone who may have violated OFAC-administered sanctions programs, or anyone who is aware of potential violations, to disclose the apparent or potential violation to OFAC. Voluntary self-disclosure to OFAC is considered a mitigating factor by OFAC in enforcement actions, and pursuant to OFAC's Economic Sanctions Enforcement Guidelines, will result in a reduction in the base amount of any proposed civil penalty.

Please submit all voluntary self-disclosures electronically to OFACDisclosures@treasury.gov. OFAC's Economic Sanctions Enforcement Guidelines explain what constitutes a voluntary self-disclosure for purposes of receiving mitigation. Among other factors, the guidelines state that in addition to notification of an apparent violation, a voluntary self-disclosure must include, or be followed within a reasonable period of time by, a report of sufficient detail to afford OFAC a complete understanding of an apparent violation's circumstances. When such a report is not included with an initial notification, OFAC will generally expect such a report within 180 days after the initial notification.

Please review OFAC's Production Submission Standards , which detail OFAC's preferred technical standards for formatting electronic document productions.

OFAC does not have an "amnesty" program. OFAC does, however, review the totality of the circumstances surrounding any apparent violation, including whether a matter was voluntarily self-disclosed to OFAC. Such disclosure may also support credit for cooperation. OFAC will also consider the existence, nature, and adequacy of a subject person's risk-based OFAC compliance program at the time of the apparent violation. Please see OFAC's Economic Sanctions Enforcement Guidelines and OFAC's Framework for OFAC Compliance Commitments for additional information regarding voluntary self-disclosures and other mitigating factors, as well as OFAC's general framework for the enforcement of its sanctions programs. For more information on OFAC's enforcement process and self-disclosing violations, please see the Civil Penalties and Enforcement Information page on OFAC's website.

Other U.S. government agencies, including the U.S. Department of Justice (DOJ) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) have their own disclosure procedures for voluntarily self-disclosing violations of U.S. sanctions and export control laws. Moreover, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) maintains a whistleblower incentive program for violations of OFAC-administered sanctions, in addition to violations of the Bank Secrecy Act. Individuals located in the United States or abroad who provide information may be eligible for awards, if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding $1,000,000.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

14. Can I regard previously issued and published opinion letters, regulatory interpretations, or other statements as guidance for my transactions?

Great care should be taken when placing reliance on such materials to ensure that the transactions in question fully conform to the letter and spirit of the published materials and that the materials have not been superseded.

Basic Information on OFAC and Sanctions

15. Can OFAC change its previously stated, non-published interpretation or opinion without first giving public notice?

Yes. OFAC, therefore, strongly encourages parties to exercise due diligence when their business activities may touch on an OFAC-administered program and to contact OFAC if they have any questions about their transactions.

Basic Information on OFAC and Sanctions

91. What lists does OFAC maintain? Where can I find these lists?

OFAC publishes lists of individuals and entities that are subject to OFAC-administered sanctions. One such list is known as the List of Specially Designated Nationals and Blocked Persons List, or "SDN List," which is available on OFAC's website. Property and interests in property of the individuals and entities on the

SDN List, that is within the United States or within the possession or control of U.S. persons are blocked. Additionally, U.S. persons are generally prohibited from dealing with the individuals and entities on the SDN List.

It is important to note that some OFAC sanctions block categories of persons even if those persons do not appear on the SDN List, including most Cuban nationals, blocked foreign governments, or persons blocked pursuant to OFAC's "50 Percent Rule " (i.e., any entity owned individually or in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons). The property and interests in property of such an entity are blocked regardless of whether the entity itself is listed on the SDN List.

In addition, OFAC maintains other sanctions lists of persons that are subject to non-blocking sanctions. These lists are also available on OFAC's website. For information on specific prohibitions under a particular OFAC sanctions program, please see the relevant OFAC implementing regulations and the Sanctions Programs and Country Information page on OFAC's website.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

126. I tried to ship a package and it was either "blocked" by a shipping company or returned to me because of "OFAC sanctions." Why? How do I get my package back?

A package may be blocked or rejected for multiple reasons. U.S. persons, including shipping companies, are required to "block" packages in which a person blocked by OFAC-administered sanctions has an interest. When a package is required to be "blocked" due to sanctions, the shipper must retain the package rather than return it to the sender. In other circumstances, sanctions may not require that the package be blocked, but a shipping company may have to return your package, or "reject" it. For example, if the package was destined for a location under a U.S. trade embargo and was not otherwise eligible to be shipped in accordance with an existing exemption or OFAC authorization, the shipping company may reject and return your package.

If your package was blocked due to OFAC sanctions, you may request authorization from OFAC for the blocked package to be released by submitting a License Application that includes a detailed description of the package's contents and an explanation of the package's air waybill or Customs Declaration and Dispatch form.

Please see the Sanctions Programs and Country Information page on OFAC's website for more information on the restrictions on shipments to sanctioned jurisdictions.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

468. How do I verify the authenticity of an OFAC document?

If you have questions about the authenticity of an OFAC-issued document that is not publicly posted on OFAC's website, you may contact OFAC and reference the specific case ID or FAC number that is included on the document.

- For specific licenses, please visit OFAC's Licensing Portal and select the "Check Application Status" feature.
- For a removal letter regarding OFAC's List of Specially Designated Nationals and Blocked Persons or any other sanctions list maintained by OFAC, please email OFAC.Reconsideration@treasury.gov. Alternatively, you may check OFAC's Sanctions List Search tool to search OFAC's current sanctions lists.
- For any another OFAC-issued document, please contact OFAC as described here.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

469. Does OFAC issue certificates of non-inclusion, or issue a so-called "safe list" to help prove that an entity or individual is not on one of OFAC's sanctions lists?

No. OFAC does not issue non-inclusion certificates to show an entity or individual is not listed on one of OFAC's sanctions lists, nor does OFAC publish a "safe list." For questions regarding whether a specific entity or individual may be a positive match to an entry on one of OFAC's sanctions lists, please see FAQ 5 or the OFAC Basics Videos Series.

Date Updated: August 21, 2024.

Basic Information on OFAC and Sanctions

Supervisory Highlights, Mortgage Servicing Edition

Issue 33, Spring 2024

1. Introduction

The residential mortgage servicing market exceeds $13 trillion in current outstanding balances. When servicers do not comply with the law, they impose significant costs on consumers.

The CFPB is actively monitoring the market for emerging risks during a period of increasing default servicing activity since the end of the COVID-19 pandemic emergency. The mortgage industry has grappled with many challenges during this period, including increased requests for loss mitigation, changes to housing policies and programs, and staffing issues. Violations described in prior editions of *Supervisory Highlights* raised concerns about servicers' ability to appropriately respond to consumer requests for assistance, especially consumers at risk of foreclosure. While mortgage delinquencies and foreclosure rates remain near all-time lows, this may change in the future as consumers grapple with higher levels of debt and affordability challenges due to high rates and low housing supply. Foreclosure starts have risen in recent months, increasing the risks that vulnerable consumers face.

The CFPB also continues to prioritize scrutiny of exploitative illegal fees charged by banks and financial companies, commonly referred to as "junk fees." Examiners continue to find supervised mortgage servicers assessing junk fees, including unnecessary property inspection fees and improper late fees. Additionally, examiners found that mortgage servicers engaged in other unfair, deceptive, and abusive acts or practices (UDAAP) such as sending deceptive loss mitigation eligibility notices to consumers.[1] Mortgage servicers also violated several of Regulation X's loss mitigation provisions.[2]

The CFPB is currently reviewing Regulation X's existing framework to identify ways to simplify and streamline the mortgage servicing rules. The CFPB is considering a proposal to streamline the mortgage servicing rules, only if it would promote greater agility on the part of mortgage servicers in responding to future economic shocks while also continuing to ensure they meet their obligations for assisting borrowers promptly and fairly.

The findings in this report cover select examinations regarding mortgage servicing, that were completed from April 1, 2023 through December 31, 2023. To maintain the anonymity of the

[1] 12 U.S.C. §§ 5531, 5536

[2] If a supervisory matter is referred to the Office of Enforcement, Enforcement may cite additional violations based on these facts or uncover additional information that could impact the conclusion as to what violations may exist.

supervised institutions discussed in *Supervisory Highlights*, references to institutions generally are in the plural and related findings may pertain to one or more institutions.

2. Supervisory Observations

2.1 Mortgage Servicing

Examiners found that mortgage servicers engaged in UDAAPs and regulatory violations while processing payments by overcharging certain fees, failing to adequately describe fees in periodic statements, and not making timely escrow account disbursements. Additionally, as in prior editions of *Supervisory Highlights*, examiners identified persistent UDAAP and regulatory violations at mortgage servicers related to loss mitigation practices.

2.1.1 Unfair charges for property inspections prohibited by investor guidelines

Mortgage investors generally require servicers to perform property inspection visits for accounts that reach a specified level of delinquency. Investor guidelines stipulate when servicers should complete these property inspections. Servicers pass along the cost of property inspections to the consumers; the fees for this action generally range from $10 to $50.

Examiners found that servicers engaged in unfair acts or practices by charging property inspection fees on Fannie Mae loans where such inspections were prohibited by Fannie Mae guidelines. The CFPA defines an unfair act or practice as an act or practice that: (1) causes or is likely to cause substantial injury to consumers; (2) is not reasonably avoidable by consumers, and (3) is not outweighed by countervailing benefits to consumers or to competition.[3]

Fannie Mae guidelines prohibit property inspections if the property is borrower-or tenant-occupied and one of the following applies: the servicer has established quality right party contact with the borrower within the last 30 days, the borrower made a full payment within the last 30 days, or the borrower is performing under a loss mitigation option or bankruptcy plan. Examiners found that in some instances a servicer would charge a property inspection fee on Fannie Mae loans even though the property was borrower-or tenant-occupied and the servicer had established quality right party contact within 30 days, the borrower had made a full payment within the last 30 days, or the borrower was performing under a loss mitigation option. In total, the servicers charged hundreds of borrowers fees for property inspections that were prohibited by Fannie Mae's guidelines, causing consumers substantial injury. Consumers were unable to anticipate the property inspection fees or mitigate them because they have no

[3] 12 U.S.C. §§ 5531, 5536.

influence over the servicer's practices. Charging improper fees has no benefit to consumers or competition. In response to these findings, the servicers corrected automation flaws behind some of the improper charges and implemented testing and monitoring to address the others. The servicers were also directed to identify and remediate borrowers who were charged fees contrary to investor guidelines.

2.1.2 Unfair late fee overcharges

Examiners found that servicers engaged in unfair acts or practices by assessing unauthorized late fees.[4] These errors occurred for one of two reasons. First, in some instances servicers charged late fees that exceeded the amount allowed in the loan agreement. Second, in some instances servicers charged late fees even though consumers had entered into loss mitigation agreements that should have prevented late fees. Examiners found these practices constituted unfair acts or practices.

The servicers caused substantial injury to consumers when they imposed these unauthorized late fees. Consumers could not reasonably avoid the injury because they do not control how servicers calculate late fees and had no reason to anticipate that servicers would impose unauthorized late fees. Charging unauthorized late fees had no benefits to consumers or competition. In response to these findings, servicers refunded the fees and improved internal processes.

2.1.3 Failing to waive existing fees following acceptance of COVID-19 loan modifications

Regulation X generally allows certain servicers to offer streamlined loan modifications made available to borrowers experiencing a COVID-19 related hardship based on the evaluation of incomplete loss mitigation applications if the modifications meet certain requirements.[5] One requirement is that the servicer "waives all existing late charges, penalties, stop payment fees, or similar charges that were incurred on or after March 1, 2020, promptly upon the borrower's acceptance of the loan modification."[6]

[4] Supervision previously reported a similar unfair act or practice of overcharging late fees in *Supervisory Highlights*, Issue 29 (Winter 2023), available at: https://www.consumerfinance.gov/compliance/supervisory-highlights/

[5] 12 CFR 1024.41(c)(vi)(A).

[6] 12 CFR 1024.41(c)(vi)(A)(5).

Examiners found that servicers offered streamlined COVID-19 loan modifications but, in violation of Regulation X, failed to waive existing fees after borrowers accepted the modifications. In response to these findings, servicers are remediating consumers.

2.1.4 Failing to provide adequate description of fees in periodic statements

Regulation Z requires servicers to provide billing statements that include a list of all transaction activity that occurred since the last statement, including, among other things, "a brief description of the transaction."[7] Examiners found that servicers failed to provide a brief description of certain fees and charges in violation of this provision when they used the general label "service fee" for 18 different fee types, without including any additional descriptive information. In response to these findings, the servicers implemented changes to provide more specific descriptions of each service fee.

2.1.5 Failing to make timely disbursements from escrow accounts

Regulation X requires servicers to make timely disbursements from escrow accounts if the borrower is not more than 30 days overdue.[8] Timely disbursements are defined as payments made on or before the deadline to avoid a penalty.[9] Examiners found servicers attempted to make timely escrow disbursements, but the payments did not reach the payees. The servicers did not resend the payments until months after the initial payment attempts. Some borrowers incurred penalties due to the late payments, which the servicers only reimbursed after the borrowers complained. Because the initial payments were unsuccessful, and the second payments were late, the servicers did not make timely disbursements and violated Regulation X. In response to these findings, the servicers were directed to comply with this regulation and remediate borrowers.

2.1.6 Deceptive loss mitigation eligibility notices

Examiners found that servicers engaged in deceptive acts or practices when they sent notices to consumers representing that the consumers had been approved for a streamlined loss

[7] 12 C.F.R. § 1026.41(d)(4).

[8] 12 C.F.R. § 1024.17(k)(1).

[9] *Id*.

mitigation option even though the servicers had not yet determined whether the consumers were eligible for the option. In fact, some consumers were ultimately denied the option.

An act or practice is deceptive when: (1) the representation, omission, act, or practice misleads or is likely to mislead the consumer; (2) the consumer's interpretation of the representation, omission, act, or practice is reasonable under the circumstances; and (3) the misleading representation, omission, act, or practice is material.[10]

The notices were misleading because the servicers had not yet determined the consumers were eligible for the loss mitigation option. Consumers reasonably interpreted the representations to mean that the loss mitigation option was available to them. The representations were material because consumers could have made budgeting decisions on the false assumption that they were approved for a loss mitigation option or were discouraged from submitting complete loss mitigation applications or taking other steps to cure their delinquencies and avoid foreclosure. In response to these findings, the servicers reviewed affected borrowers who remained delinquent to ensure they were considered for appropriate loss mitigation options.

2.1.7 Deceptive delinquency notices

Examiners found that servicers engaged in deceptive acts or practices when they sent notices informing certain consumers that they had missed payments and should fill out loss mitigation applications. In fact, these consumers did not need to make a payment because they were current on their payments, in a trial modification plan, or had an inactive loan (e.g., loan was paid off or subject to short sale). These misrepresentations were likely to mislead consumers and it was reasonable for consumers under the circumstances to believe that the notices from their servicers were accurate. The representations were material because they were likely to influence consumers' course of conduct. For example, in response to the notice, a consumer may contact their servicer to correct the error or fill out unnecessary loss mitigation applications. In response to these findings, servicers are implementing additional policies and procedures to ensure accuracy of notices.

2.1.8 Loss mitigation violations

Regulation X generally requires servicers to send borrowers a written notice acknowledging receipt of their loss mitigation application and notifying the borrowers of the servicers' determination that the loss mitigation application is either complete or incomplete after

[10] *Consumer Financial Protection Bureau v. Gordon*, 819 F.3d 1179, 1192 (9th Cir. 2016).

receiving the application.[11] Examiners found that servicers violated Regulation X by sending acknowledgment notices to borrowers that failed to specify whether the borrowers' applications were complete or incomplete.

Additionally, after receiving borrowers' complete loss mitigation applications, Regulation X generally requires servicers to provide borrowers with a written notice stating the servicers' determination of which loss mitigation options, if any, the servicers will offer to the borrower.[12] Among other requirements, the written notice must include the amount of time the borrower has to accept or reject an offer of a loss mitigation option.[13] Examiners found that servicers violated Regulation X because the servicers did not provide timely notices stating the servicers' determination regarding loss mitigation options. The servicers were directed to enhance policies and procedures to ensure timely loss mitigation determinations. One servicer also violated Regulation X because its written notices did not provide a deadline for accepting or rejecting loss mitigation offers. In response to the finding, the servicers updated the offer letter templates to include a deadline to accept or reject the loss mitigation offer.

Finally, Regulation X requires servicers to maintain policies and procedures that are reasonably designed to ensure that they can properly evaluate borrowers who submit applications for all available loss mitigation options for which they may be eligible.[14] Examiners found that servicers violated Regulation X because they failed to maintain policies and procedures reasonably designed to achieve this objective. Specifically, the servicers did not follow investor guidelines for evaluating loss mitigation applications when they automatically denied certain consumers a payment deferral option rather than submitting the consumers' applications to the investor for review. In response to these findings, the servicers updated their policies and procedures and refunded or waived late charges and corrected negative credit reporting for impacted consumers.

2.1.9 Live contact and early intervention violations

Regulation X requires servicers to make good faith efforts to establish live contact with delinquent borrowers no later than the 36th day of delinquency.[15] Examiners found that servicers violated this provision when they failed to make good faith efforts to establish live

[11] 12 C.F.R. § 1024.41(b)(2)(i)(B). This notice is only required if the servicer receives a loss mitigation application 45 days or more before a foreclosure sale.

[12] 12 C.F.R. § 1024.41(c)(1). This notice is only required if the servicer receives a complete loss mitigation application more than 37 days before a foreclosure sale.

[13] 12 C.F.R. § 1024.41(c)(1)(ii).

[14] 12 C.F.R. § 1024.38(b)(2)(v).

[15] 12 C.F.R. § 1024.39(a).

contact with hundreds of delinquent borrowers. The servicers took corrective action which included providing remediation to harmed borrowers including refunding or waiving late fees.

Regulation X also requires servicers to provide written early intervention notices to delinquent borrowers no later than the 45th day of delinquency and again every 180 days thereafter.[16] Examiners found that servicers violated this provision when they failed to send written early intervention notices to thousands of delinquent borrowers. In response to these findings, the servicers identified and provided remediation to affected borrowers who were assessed late fees for missed payments after the 45th day of delinquency.

2.1.10 Failing to retain records documenting actions taken on mortgage loan accounts

Regulation X requires servicers to retain records documenting actions taken with respect to a borrower's mortgage loan account until one year after the date the loan was discharged or servicing of the loan was transferred to another servicer.[17] Examiners found that servicers failed to document certain actions in their servicing systems, such as establishing live contact with borrowers, in violation of this provision. In response to these findings, the servicers were directed to enhance training and monitoring to ensure compliance with this requirement.

[16] 12 C.F.R. § 1024.39(b)(1).

[17] 12 C.F.R. § 1024.38(c)(1).

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

For Release

Federal Trade Commission Announces Proposed Rule Banning Fake Reviews and Testimonials

June 30, 2023

Tags: Consumer Protection | Bureau of Consumer Protection | Advertising and Marketing | Endorsements, Influencers, and Reviews | Online Advertising and Marketing

The Federal Trade Commission proposed a new rule to stop marketers from using illicit review and endorsement practices such as using fake reviews, suppressing honest negative reviews, and paying for positive reviews, which deceive consumers looking for real feedback on a product or service and undercut honest businesses.

"Our proposed rule on fake reviews shows that we're using all available means to attack deceptive advertising in the digital age," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The rule would trigger civil penalties for violators and should help level the playing fie for honest companies."

In its notice of proposed rulemaking, the Commission cited examples of clearly deceptive practices involving consumer reviews and testimonials from its past cases, and noted the widespread emergence of generative AI, which is likely to make it easier for bad actors to write fake reviews.

The Commission is seeking comments on proposed measures that would fight these clearly deceptive practices. For example, the proposed rule would prohibit:

- **Selling or Obtaining Fake Consumer Reviews and Testimonials:** The proposed rule would prohibit businesses from writing or selling consumer reviews or testimonials by someone who does not exist, who did not have experience with the product or

service, or who misrepresented their experiences. It also would prohibit businesses from procuring such reviews or disseminating such testimonials if the businesses knew or should have known that they were fake or false.

- **Review Hijacking:** Businesses would be prohibited from using or repurposing a consumer review written for one product so that it appears to have been written for a substantially different product. The FTC recently brought its first review hijacking enforcement action.

- **Buying Positive or Negative Reviews:** Businesses would be prohibited from providing compensation or other incentives conditioned on the writing of consumer reviews expressing a particular sentiment, either positive or negative.

- **Insider Reviews and Consumer Testimonials:** The proposed rule would prohibit a company's officers and managers from writing reviews or testimonials of its products or services, without clearly disclosing their relationships. It also would prohibit businesses from disseminating testimonials by insiders without clear disclosures of their relationships, and it would prohibit certain solicitations by officers or managers of reviews from company employees or their relatives, depending on whether the businesses knew or should have known of these relationships.

- **Company Controlled Review Websites:** Businesses would be prohibited from creating or controlling a website that claims to provide independent opinions about a category of products or services that includes its own products or services.

- **Illegal Review Suppression:** Businesses would be prohibited from using unjustified legal threats, other intimidation, or false accusations to prevent or remove a negative consumer review. The proposed rule also would bar a business from misrepresenting that the reviews on its website represent all reviews submitted when negative reviews have been suppressed.

- **Selling Fake Social Media Indicators:** Businesses would be prohibited from selling false indicators of social media influence, like fake followers or views. The proposed rule also would bar anyone from buying such indicators to misrepresent their importance for a commercial purpose.

The proposed rule follows an advance notice of proposed rulemaking the Commission announced last November. The FTC received comments from individual consumers, trade associations, review platform operators, small businesses, consumer advocacy organizations, entities dedicated to fighting fake reviews, and academic researchers.

Although the FTC has taken strong enforcement action in this area recently, case-by-case enforcement without civil penalty authority might not be enough to deter clearly deceptive review and testimonial practices. The Supreme Court's decision in *AMG Capital Management LLC v. FTC* has hindered the FTC's ability to seek monetary relief for consumers under the FTC Act. A rule clearly spelling out prohibited practices and allowing for the judicial imposition of civil penalties could strengthen deterrence and FTC enforcement actions.

The notice includes questions for public comment to inform the Commission's decision-making on the proposal. These questions focus on provisions in the proposed rule and whether other provisions should or should not be included in the rule. After the Commission reviews the comments received, it will decide whether to take the necessary next steps toward issuing a final rule.

The Commission vote to approve the NPRM was 3-0. Instructions for filing comments appear in the Federal Register notice. Comments must be received by September 29, 2023.

The primary staff member on these matters is Michael Ostheimer in the FTC's Bureau of Consumer Protection.

The Federal Trade Commission works to promote competition and protect and educate consumers. The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. Learn more about consumer topics at consumer.ftc.gov, or report fraud, scams, and bad business practices at ReportFraud.ftc.gov. Follow the FTC on social media, read consumer alerts and the business blog, and sign up to get the latest FTC news and alerts.

Press Release Reference

FTC Sues Walmart for Facilitating Money Transfer Fraud That Fleeced Customers Out of Hundreds of Millions

Contact Information

Media Contact

Office of Public Affairs
Office of Public Affairs
202-326-2180

News Release

FHFA Releases Mortgage Loan and Natural Disaster Dashboard

Agency unveils online tool using existing information to estimate county-level damages and mortgage loan concentrations in disaster-prone areas, and to identify U.S. communities most vulnerable to natural hazards.

FOR IMMEDIATE RELEASE

09/09/2024

Washington, D.C. – The Federal Housing Finance Agency (FHFA) released an online risk analysis tool that provides geographic estimates for physical risks from various types of natural disasters as well as nationwide data on housing and the mortgage market.

The tool — known as the Mortgage Loan and Natural Disaster Dashboard— is intended to give property owners, community leaders, financial institutions, policymakers, and other stakeholders better insight into which areas of the country are most likely to incur greater damages from hurricanes, flooding, wildfires, and other types of natural hazards.

Users can combine FHFA's Public Use Database (PUDB) with data on previous disasters and other analysis from the Federal Emergency Management Agency (FEMA). They can identify areas of the country with elevated disaster risk based on several factors, and which of those areas have concentrations of properties financed with loans acquired by Fannie Mae, Freddie Mac, and the Federal Home Loan Banks.

Scientists widely attribute more intense storm seasons — along with higher human and financial costs — in recent years to climate risks. Tools such as FHFA's new dashboard provide stakeholders with greater visibility of communities already facing economic challenges that are susceptible to natural disasters.

"Climate risks, especially natural disasters, pose a serious threat to housing and other critical infrastructure, particularly in vulnerable communities," said FHFA Director Sandra L. Thompson. "Providing geographic information on disasters as well as concentrated exposures of loans acquired by our regulated entities can help policymakers and the industry develop solutions to better safeguard those communities from the impact of future catastrophes."

The dashboard utilizes data from three publicly available sources. The PUDB provides a geographic breakdown of loans acquired by FHFA's regulated entities. FEMA's National Risk Index identifies communities most at risk for 18 types of natural hazards. The third source, FHFA's Duty to Serve High-Needs Rural Areas data, pinpoints rural areas in the country that are characterized by a high concentration of poverty and substandard housing conditions.

The data on mortgages were updated as of 2022 and the data on past natural disasters reflected in the online tool were updated as of 2023, while the Census tracts were drawn from the 2020 U.S. Census. Dashboard users can view nationwide mortgage data at the Census-tract level overlaid with expected annual damages for 18 different types of natural disasters.

Additional layers measure other factors affecting an area's susceptibility to certain disasters, including a social vulnerability index, a community resilience index, and an additional layer enabling users to analyze FHFA's Duty to Serve High-Needs Rural areas.

FHFA released this dashboard along with a blog post and answers to frequently asked questions (FAQs), outlining potential uses of the new data tool and how disaster assistance resources developed by federal agencies and the Enterprises can assist homeowners affected by natural disasters.

Related Resources:

Mortgage Loan and Natural Disaster Dashboard

FHFA Mortgage Loan and Natural Disaster Dashboard Blog: A Case Study of Hurricane Beryl

Mortgage Loan and Natural Disaster Dashboard Instructions and FAQs

Instructions

Overview

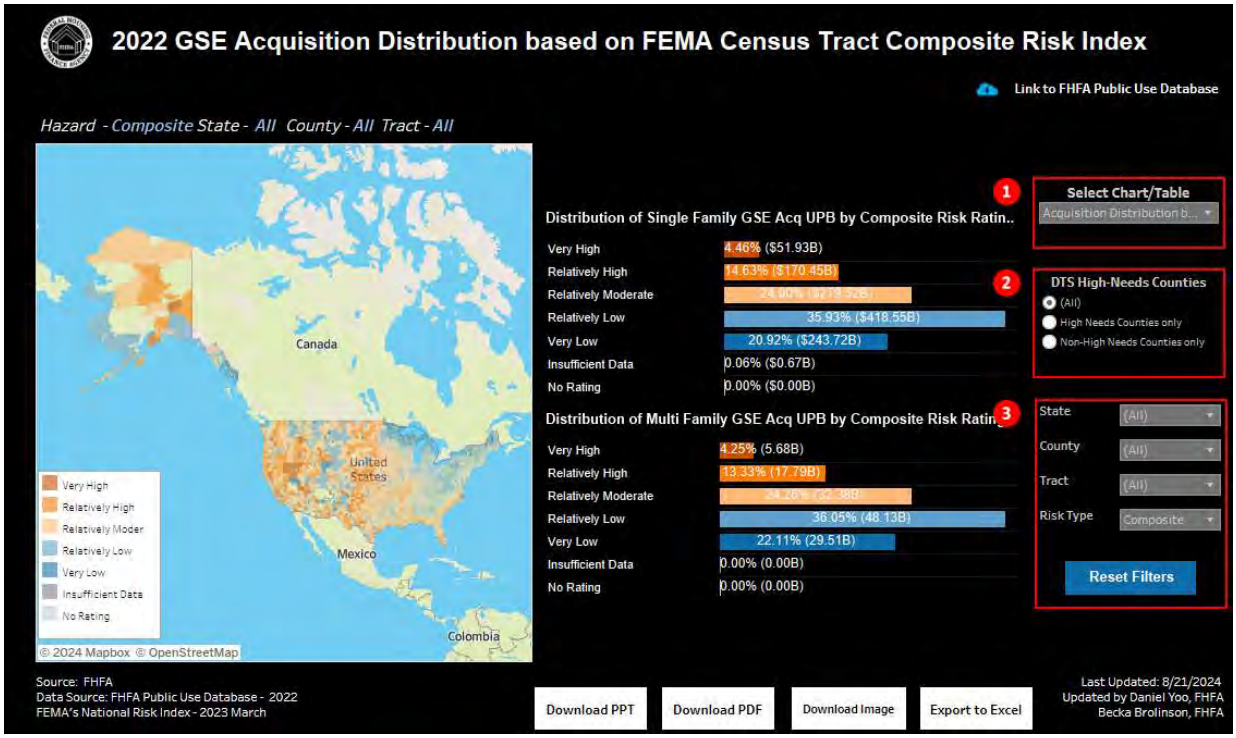


Figure 1: Dashboard Landing Page

The official name of the dashboard is the “Mortgage Loan and Natural Disaster Dashboard,” but throughout these FAQs we will refer to it as the “dashboard” for simplicity. The default settings of the dashboard show the nationwide map with the census-tract-level composite National Risk Index (NRI) Ratings. The filters are located on the dashboard's right side, allowing the user to navigate the map, charts, and tables in the dashboard.

The first filter box, "Select Chart/Table," will enable you to browse various information in the dashboard. The "Acquisition" option in the filter shows the loan acquisition counts and total acquisition unpaid principal balance (UPB) of the loans

indices and Expected Annual Losses from the selected hazard. It also provides state and national averages of NRI indices. The "Acquisition Distribution by Risk Rating" tab shows the distributions of acquisition UPB by the risk ratings for selected hazards. It provides nationwide distribution, as well as for the selected state, county, and census tract.

The filter box number 2, "Duty to Serve High Needs Area," allows users to keep only the Duty to Serve high needs areas or exclude them from their results.

The last filter box lets users change the geographic area. It applies to all the maps, tables, and charts in the dashboard. The dashboard shows the nationwide result when all the geographic filters are (all). Once a state is selected, the results will be state-level, once a county is selected, the results will be county-level, and once a tract is selected, the results will be tract-level. The dashboard provides information down to the census-tract level.

Acquisition Distribution by Risk Rating Tab

The Acquisition Distribution by Risk Rating Tab in the “Select Chart/Table” filter shows the total acquisition UPB distributed in each risk rating category. The first chart shows the Single-Family Acquisition UPB distribution, and the chart below shows the Multifamily Acquisition UPB distribution. Figure 1 shows the nationwide information by composite risk rating. Selecting communities and hazards in the filter box, number 3 in Figure 1, allows users to see the UPB distribution of a state, county, and census tract by 18 hazards.

National Risk Index Tab

The National Risk Index tab in the “Select Chart/Table” filter shows the census tract-level risk index for 18 hazards and composite risk. These represent census tract-level data, and no results will be shown unless a census tract is selected in the geographic filter area.

Once a state is selected in the “State” filter, the map will zoom to the state and the state averages will be populated. Once the “County” filter is selected, the map will

Resilience Index. The first column of the circles shows the census tract's index, the state average index in the second column, and the national average in the third. Below the colored circles are the census tract-level expected annual losses for composite risk and the selected hazard. To see total expected annual loss broken down into each hazard type for the selected census tract, hover over any of the "Expected Annual Loss Composite ($)" cells. The tab provides information on 18 hazards and composite risk, and users can select hazard in the "Risk Type" filter in the third filter box.

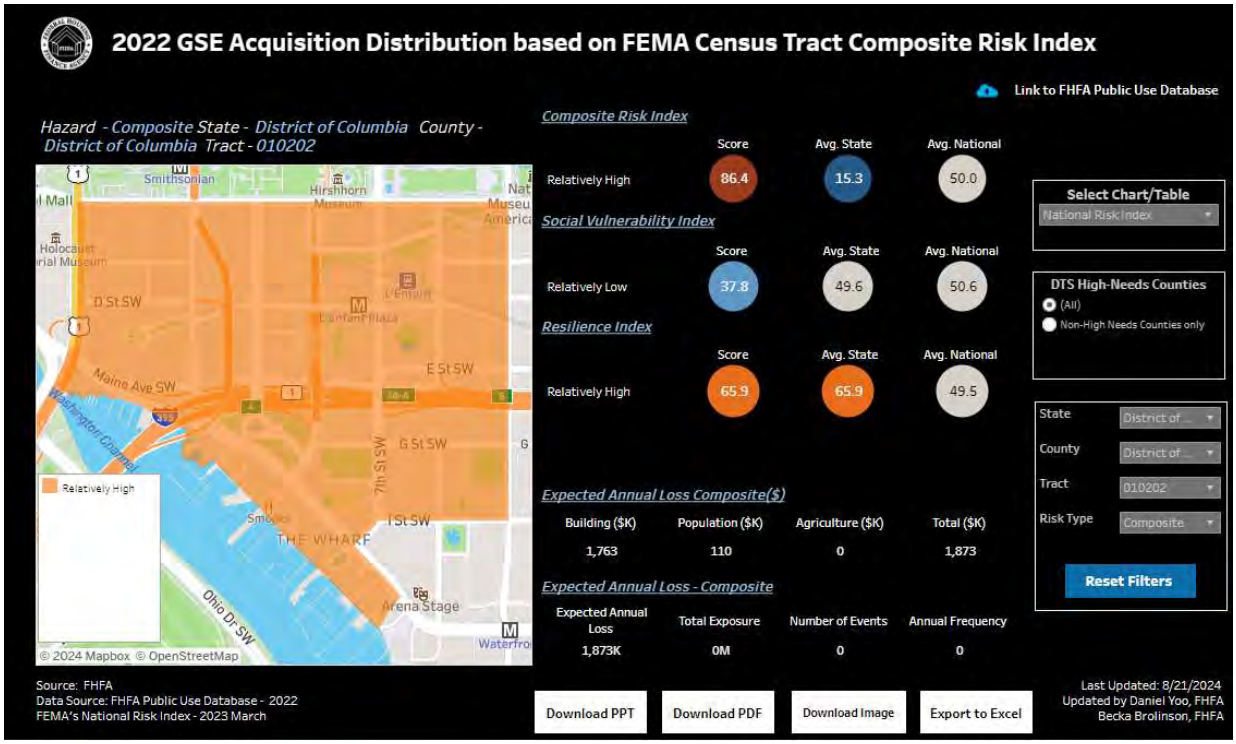


Figure 2: Example of National Risk Index Information for Composite Risk

Acquisition Tab

The Acquisition tab shows the counts and total acquisition UPB of the loans purchased by Fannie Mae, Freddie Mac, and the Federal Home Loan Banks (FHLBanks) in 2022. The geographic filters allow users to find the statistics for the communities in which they are interested. Once the filters are selected, the tab will show the information for the selected state, county, and census tract.

FEDERAL HOUSING FINANCE AGENCY

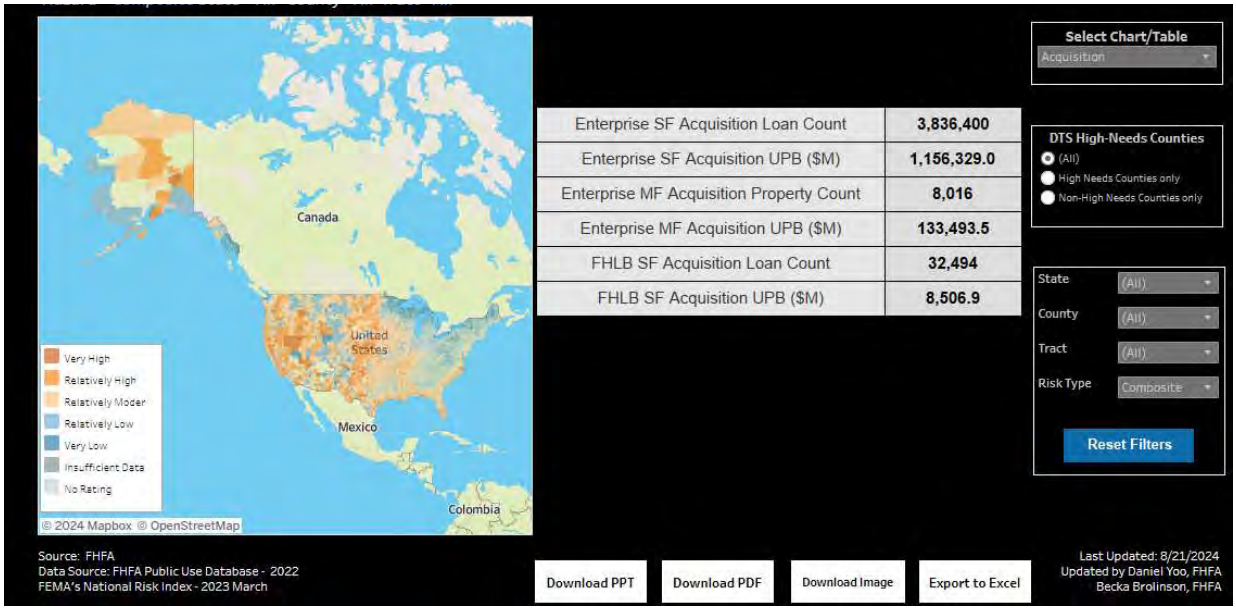


Figure 3: Acquisition Tab

Frequently Asked Questions

For questions regarding FEMA's NRI data, please refer to the technical documentation here.

- **Why are "National Risk Index" and "Expected Annual Loss" blank in the default setting?**
    - The National Risk Index Score and Expected Annual Loss (Figure 4, highlighted in red) are census tract-level data. It will be blank until a "State," "County," and "Tract" in the Filter section is selected (Figure 4, highlighted in yellow). The census-level information will be populated once a census tract is selected, as shown in Figure 5.
    - The "Avg. State" represents an average of indices in the census tracts in a selected state and it will be populated once a State is selected.

FEDERAL HOUSING FINANCE AGENCY

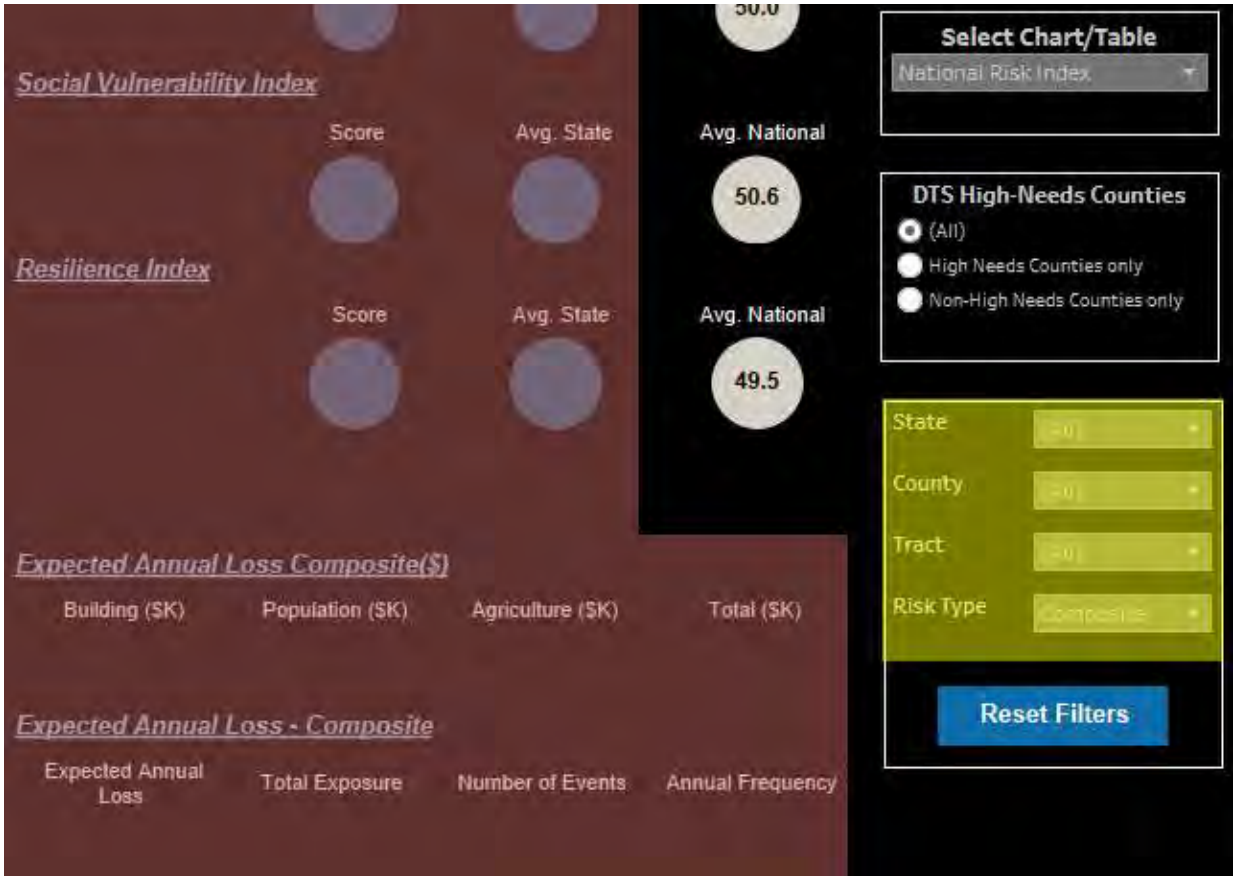


Figure 4: NRI and EAL

FEDERAL HOUSING FINANCE AGENCY

Figure 5: NRI and EAL Populated with Census-Tract Selection

- **What information about natural hazard risk does the NRI provide?**
    - The NRI provides information about the relative risk of a hazard in a particular community. Because the hazard data is scaled to the national level, within a particular hazard the risks can be compared across communities, but it is more difficult to compare within a community across hazard types. For example, the 90th percentile risk of a hurricane will have different expected losses than the 90th percentile risk for a winter storm.
- **How to select states or counties in the geographic filter area?**
    - The geographic filter is located in the last square box on the right-hand side of the dashboard (Figure 1, filter box number 3).
    - **To select single or multiple States or Counties**

disappear. Select State/County one by one, and it will generate the chart and tables for the selected area.

- **To Select All States or Counties**
  - Open the State or County filter drop-down menu and select (All). To see all-state results, click "Reset Button."

- **The map doesn't move automatically when I select a geographic area in the filter.**
  - The Tableau map will be fixed when a user pans or zooms in the map. Unfix the map by clicking "Zoom Home" (Figure 6).

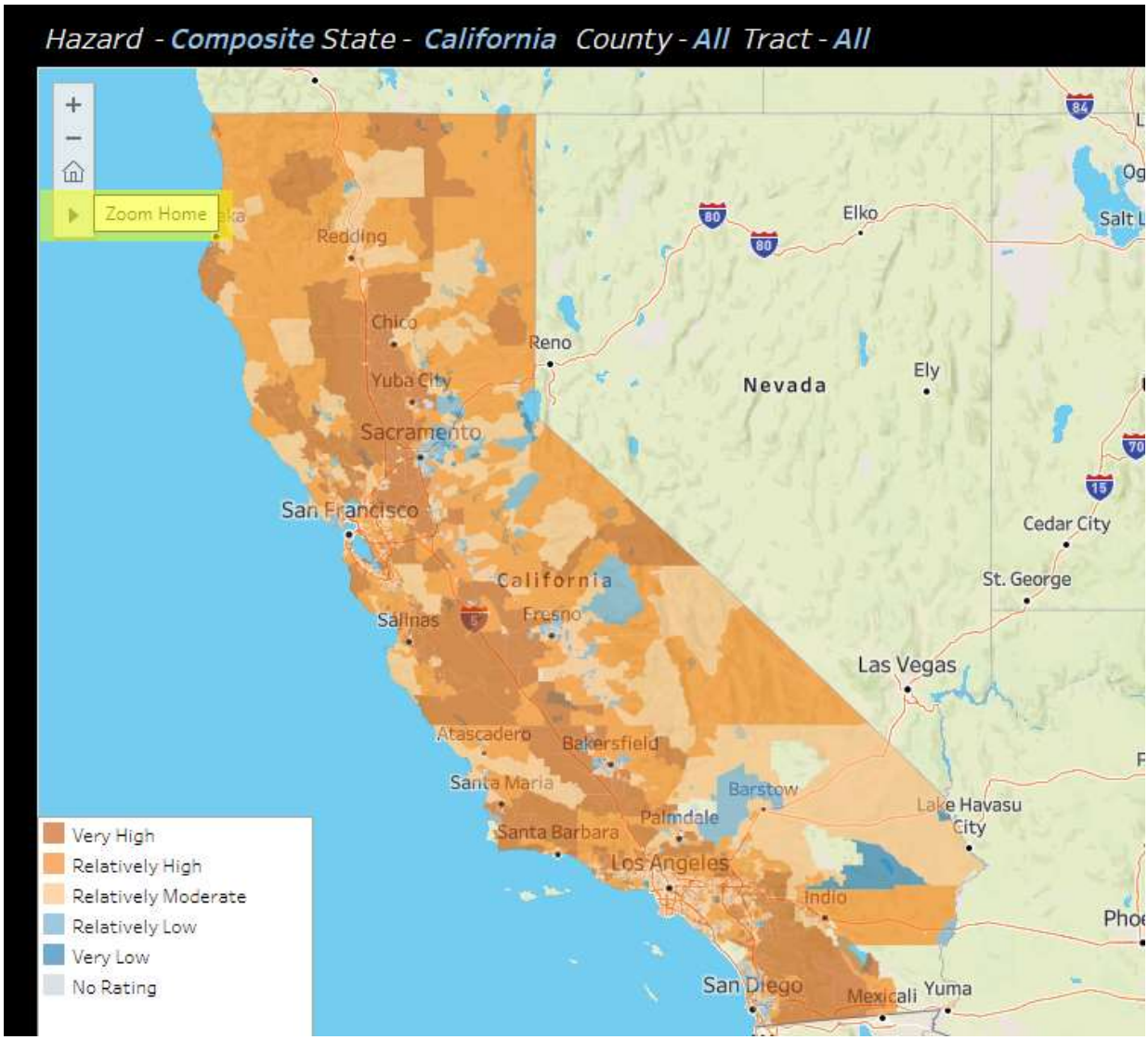


Figure 6: How to Unfix the Map

    - "high-needs rural region" as any of the following regions provided the region is located in a "rural area":
        1. Middle Appalachia;
        2. the Lower Mississippi Delta;
        3. a colonia census tract; or
        4. a tract located in a persistent poverty county and not included in Middle Appalachia, the Lower Mississippi Delta, or a colonia census tract.

- **The Duty to Serve High-Needs Area filter doesn't give me any options.**
    - The "High-needs areas only" option is unavailable when there is no Duty to Serve High-Needs area in the selected map region. Likewise, the "Non-High-needs areas only" option is not available when there are only Duty to Serve High-Needs rural areas in the selected map region.
- **What are the differences between Insufficient Data, No Rating, and Not Applicable in Risk Ratings?**
    - If a community is displayed in the application as having "No Expected Annual Loss" for the selected hazard type, the rating will show "No Rating" for its Risk Index for that hazard type. "No Rating" indicates that this community does not have any expected physical risk for the selected hazard type.
    - If a factor used to calculate the Expected Annual Loss of a census tract or county for a hazard type has a null value, the community is rated as having "Insufficient Data."
    - The communities are displayed as "Not Applicable" if communities are located where no documented risk exists for the hazard type and where the hazard type is deemed not likely to occur.
    - Please review page 36 of FEMA's NRI Technical Document for more details.

"Select Chart/Table" filter and select other filters based on your interest. Then click "Export to Excel" and select "Acquisition." Select a format and click "Download."

- To export the "Acquisition Distribution by Risk Rating" Tab results, click "Acquisition Distribution by Risk Rating" in the "Select Chart/Table" filter and select other filters based on your interest. Then click "Export to Excel" and select "DIST-SF" to download Single-Family distribution. Select a format and click "Download." Click "Export to Excel" again and download "DIST-MF." Combine the two Excel files.
- To export the "National Risk Index" Tab results, click "National Risk Index" in the "Select Chart/Table" filter and select other filters based on your interest. Then click "Export to Excel" and select "NRI-1" to download Single-Family distribution. Select a format and click "Download." Do the same process for NRI-2 to NRI-5 as well and combine those.

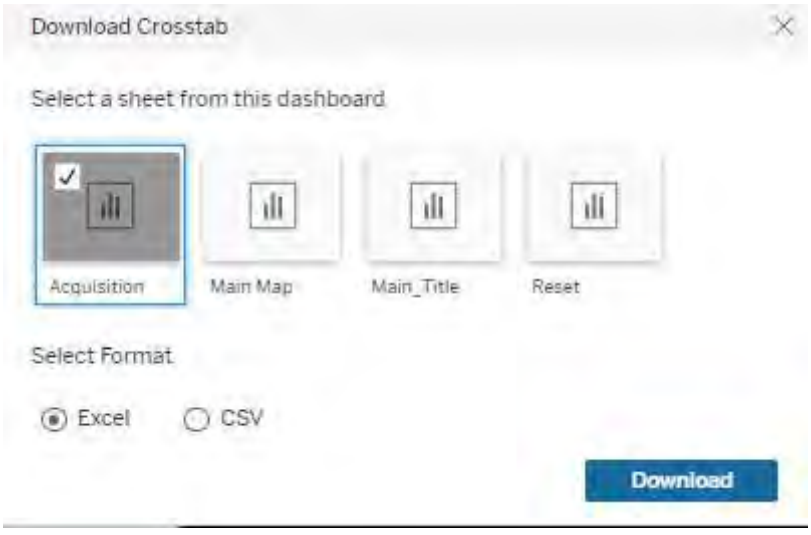


Figure 7: Export to Excel Example

- **How can I download data embedded in the dashboard?**
  - To download the complete imported data underlying the dashboard, reset all the filters. Then, click an empty space on the map. Click the "Choose a format to download" button at the bottom of the dashboard

- To download aggregated PUDB data, go to "GSE_2022" in the "View Data" pop-up window and click "Download all rows as a text file." Please check Appendix I for the data dictionary for GSE_2022.
- To download NRI data, go to "NRI_CensusTacts" in the "View Data" pop-up window and click "Download all rows as a text file." Please check Appendix II for the data dictionary for NRI_CensusTacts.

Figure 8: Choose a format to download button

Appendix I: Data Dictionary - GSE_2022

Field Name	Field Description
State	State Name
County	County Name
Tract	2020 Census Tract
Tractfips	State-County-Tract FIPS Code
Stcofips	State-County FIPS Code
Ym	Acquisition Year
pov_ind	Persistent Poverty County Indicator

Risk_Rating_S	National Risk Index Rating for selected Hazard
rural_ind	Rural area for purposes of Duty to Serve Indicator
Gsel	SF Loan Count - Purchased by Enterprise
Gsemfl	MF Property Count - Purchased by Enterprise
Gseu	Total SF Acquisition UPB - Purchased by Enterprise
Gsemfu	Total MF Acquisition UPB - Purchased by Enterprise
Hlbl	SF Loan Count - Purchased by FHLBanks
Hlbu	Total SF Acquisition UPB - Purchased by FHLBanks

Appendix II: Data Dictionary - NRI_Census_Tracts

Field Name	Field Description
State	State Name
County	County Name
Tract	2020 Census Tract
Stcofips	State-County-Tract FIPS Code

Tractfips	State-County FIPS Code
pov_ind	Persistent Poverty County Indicator
Risk_Rating_S	National Risk Index Rating for selected Hazard
rural_ind	Rural area for purposes of Duty to Serve Indicator
Avln Riskr	Hazard Type Risk Index Rating - Avalanche
Cfld Riskr	Hazard Type Risk Index Rating - Coastal Flooding
Cwav Riskr	Hazard Type Risk Index Rating - Cold Wave
Drgt Riskr	Hazard Type Risk Index Rating - Drought
Erqk Riskr	Hazard Type Risk Index Rating - Earthquake
Hail Riskr	Hazard Type Risk Index Rating - Hail
Hwav Riskr	Hazard Type Risk Index Rating - Heat Wave
Hrcn Riskr	Hazard Type Risk Index Rating - Hurricane
Istm Riskr	Hazard Type Risk Index Rating - Ice Storm
Lnds Riskr	Hazard Type Risk Index Rating - Landslide
Ltng Riskr	Hazard Type Risk Index Rating - Lightning

Rfld Riskr	Hazard Type Risk Index Rating - Riverine Flooding
Swnd Riskr	Hazard Type Risk Index Rating - Strong Wind
Trnd Riskr	Hazard Type Risk Index Rating - Tornado
Tsun Riskr	Hazard Type Risk Index Rating - Tsunami
Vlcn Riskr	Hazard Type Risk Index Rating - Volcanic Activity
Wfir Riskr	Hazard Type Risk Index Rating - Wildfire
Wntw Riskr	Hazard Type Risk Index Rating - Winter Weather
Risk Ratng	Hazard Type Risk Index Rating - Composite
Resl Ratng	Community Resilience - Rating
Sovi Ratng	Social Vulnerability - Score

[1] Please see the link here for more information about FHFA's Duty to Serve High-Needs Rural areas.

FFIEC Information Technology Examination Handbook

Development, Acquisition, and Maintenance

AUGUST 2024

INTRODUCTION

The "Development, Acquisition, and Maintenance" booklet is one in a series of booklets that compose the *Federal Financial Institutions Examination Council (FFIEC)*[1] *Information Technology Examination Handbook (IT Handbook)*. The *FFIEC IT Handbook* is prepared for use by examiners.[2] With the publication of this booklet, the FFIEC members replace the "Development and Acquisition" booklet issued in April 2004. The revised title now reflects the importance of maintenance in the life of a system or component.[3] This booklet

- Describes system and component development, acquisition, and maintenance.
- Highlights key risk management practices when developing, acquiring, or maintaining systems and components.
- Provides an overview of and discusses information technology (IT) project management, the system development life cycle (SDLC), and supply chain risk management (SCRM).
- Addresses the importance of system and software maintenance to an entity's resilience.

For *FFIEC IT Handbook* purposes, the term "entity" includes depository financial institutions,[4] nonbank financial institutions,[5] bank holding companies,[6] savings and loan holding companies,[7] and third-party service providers.[8]

[1] The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. 95-630. The FFIEC comprises the principals of the Board of Governors of the Federal Reserve System (FRB), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the State Liaison Committee (SLC).

[2] Each FFIEC member uses the principles outlined in this booklet consistent with the member's supervisory authority.

[3] Examples of systems and components include hardware, firmware, software, peripherals, and network components.

[4] The term "depository financial institution" includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions.

[5] The term "nonbank financial institution" includes nondepository financial institutions under the jurisdiction of either state banking departments or the CFPB.

[6] The term "bank holding company" includes any company that has control over any bank or over any company that is or becomes a bank holding company as defined by the Bank Holding Company Act.

[7] The term "savings and loan holding company" includes any company that directly or indirectly controls a savings association or controls any other company that is a savings and loan holding company as defined by the Home Owners' Loan Act.

[8] The term "third-party service provider" means third parties that provide services, the provision of which is subject to examination under the Bank Service Company Act, the Home Owners' Loan Act, the Dodd–Frank Wall Street Reform and Consumer Protection Act, or other relevant law.

This booklet does not impose new requirements on entities. Instead, this booklet describes the principles and practices that examiners can use when assessing an entity's system development, acquisition, and maintenance activities.

Appendix A of this booklet provides objectives-based examination procedures. Application of principles and related examination procedures will vary consistent with the examined entity's complexity and risk profile (including the size of the entity or the nature of the systems and components).

I OVERVIEW OF DEVELOPMENT, ACQUISITION, AND MAINTENANCE

Development, acquisition, and maintenance activities are integral to an entity's operations. This booklet discusses how weaknesses in IT development, acquisition, and maintenance processes may lead to issues with confidentiality, integrity, availability, and resilience of the entity's systems, components, and data. Management determines the systems, products, and services that the entity will provide, whether to develop or acquire them, and how to maintain and service those systems, products, and services. Generally, whether developing or acquiring systems, products, and services, management performs some form of acquisition activity, including procurement. Management also oversees maintenance activities to prolong the life of systems and components (i.e., IT assets) and support continuity of operations. Management should plan for maintenance activities from the outset of acquisition or development to ensure secure continuity of operations. The following definitions and explanations provide an overview of IT development, acquisition, and maintenance.

Development: Systematic application of knowledge toward the production of useful materials, devices, and systems, or processes of defining, designing, testing, and implementing systems or components. Development includes validation and demonstration of a chosen technology, use of test and production environments, improvement of developed prototypes, integration into systems and subsystems, and inclusion of hardware builds. Development activities may be performed by the entity's personnel or third parties who develop systems and components on the entity's behalf. Management may choose to acquire systems and components from third parties and may customize them to meet the entity's needs.

Acquisition: All stages for acquiring products or services, beginning with determining the need for the product or service and ending with contract completion and closeout. Acquisition generally involves creating a relationship with a third party in the supply chain; therefore, effective SCRM is integral to the acquisition process. Acquisition activities include procurement processes that help ensure that management receives the contracted products or services. Acquisition activities, including procurement processes, help management achieve and maintain confidentiality, integrity, availability, as well as resilience, including supply chain resilience, throughout the life of systems and components.

Maintenance: Any act that either prevents the failure or malfunction of equipment or restores its operating capability. This includes incremental changes to improve performance. Maintenance activities include the processes to monitor systems and components and make changes (e.g., install patches and add new functions) to prevent their failure or malfunction and continue to meet user and customer needs. Management should perform preventive maintenance throughout the IT asset's useful life to prevent or minimize catastrophic failure and promote confidentiality, integrity, availability, and resilience. Maintenance may be performed by the entity's personnel or third parties. Maintenance activities should be performed regardless of the origin or location (e.g., geographic or virtual) of the systems or components.

The next section of this booklet addresses governance and risk management elements. Also addressed are common risk topics related to development, acquisition, and maintenance. The

booklet explains key topics, such as IT project management, SDLC, and supply chain risk management considerations, which are integral to development, acquisition, and maintenance activities to provide for ongoing operations. Appendices provide examination procedures, agency and industry references, and a glossary.

Consumer Financial Protection Bureau (cfpb.gov/)

CFPB Report Finds Large Retail Chains Charging Cash-back Fees to Customers Using Debit and Prepaid Cards

Closures of banks have created conditions for major dollar store chains to charge for cash back

AUG 27, 2024

WASHINGTON, D.C. – Today, the Consumer Financial Protection Bureau (CFPB) published a new report finding Americans are paying tens of millions of dollars in fees to access their own money when getting "cash back" at large retail stores when making a purchase with a debit or prepaid card. These cash-back fees are occurring against the backdrop of bank mergers, branch closures, and prevalence of out-of-network ATM fees that have reduced the supply of free cash access points for consumers.

"While retail chains had long provided cash back on debit card purchases for free, the CFPB has found that dollar store chains and other retailers are now charging fees for access to cash," said CFPB Director Rohit Chopra. "Many people living in small towns no longer have access to a local bank where they can withdraw money from their account for free. This has created the competitive conditions for retailers to charge fees for cash back."

Getting cash back at a store is a common way for people to get cash. While making a purchase at a retailer that offers the service, people can get access to their money by requesting cash back at the register. Retailers typically have pre-set withdrawal amounts, including maximum withdrawal limits. Consumers benefit from having the cash, and merchants benefit by having a way to attract consumers and reduce their cash-handling costs.

While this was often a convenient offering, getting cash at a store is sometimes the only option for people. Many retailers are filling a void in providing access to cash, as some communities lack access to a local bank. While some retailers have typically offered cash back for free, the CFPB's recent market scan suggests that this is changing, particular at dollar store chains.

The CFPB sampled eight large retail companies (Dollar General, Dollar Tree/Family Dollar, Kroger, Albertsons, Walgreens, CVS, Walmart and Target) and assessed their practices for

charging cash-back fees.

The report's findings include:

- **Cash-back fees cost consumers millions of dollars**. The CFPB found that three companies in the sample charge cash-back fees and estimates that they collect over $90 million in fees annually. The CFPB also estimates that the marginal cost to merchants for processing each transaction may be a few pennies, compared to the much higher fees these retailers charge consumers.
- **Cash-back fees are levied on low withdrawal amounts**. Many merchants pre-determine the withdrawal amount options in a single transaction, commonly between $5 and $50. Levying a fee on small transactions may constitute a hefty percentage of the withdrawal amount, and it may also induce repeat withdrawals, with consumers incurring a new fee each time.
- **Three major retail chains in the sample charged cash-back fees**. Dollar General, Dollar Tree/Family Dollar, and Kroger charge fees for this service while the other companies did not. At Dollar General and Dollar Tree/Family Dollar, cash-back fees for small withdrawal amounts are the highest in the sample ($1 fee or more for cash-back amounts under $50). Kroger, the country's largest grocery chain, recently announced new charges at their Harris Teeter stores (75 cents for $100 cash back or less), and charges 50 cents for up to $100 cash back at their other brand stores such as Ralph's, Fred Meyer, and others.
- **Consumers with lower incomes or fewer banking choices encounter cash-back fees disproportionately**. Dollar stores are frequently located in small rural towns, communities of color, and low-income communities. These areas are also more likely to have fewer bank branch locations and more residents reliant on cash for daily transactions than others.

Read today's report (cfpb.gov/data-research/research-reports/issue-spotlight-cash-back-fees/).

Read the Director's Notebook statement (cfpb.gov/about-us/blog/preserving-free-access-to-money-in-your-account/).

Employees of companies who they believe their company has violated federal consumer financial laws are encouraged to send information about what they know to whistleblower@cfpb.gov.

Consumers can submit complaints about financial products or services by visiting the CFPB's website (https://www.consumerfinance.gov/complaint/) or by calling (855) 411-CFPB (2372).

The Consumer Financial Protection Bureau is a 21st century agency that implements and enforces Federal consumer financial law and ensures that markets for consumer financial products are fair, transparent, and competitive. For more information, visit www.consumerfinance.gov (http://www.consumerfinance.gov/).

Consumer Financial Protection Bureau

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

Circular 2024-05

September 17, 2024

Consumer Financial Protection Circular 2024-05

Improper Overdraft Opt-In Practices

September 17, 2024

Question presented

Can a financial institution violate the law if there is no proof that it has obtained consumers' affirmative consent before levying overdraft fees for ATM and one-time debit card transactions?

Response

Yes. A bank or credit union can be in violation of the Electronic Fund Transfer Act (EFTA) and Regulation E if there is no proof that it obtained affirmative consent to enrollment in covered overdraft services. The form of the records that demonstrate consumer consent to enrollment may vary according to the channel through which the consumer opts into covered overdraft services.

Regulation E's overdraft provisions establish an opt-in regime, not an opt-out regime, where the default condition is that consumers are not enrolled in covered overdraft services. Financial institutions are prohibited from charging fees for such services until consumers affirmatively consent to enrollment. Violations of 12 CFR 1005.17(b)(1) can be proven in part by showing evidence that a consumer was charged an overdraft fee on a covered transaction where the available evidence does not adequately validate that the consumer opted in.[1]

Regulatory background

Regulation E implements the EFTA and governs the assessment of certain overdraft fees. Specifically, before a financial institution may charge a consumer a fee in connection with an

[1] Depending on the circumstances, a financial institution's overdraft practices may also implicate the CFPA's prohibition on unfair, deceptive, or abusive acts or practices. 12 U.S.C. 5531, 5536. *See e.g.,* Consumer Financial Protection Circular 2022-06, Unanticipated Overdraft Fee Assessment Practices (Oct. 26, 2022).

ATM or one-time debit transaction, Regulation E requires the financial institution to provide consumers with a "reasonable opportunity for the consumer to affirmatively consent, or opt in" to covered overdraft services, and to obtain the consumer's "affirmative consent, or opt in" to such services.[2] Institutions are also required to provide consumers with a written or electronic notice describing the institution's overdraft services prior to opt in, and to provide consumers with confirmation of the consumer's consent to enrollment in writing or electronically with a notice informing the consumer of the right to revoke such consent.[3] These rules do not apply to overdraft fees charged on written checks, recurring debit transactions, or ACH transactions.

Analysis

As noted above, Regulation E sets forth an opt-in, rather than opt-out, process before financial institutions are permitted to assess fees for covered overdraft services. The opt-in provisions provide that, absent affirmative enrollment by consumers, consumers' default status is to not be enrolled in covered overdraft services. Regulation E's opt-in provisions were established after the Federal Reserve Board found that consumers who were automatically enrolled in overdraft services may prefer to "avoid fees for a service they did not request."[4] Therefore, consistent with this opt-in design, when determining compliance with Regulation E's opt-in provisions, regulators and enforcers should inspect the financial institutions' records to determine whether there is evidence of affirmative consent to enrollment in covered overdraft services.

In the CFPB's supervisory work, examinations have found that some institutions have been unable to provide evidence that consumers had opted into overdraft coverage before they were charged fees for ATM and one-time debit transactions. While some institutions maintained policies and procedures relating to Regulation E's overdraft opt-in requirements, supervisory examinations found that the institutions were unable to show that these policies and procedures were actually followed with respect to individual consumers. In response to examination findings, institutions began maintaining records to prove the consumer's affirmative consent to enrollment in covered overdraft services.

In supervisory and enforcement work, the CFPB has also identified numerous other violations of law relating to Regulation E's overdraft opt-in requirements over the years. These violations have included, for example: the failure of institutions to obtain consumers' affirmative consent

[2] 12 CFR 1005.17(b)(1)(ii) & (iii).

[3] 12 CFR 1005.17(b)(1)(i) & (iv). 12 CFR 1005.13(b)(1) requires a person to retain evidence of compliance with the requirements of EFTA and Regulation E for a period of not less than two years from the date disclosures are required to be made or action is required to be taken. This is an independent legal obligation, which does not change the fact that the absence of records proving that an opt-in occurred is suggestive that a consumer did not opt in.

[4] Electronic Fund Transfers, 74 Fed Reg. 59033, 59038-59039 (Nov 17, 2009) (amending 12 CFR 205).

to enrollment in covered overdraft services,[5] and obtaining consumers' opt-in to covered overdraft services through deceptive and abusive acts or practices.[6] The prevalence of violations related to overdraft opt in underscores the need for effective supervision and enforcement of Regulation E's overdraft opt-in provisions.

Form of records evidencing opt-in

The form of the records that demonstrate consumer consent to enrollment may vary according to the channel through which the consumer opts into covered overdraft services. For example:

- For consumers who opt into covered overdraft services in person or by postal mail, a copy of a form signed or initialed by the consumer indicating the consumer's affirmative consent to opting into covered overdraft services would constitute evidence of consumer consent to enrollment.

- For consumers who opt into covered overdraft services over the phone, a recording of the phone call in which the consumer elected to opt into covered overdraft services would constitute evidence of consumer consent to enrollment.

- For consumers who opt into covered overdraft services online or through a mobile app, a securely stored and unalterable "electronic signature" as defined in the E-Sign Act (15 U.S.C. 7006(5)) conclusively demonstrating the specific consumer's action to affirmatively opt in and the date that the consumer opted in would constitute evidence of consumer consent to enrollment.

[5] *See e.g.*, CFPB Consent Order, In the Matter of Atlantic Union Bank, No. 2023-CFPB-0017 (December 7, 2023); CFPB Consent Order, In the Matter of Regions Bank, No. 2015-CFPB-0009 (April 28, 2015); Supervisory Highlights, Summer 2015 Edition, at 23, *available at* https://files.consumerfinance.gov/f/201506_cfpb_supervisory-highlights.pdf.

[6] *See e.g.*, CFPB Consent Order, In the Matter of TD Bank, N.A.. No. 2020-BCFP-0007 (August 20, 2020); *CFPB v. TCF National Bank*, Stipulated Final Judgment and Order, 17-cv-00166 (July 20, 2018).

Consumer Financial Protection Bureau (cfpb.gov/)

CFPB Orders TD Bank to Pay $28 Million for Breakdowns that Illegally Tarnished Consumer Credit Reports

TD Bank's illegal behavior threatened the ability of tens of thousands of consumers to access credit, housing, and employment

SEP 11, 2024

WASHINGTON, D.C. – Today, the Consumer Financial Protection Bureau (CFPB) ordered TD Bank to pay $7.76 million to tens of thousands of victims of the bank's illegal actions. For years, the bank repeatedly shared inaccurate, negative information about its customers to consumer reporting companies. The information included systemic errors about credit card delinquencies and bankruptcies. In addition to the redress, the CFPB is ordering TD Bank to pay a $20 million civil money penalty.

Consumer reports, including credit reports, employment screening reports, tenant screening reports, and other background reports, are used by financial institutions, employers, and landlords, among others, to decide whether to extend credit, housing, or employment to a consumer. The inaccurate information shared by TD Bank related to credit card and bank deposit accounts, including accounts TD Bank knew or suspected were fraudulently opened. After the bank realized it was botching its reporting to consumer reporting companies, it took far too long to correct many of its errors.

"The CFPB's investigation found that TD Bank illegally threatened the consumer reports of its customers with fraudulent information and then barely lifted a finger to fix it," said CFPB Director Rohit Chopra. "Rather than treating its customers fairly and following the law, TD Bank's management clearly cared more about growth and expanding its empire through mergers. Regulators will need to focus major attention on TD Bank to change its course."

TD Bank, N.A. is a national bank headquartered in Cherry Hill, New Jersey. It is one of many subsidiaries of Toronto-based Toronto-Dominion Bank (NYSE: TD). Toronto-Dominion Bank and its subsidiaries are collectively known as TD Bank Group. TD Bank Group reported $1.97 trillion in assets as of the third quarter of 2024. The U.S.-based TD Bank is the tenth-largest commercial bank in the country with more than 1,200 branches. As of June 30, 2024,

TD Bank had $370 billion in total assets. Among the products and services offered by TD Bank are credit cards and deposit accounts. TD Bank furnishes information to credit and other consumer reporting companies about its customers related to their credit cards and deposit accounts. In February 2022, TD Bank announced that it would acquire another large financial institution, First Horizon Bank. The deal was later abandoned in 2023.

The CFPB's investigation found that for several years TD Bank repeatedly gave inaccurate account information to consumer reporting companies. At times, the information contained systemic errors about personal bankruptcies and credit card delinquencies. Other times, the bank gave consumer reporting companies information it knew or suspected was fraudulent. The bank knew of many of these inaccuracies for more than a year before fixing them. Additionally, when customers or consumer reporting companies submitted disputes to TD Bank, it failed to conduct proper investigations and sometimes to conduct any investigation at all. TD Bank's actions affected hundreds of thousands of its customers. The bank's actions violated both the Fair Credit Reporting Act and the Consumer Financial Protection Act.

Specifically, TD Bank harmed consumers by:

- **Failing to fix its credit card reporting errors**: TD Bank reported inaccurate information about its customers' credit card accounts to consumer reporting companies. Even though it knew it was sending incorrect information for consumer reports, the bank failed to promptly correct its mistakes. In some instances, TD Bank shared inaccurate information about credit card delinquencies. In other instances, the bank shared information that made it look like accounts were in use even though customers had voluntarily closed them.
- **Sharing fraudulent information with consumer reporting companies**: By January 2022, TD Bank identified hundreds of thousands of deposit account openings that were either confirmed or suspected to be fraudulent. By April 2023, instead of making sure only accurate information about its customers was sent to consumer reporting companies, TD Bank kept sharing fraudulent information about those accounts as if it belonged to the bank's customers. Derogatory information, including information that some of the fraudulent accounts were overdrawn, was shared with consumer reporting companies.
- **Failing to investigate and resolve consumer disputes:** TD Bank did not have sufficient processes in place to investigate consumer reporting disputes and diverted resources from investigating disputes to other parts of its business. It then, among other things, failed to conduct reasonable and timely investigations of consumer disputes, including sometimes by not conducting any investigation at all. It also failed to properly notify consumers after deeming a dispute frivolous or irrelevant.

Enforcement Action

Under the Consumer Financial Protection Act, the CFPB has the authority to take action against institutions violating consumer financial protection laws, including the Fair Credit Reporting Act and its implementing regulation, Regulation V, and for engaging in unfair,

deceptive, or abusive acts or practices. The CFPB's order requires TD Bank, among other things, to:

- **Pay redress to affected consumers:** TD Bank must pay $7.76 million in redress to tens of thousands of consumers affected by its unlawful behavior.
- **Pay a $20 million penalty:** TD Bank will pay $20 million to the CFPB's victims relief fund (cfpb.gov/enforcement/payments-harmed-consumers/civil-penalty-fund/).

Read today's order (cfpb.gov/enforcement/actions/td-bank-na-furnishing-2024/).

This is the CFPB's second enforcement action against TD Bank. In 2020, the CFPB ordered (cfpb.gov/about-us/newsroom/cfpb-announces-settlement-td-bank-illegal-overdraft-practices/) TD Bank to provide an estimated $97 million in restitution to about 1.42 million consumers and to pay a $25 million penalty for illegal overdraft practices.

Learn more about credit reports and scores. (cfpb.gov/consumer-tools/credit-reports-and-scores/)

Read the CFPB's April 2024 report on violations of credit report accuracy requirements. (cfpb.gov/about-us/newsroom/cfpb-finds-violations-of-credit-report-accuracy-requirements-including-for-survivors-of-human-trafficking/)

Read consumer complaints about TD Bank and credit furnishing. (cfpb.gov/data-research/consumer-complaints/search/?date_received_max=2024-08-23&date_received_min=2011-12-01&page=1&searchField=all&searchText=credit%20furnishing%20td%20bank&size=25&sort=created_date_desc&tab=List)

Consumers can submit complaints about financial products and services by visiting the CFPB's website (cfpb.gov/complaint/) or by calling (855) 411-CFPB (2372).

Employees who believe their company has violated federal consumer financial protection laws are encouraged to send information about what they know to whistleblower@cfpb.gov. To learn more about reporting potential industry misconduct, visit the CFPB's website (cfpb.gov/enforcement/information-industry-whistleblowers/).

The Consumer Financial Protection Bureau is a 21st century agency that implements and enforces Federal consumer financial law and ensures that markets for consumer financial products are fair, transparent, and competitive. For more information, visit www.consumerfinance.gov (http://www.consumerfinance.gov/).

Topics

- FINANCIAL SERVICE PROVIDERS (CFPB.GOV/ABOUT-US/NEWSROOM/?TOPICS=FINANCIAL-SERVICE-PROVIDERS)

AGREEMENT BY AND BETWEEN
Wells Fargo Bank, N.A.
Sioux Falls, South Dakota
and
The Office of the Comptroller of the Currency

AA-ENF-2024-72

Wells Fargo Bank, N.A., Sioux Falls, South Dakota ("Bank") and the Office of the Comptroller of the Currency ("OCC") wish to assure the safety and soundness of the Bank and its compliance with laws and regulations.

The Comptroller of the Currency ("Comptroller") has identified deficiencies relating to the Bank's anti-money laundering ("AML") internal controls and financial crimes risk management practices and violations of law, rule, or regulation, including 12 C.F.R. § 21.21(d)(1) (internal control pillar), 12 C.F.R. § 21.11(d) (suspicious activity reporting), 31 C.F.R. § 1020.210(a)(2)(v)(A) (customer due diligence), 31 C.F.R. § 1020.220(a)(2)(i)(A)(3) (customer identification program), 31 C.F.R. § 1010.230(b)(2) (beneficial ownership), 31 C.F.R. § 1010.313 (currency transaction reporting), and 31 C.F.R. § 1010.410(f)(1) (travel rule).

The Bank has begun to take corrective action and has committed to taking all necessary and appropriate steps to remedy the deficiencies identified by the OCC and to enhance its internal controls and financial crimes risk management practices.

Therefore, the OCC, through the duly authorized representative of the Comptroller, and the Bank, through its duly elected and acting Board of Directors ("Board"), hereby agree that the Bank shall operate at all times in compliance with the following:

ARTICLE I

JURISDICTION

(1) The Bank is an "insured depository institution" as that term is defined in 12 U.S.C. § 1813(c)(2).

(2) The Bank is a national banking association within the meaning of 12 U.S.C. § 1813(q)(1)(A), and is chartered and examined by the OCC. *See* 12 U.S.C. § 1 *et seq.*

ARTICLE II

COMPLIANCE COMMITTEE

(1) The Board shall maintain a Compliance Committee of at least three (3) members, of which a majority shall be directors who are not employees or officers of the Bank or any of its subsidiaries or affiliates. In the event of a change of the membership, the Board shall submit in writing to the Examiner-in-Charge within ten (10) days the name of any new or resigning committee member. The Compliance Committee shall be responsible for approving the action plan required under Article III of this Agreement, along with monitoring and overseeing the Bank's compliance with the provisions of this Agreement. The Compliance Committee shall meet at least quarterly and maintain minutes of its meetings.

(2) Within forty-five (45) days after the end of the first full calendar quarter after the Bank receives a written determination of no supervisory objection to the action plan required under Article III of this Agreement, and thereafter within forty-five (45) days after the end of each calendar quarter, the Bank shall prepare, and the Compliance Committee shall submit to the Board, a written progress report setting forth in detail:

(a) the specific corrective actions undertaken to comply with each Article of this Agreement;

(b) the results and status of the corrective actions; and

(c) a description of the outstanding corrective actions needed to achieve compliance with each Article of this Agreement and the party or parties responsible for the completion of outstanding corrective actions.

(3) The Board shall forward a copy of the progress report, with any additional comments by the Board, to the Examiner-in-Charge within fifteen (15) days following the first Board meeting following the Board's receipt of such report.

ARTICLE III

BSA/AML AND OFAC SANCTIONS ACTION PLAN

(1) Within one-hundred twenty (120) days of the effective date of this Agreement, the Bank shall submit to the Examiner-in-Charge for review and prior written determination of no supervisory objection an acceptable written plan ("Action Plan") that details the remedial actions necessary to achieve and sustain compliance with the Bank Secrecy Act, as amended (31 U.S.C. § 5311 et seq.), and the rules and regulations promulgated thereunder (collectively, the "BSA"), and all relevant U.S. economic sanctions laws, Executive Orders, rules and regulations, including the rules and regulations of the Office of Foreign Assets Control (collectively, "OFAC Sanctions"), and that incorporates the substantive requirements of Articles IV through XII of this Agreement and all corrective actions addressing BSA/AML or OFAC Sanctions concerns and violations formally communicated by the OCC to the Bank in writing that remain open as of the effective date of this Agreement.

(2) The Action Plan shall include, at a minimum:

(a) a description of the required corrective actions;

(b) the specific Article and associated paragraph (and, if applicable, subparagraph) that each corrective action will address;

(c) reasonable and well-supported timelines for completing the corrective actions. These timelines shall reflect appropriate consideration of the possible impact on timing caused by any interdependencies between

corrective actions, and further, shall be inclusive of time needed for the Bank to validate completion and effectiveness of the corrective actions; and

(d) the person(s) responsible for completing the corrective actions.

(3) Upon receipt of a written determination of no supervisory objection to the Action Plan from the Examiner-in-Charge, the Board shall ensure the Bank has timely adopted the Action Plan and shall verify that the Bank thereafter adheres to the Action Plan, including the timelines set forth within the Action Plan.

(4) The Compliance Committee shall review the implementation of the Action Plan at least quarterly, and more frequently if necessary or if required by the OCC in writing, and direct Bank management to amend the Action Plan as needed.

(5) In the event the Examiner-in-Charge requires changes to the Action Plan, the Bank shall promptly incorporate the required changes into the Action Plan and submit the revised Action Plan to the Examiner-in-Charge for review and prior written determination of no supervisory objection.

(6) The Bank shall not take any action, including modifications to the Action Plan that has received a written determination of no supervisory objection from the Examiner-in-Charge, that will cause a significant deviation from, or material change to, the Action Plan.

(7) Where the Bank considers significant deviations from or material changes to the Action Plan appropriate, the Bank shall submit the proposed modifications to the Action Plan to the Examiner-in-Charge for prior written determination of no supervisory objection. Following receipt of a written determination of no supervisory objection, the Board shall ensure the Bank has timely adopted the revised Action Plan and shall verify that the Bank thereafter adheres to

the revised Action Plan, including the timelines set forth within the revised Action Plan. The Bank shall provide quarterly written notifications to the Examiner-in-Charge of any other modifications to the Action Plan.

(8) Within one hundred twenty (120) days of receipt of a prior written determination of no supervisory objection to the Action Plan, the Bank's Internal Audit department shall complete a review of the Bank's progress towards implementing the Action Plan. On a quarterly basis thereafter, Internal Audit should review and communicate that Bank management's Action Plan progress report is accurate, including a review of whether any changes have occurred that require no supervisory objection. The review shall be memorialized in writing and, within thirty (30) days of completion, Internal Audit shall provide its report to the Compliance Committee and the Examiner-in-Charge.

ARTICLE IV

FRONT-LINE FINANCIAL CRIMES RISK MANAGEMENT

(1) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Bank shall enhance BSA/AML and OFAC Sanctions compliance risk management by front-line units by, at a minimum:

(a) delineating clear roles and responsibilities and lines of authority for BSA/AML and OFAC Sanctions front-line compliance risk management functions;

(b) strengthening policies, procedures, and controls to ensure the effective implementation by front-line units of the Bank's enterprise-wide BSA/AML and OFAC Sanctions programs;

(c) strengthening front-line BSA/AML and OFAC Sanctions controls testing to ensure effective testing by personnel with the requisite knowledge, skills, and experience and a process to report the results;

(d) improving and implementing an effective process to ensure the Bank maintains sufficient front-line financial crimes operations staff with the appropriate knowledge, skills, and experience needed to support the Bank's BSA/AML and OFAC Sanctions programs; and

(e) providing sufficient and ongoing BSA/AML and OFAC Sanctions training to front-line employees based on the individual's job-specific duties and responsibilities.

ARTICLE V

INDEPENDENT RISK MANAGEMENT

(1) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Bank shall enhance the independent second-line Financial Crimes Risk Management ("FCRM") function and its oversight of front-line units by, at a minimum:

(a) delineating clear roles and responsibilities and lines of authority for BSA/AML and OFAC Sanctions compliance risk management within the FCRM function;

(b) strengthening policies, procedures, and controls to ensure effective implementation by FCRM of the Bank's enterprise-wide BSA/AML and OFAC Sanctions programs, including with respect to management

information reporting, the functioning of FCRM-related forums, and oversight of front-line units;

(c) developing and implementing effective policies, procedures, and controls to oversee the appropriate risk rating, monitoring, escalation, performance of root cause and impact analyses, and resolution of BSA/AML and OFAC Sanctions issues in a timely manner;

(d) strengthening the Bank's second-line BSA/AML and OFAC Sanctions testing program to ensure effective testing by personnel with the requisite knowledge, skills, and experience and a process to report the results;

(e) reviewing, improving, and implementing an effective process to ensure the Bank maintains sufficient FCRM staff with the appropriate knowledge, skills, and experience needed to support the Bank's BSA/AML and OFAC Sanctions programs; and

(f) providing sufficient and ongoing BSA/AML and OFAC Sanctions training to FCRM employees.

ARTICLE VI

BSA/AML AND OFAC SANCTIONS INDEPENDENT TESTING

(1) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Bank shall develop, and the Audit Committee of the Board ("Audit Committee") shall approve, enhancements to the Bank's written audit program component concerning BSA/AML and OFAC Sanctions to ensure effective independent testing of the Bank's compliance with the BSA and OFAC Sanctions, relative to its risk profile, and the overall adequacy of the Bank's BSA/AML and OFAC Sanctions compliance

programs ("BSA/AML/OFAC Audit Program"). Refer to the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual*: "BSA/AML Independent Testing" (2020).

(2) The BSA/AML/OFAC Audit Program shall address and determine, at a minimum, whether:

(a) the Bank's BSA/AML and OFAC Sanctions Risk Assessment adequately captures its risk profile;

(b) the Bank's policies, procedures, and controls are reasonably designed to achieve compliance with the BSA and OFAC Sanctions and appropriate for the Bank's risk profile;

(c) the Bank adheres to its policies, procedures, and controls for BSA/AML and OFAC Sanctions compliance;

(d) the Bank's information technology sources, systems, and controls used to support the BSA/AML and OFAC Sanctions compliance program are adequate;

(e) management is taking appropriate and timely action to address any deficiencies noted in independent testing and regulatory examinations; and

(f) BSA/AML and OFAC Sanctions training is provided for appropriate personnel, tailored to specific functions and positions, and includes supporting documentation.

(3) The BSA/AML/OFAC Audit Program shall also, at a minimum:

(a) include risk assessment processes that document the products, services, customers, and geographies that impact the quantity and quality of the Bank's BSA/AML and OFAC Sanctions risks and the Bank's controls;

(b) include processes for the development of and adherence to an appropriate BSA/AML and OFAC Sanctions audit plan that takes into account the Bank's BSA/AML and OFAC Sanctions risks;

(c) require appropriate documentation supporting:

(i) the inclusion and exclusion of auditable areas in the Bank's audit universe and of internal controls for testing; and

(ii) changes to planned design of control and control effectiveness testing;

(d) include controls for periodically reviewing, updating, and documenting changes to the audit plan and communicating significant changes to the Audit Committee;

(e) include appropriate audit test scripts designed to ensure consistent execution of BSA/AML and OFAC Sanctions audits across the enterprise; and

(f) include controls to ensure sufficient staff with the appropriate knowledge, skills, and experience needed to support the BSA/AML/OFAC Audit Program.

(4) Management shall require prompt reporting of deficiencies in BSA/AML and OFAC Sanctions controls identified by Internal Audit through the BSA/AML/OFAC Audit Program to the Audit Committee, and to senior management. The reports shall indicate the severity of the deficiencies, the risks, and the required corrective actions. The Compliance Committee shall ensure that management takes prompt action to remedy deficiencies cited in

audit reports. The Audit Committee shall ensure that the BSA/AML/OFAC Audit Program reviews and validates corrective action promptly.

ARTICLE VII

CUSTOMER IDENTIFICATION PROGRAM, CUSTOMER DUE DILIGENCE, AND CUSTOMER RISK IDENTIFICATION

(1) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Board shall ensure that Bank management develops and adopts an enhanced written customer due diligence program to ensure appropriate and effective collection and analysis of customer due diligence ("CDD") information by all business lines ("CDD Program"). The CDD Program shall also ensure the Bank operates in accordance with applicable laws and regulations, including applicable laws and regulations addressing Customer Identification Program ("CIP") requirements, CDD, and beneficial ownership, and be consistent with the Bank's money laundering, terrorist financing and other illicit financial activity risk assessments. Refer to the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual*: "Customer Due Diligence" (2018), "Beneficial Ownership Requirements for Legal Entity Customers" (2018), and "Customer Identification Program" (2021).

(2) The Bank's CDD Program shall include, at a minimum:

(a) clear definitions for customer risk levels;

(b) a methodology for assigning defined risk levels to the customer base that considers the customer's entire relationship and appropriate factors such as type of customer; purpose of the account; geographic location; and the expected account activity by type of service used, including the volume, velocity, and frequency by dollar amount and number;

(c) risk-based requirements to collect, maintain, and timely update all information necessary to establish an accurate customer risk profile;

(d) procedures to require the collection and verification of appropriate CIP information for the opening of new accounts in compliance with 31 C.F.R. § 1020.220;

(e) procedures to require the collection and verification of appropriate beneficial ownership information for the opening of new accounts for legal entity customers in compliance with 31 C.F.R. § 1010.230;

(f) procedures that contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable;

(g) procedures to ensure staff responsible for CDD and CIP information have sufficient authority, training, and skills to perform their assigned responsibilities;

(h) procedures for identifying and timely remediating instances where required CDD and CIP information is missing or incomplete;

(i) a process documented in writing to identify higher-risk current customers and accounts exhibiting high-risk characteristics for money laundering, terrorist financing, or other illicit activity;

(j) procedures for ongoing monitoring and periodic reviews of higher-risk customers, which shall include, at a minimum:

(i) risk-based criteria establishing how often to conduct periodic

reviews of higher-risk customers;

(ii) documented evidence of transactional analysis, including comparing expected, historical, and current activity, the source and use of funds, trends, and activity patterns; and

(iii) documented analysis of all significant information in the file, including the identification of significant disparities, investigation of high-risk indicators and potentially suspicious activity, and well-supported conclusions; and

(k) procedures to ensure that customer risk ratings are appropriately incorporated into the Bank's money laundering, terrorist financing and other illicit financial activity risk assessment.

ARTICLE VIII

SUSPICIOUS ACTIVITY IDENTIFICATION

(1) The Bank shall incorporate the remediation of any gaps and deficiencies identified by the Bank's coverage assessment of its current suspicious activity identification and transaction monitoring controls into the Action Plan required by Article III of this Agreement.

(2) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Board shall ensure that Bank management develops and adopts an enhanced suspicious activity monitoring and reporting program ("Suspicious Activity Review Program") to ensure the timely, appropriate, and effective identification of unusual activity. Refer to the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual*: "Suspicious Activity Reporting – Overview" (2015), "*Supervisory Guidance on Model Risk Management*," April 11, 2011 (OCC Bulletin 2011-12); "*Bank Secrecy*

Act/Anti-Money Laundering: Interagency Statement on Model Risk Management for Bank Systems Supporting BSA/AML Compliance," April 12, 2021 (OCC Bulletin 2021-19); and the "*Model Risk Management*" booklet of the *Comptroller's Handbook*.

(3) The Bank's Suspicious Activity Review Program shall include, at a minimum:

(a) policies, procedures, and controls for identifying reportable activity across all lines of business, including suspicious activity relating to the opening of new accounts, the monitoring of current accounts, and transactions processed by, to, or through the Bank;

(b) procedures and controls for periodically reviewing the coverage of transaction monitoring and reports; and

(c) procedures and controls to ensure that:

(i) transaction monitoring systems apply appropriate rules, thresholds, and filters for monitoring transactions, accounts, customers, products, services, and geographic areas commensurate with the Bank's BSA/AML risk profile;

(ii) the Bank's methodology for establishing and adjusting rules, thresholds and filters is appropriately documented; and

(iii) automated transaction monitoring systems are subject to periodic independent validation, the findings of which are documented, reported, and timely addressed.

ARTICLE IX

BSA/AML AND OFAC RISK ASSESSMENT

(1) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Bank shall enhance its written, enterprise-wide BSA/AML and OFAC Sanctions Risk Assessment methodology. The BSA/AML and OFAC Sanctions Risk Assessment methodology shall reflect a comprehensive analysis of the Bank's money laundering and terrorist financing, OFAC Sanctions, and other illicit financial activity risks and provide strategies to control those risks and limit any identified vulnerabilities. Refer to the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual*: "BSA/AML Risk Assessment" (2020) and "Office of Foreign Assets Control" (2015).

(2) The BSA/AML and OFAC Sanctions Risk Assessment methodology shall include, at a minimum:

(a) an analysis of the Bank's products, channels, customers (including consideration of customers that typically pose higher BSA/AML and OFAC Sanctions risk), transactions (including consideration of volumes and types of transactions and services by country or geographic location), and geographic locations in which the Bank is engaged;

(b) an assessment of BSA/AML and OFAC Sanctions risk both separately within the Bank's business lines and on a consolidated basis across all of the Bank's products, channels, transactions, customers, and geographies;

(c) a provision requiring maintenance of appropriate documentation of data and information used to support the Bank's BSA/AML and OFAC

Sanctions Risk Assessment's conclusions (with supporting documentation readily accessible for third-party review);

(d) an assessment of the adequacy of the Bank's internal controls designed to address the risks identified through the BSA/AML and OFAC Sanctions Risk Assessment that incorporates findings from regulatory examinations, front-line and second-line testing, and audit reviews; and

(e) identification of the Bank's residual risk.

(3) In accordance with the timelines set forth in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, and at least annually thereafter, Bank management shall perform a written BSA/AML and OFAC Sanctions Risk Assessment in accordance with the enhanced methodology required by this Article.

(4) Bank management shall review, and, as necessary, update the BSA/AML Risk Assessment methodology annually, and more frequently if necessary or if required by the OCC in writing, or whenever there is a significant change in BSA/AML and OFAC Sanctions risk within the Bank or the lines of businesses within the Bank.

(5) The Board shall promptly review and provide credible challenge to the BSA/AML and OFAC Sanctions Risk Assessment and any subsequent updates and document its review in the Board minutes. The Bank shall promptly provide a copy of the BSA/AML and OFAC Sanctions Risk Assessment and the minutes documenting the Board's review of the BSA/AML and OFAC Sanctions Risk Assessment to the Examiner-in-Charge.

(6) The Bank shall enhance its targeted BSA/AML and OFAC Sanctions risk assessments to ensure that such risk assessments provide meaningful risk analysis with respect

to certain products, services, customers, geographies, and affiliate relationships and shared services.

ARTICLE X

BSA/AML AND OFAC SANCTIONS SYSTEMS DESIGN AND ADEQUACY AND DATA INTEGRITY

(1) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Bank shall establish a methodology for, and conduct, an assessment to evaluate whether the Bank's current BSA/AML and OFAC Sanctions transaction monitoring systems and reports, SAR filing system, OFAC Sanctions screening systems, customer risk rating system, Currency Transaction Report filing system, and BSA/AML and OFAC Sanctions risk assessment system (collectively, the "Key BSA/AML and OFAC Compliance Systems") are commensurate with the Bank's BSA/AML and OFAC Sanctions risk profile, operations, and lines of business, are adequately designed and working as intended, and whether additional investments are needed to upgrade the Bank's Key BSA/AML and OFAC Compliance Systems ("BSA/AML and OFAC Systems Resource Assessment"). The Compliance Committee shall ensure that management corrects any deficiencies identified by the BSA/AML and OFAC Systems Resource Assessment and implements any plans or recommendations resulting from the BSA/AML and OFAC Systems Resource Assessment. The Bank shall incorporate its plan to implement effective remediation of any identified gaps and deficiencies into the Action Plan required by Article III of this Agreement.

(2) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Board shall ensure that the Bank develops and adopts an effective written program to ensure the integrity of data relevant to the Key BSA/AML and OFAC Compliance Systems ("Data Integrity Program").

(3) The Data Integrity Program shall address or include, effective policies, procedures, or associated controls, as applicable, to ensure, at a minimum, that the Bank:

(a) develops and periodically updates comprehensive inventories of Bank systems which contain data relevant to the Key BSA/AML and OFAC Sanctions Compliance Systems;

(b) establishes clear roles and responsibilities for the management and oversight of BSA/AML and OFAC Sanctions data;

(c) identifies high priority BSA/AML and OFAC Sanctions use cases related to the Key BSA/AML and OFAC Sanctions Compliance Systems;

(d) documents data dictionaries and data sourcing process maps and desktop procedure(s) related to the Key BSA/AML and OFAC Sanctions Compliance Systems;

(e) creates data lineage documentation for the Key BSA/AML and OFAC Sanctions Compliance Systems, implements controls designed to ensure the FCRM team is informed of systems-related projects impacting financial crimes use cases, and remediates data defects within the lines of business and relevant enterprise functions;

(f) creates comprehensive end-to-end data lineage documentation from Key BSA/AML and OFAC Sanctions Compliance Systems to upstream sources, performs quality assurance of lineage documentation, and defines an enterprise process for notification of systems-related projects;

(g) enhances the FCRM team's governance and oversight of data defects, defect remediation, and systems-related projects impacting financial crimes use cases;

(h) maintains procedures and controls to ensure timely and accurate information is provided to the Key BSA/AML and OFAC Sanctions Compliance Systems, including periodic data reconciliation of data feeds to Key BSA/AML and OFAC Sanctions Compliance Systems;

(i) conducts risk-based data and control testing for completeness, accuracy, and control effectiveness for Key BSA/AML and OFAC Sanctions Compliance Systems; and

(j) provides training to targeted audiences involved in the data supply chain.

ARTICLE XI

OFAC SANCTIONS COMPLIANCE PROGRAM

(1) Within the time periods specified in the Action Plan for which the Examiner-in-Charge has provided no supervisory objection, the Board shall ensure that the Bank develops and adopts an enhanced written compliance program designed to ensure that the Bank complies with OFAC Sanctions ("OFAC Compliance Program"). Refer to the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual*: "Office of Foreign Assets Control" (2015); "*Supervisory Guidance on Model Risk Management*," April 11, 2011 (OCC Bulletin 2011-12); "*Bank Secrecy Act/Anti-Money Laundering: Interagency Statement on Model Risk Management for Bank Systems Supporting BSA/AML Compliance*," April 12, 2021 (OCC Bulletin 2021-19); and the "*Model Risk Management*" booklet of the *Comptroller's Handbook*.

(2) The OFAC Compliance Program shall include, at a minimum:

(a) policies, procedures, and controls for screening and assessing new potential customers, existing customers, and transactions against applicable OFAC Sanctions lists and applicable regulatory requirements;

(b) procedures and controls to ensure that data relied upon to conduct OFAC Sanctions screening is accurate; and

(c) procedures and controls to ensure that the Bank's automatic OFAC Sanctions screening system is timely and effectively tuned and, as appropriate, validated.

ARTICLE XII

RESTRICTION ON NEW PRODUCTS, SERVICES, AND MARKETS

(1) Within sixty (60) days of the effective date of this Agreement, the Bank shall submit to the Examiner-in-Charge, for review and prior written determination of no supervisory objection, a new business initiative program to assess and mitigate the BSA/AML and OFAC Sanctions risks of new products, services, or geographic markets. The program must include:

(a) clear definitions of the BSA/AML and OFAC risk levels applicable to new products, services, and geographic markets;

(b) an effective process for assessing the BSA/AML or OFAC Sanctions risks posed by new products, services, or geographic markets; and

(c) an effective process for determining that the Bank has sufficient internal controls, including, but not limited to, sufficient CDD and suspicious activity monitoring controls, and sufficient staff across its lines of defense to mitigate such risks.

(2) Until the Bank receives a prior written determination of no supervisory objection pursuant to Paragraph (1) of this Article:

(a) the Bank shall not expand into new products, services, or geographic markets with a medium or high BSA/AML or OFAC Sanctions inherent risk without receiving a prior written determination of no supervisory objection from the Examiner-in-Charge. The Bank shall make any request for a prior written determination of no supervisory objection in writing to the Examiner-in-Charge and include a copy of the assessment discussed in Paragraph (1); and

(b) the Bank shall not expand into new products, services, or geographic markets with a low BSA/AML or OFAC Sanctions inherent risk without providing at least thirty (30) days prior written notification and a copy of the assessment discussed in Paragraph (1) to the Examiner-in-Charge.

(3) After the Bank receives a prior written determination of no supervisory objection pursuant to Paragraph (1) of this Article, the Bank shall not expand into new products, services, or geographic markets with a medium or high BSA/AML and OFAC Sanctions inherent risk without providing at least thirty (30) days prior written notification and a copy of the assessment discussed in Paragraph (1) to the Examiner-in-Charge.

(4) After receipt of any individual notification in writing, the Examiner-in-Charge may extend the notification period described in Paragraph (2)(b) or (3) for an additional thirty (30) days.

ARTICLE XIII

GENERAL BOARD RESPONSIBILITIES

(1) The Board shall ensure that the Bank has timely adopted and implemented all corrective actions required by this Agreement, and shall verify that the Bank adheres to the corrective actions and they are effective in addressing the Bank's deficiencies that resulted in this Agreement.

(2) In each instance in which this Agreement imposes responsibilities upon the Board or one of its committees, including the Compliance Committee and Audit Committee, it is intended to mean that the Board or the specified committee, as applicable, shall:

(a) authorize, direct, and adopt corrective actions as may be necessary for the Bank to perform the obligations and undertakings imposed on the Bank by this Agreement;

(b) ensure that the Bank has sufficient controls, management, personnel, control systems, and corporate and risk governance to implement and adhere to all provisions of this Agreement;

(c) require that Bank management and personnel have sufficient training and authority to execute their duties and responsibilities pertaining to or resulting from this Agreement;

(d) hold Bank management and personnel accountable for executing their duties and responsibilities pertaining to or resulting from this Agreement;

(e) require appropriate, adequate, and timely reporting to the Board by Bank management of corrective actions directed by the Board to be taken under the terms of this Agreement; and

(f) address any noncompliance with corrective actions in a timely and appropriate manner.

(3) With respect to each of the programs required by Articles VI (1), VII (1), VIII (2), X (2), XI (1), and XII (1) (each, a "Program"), the Board shall review the effectiveness of the Program at least annually, and more frequently if necessary or if required by the OCC in writing, and cause management to amend the Program as needed or directed by the OCC. The Bank shall forward a copy of each such adopted Program to the Examiner-in-Charge within fifteen (15) days of adoption. Any material amendment to the Program shall be forwarded to the Examiner-in-Charge within fifteen (15) days of adoption.

ARTICLE XIV

OTHER PROVISIONS

(1) As a result of this Agreement, the Bank is not:

(a) precluded from being treated as an "eligible bank" for the purposes of 12 C.F.R. Part 5, unless the Bank fails to meet any of the requirements contained in subparagraphs (1) – (4) of 12 C.F.R. § 5.3, Definitions, *Eligible bank or eligible savings association,* or is otherwise informed in writing by the OCC;

(b) subject to the restrictions in 12 C.F.R. § 5.51 requiring prior notice to the OCC of changes in directors and senior executive officers or the limitations on golden parachute payments set forth in 12 C.F.R. Part 359, unless the Bank is otherwise subject to such requirements pursuant to 12 C.F.R. § 5.51(c)(7)(i) and (iii); and

(c) precluded from being treated as an "eligible bank" for the purposes of 12 C.F.R. Part 24, unless the Bank fails to meet any of the requirements contained in 12 C.F.R. § 24.2(e)(1)-(3) or is otherwise informed in writing by the OCC.

(2) This Agreement supersedes all prior OCC communications issued pursuant to 12 C.F.R. §§ 5.3, 5.51(c)(7)(ii), and 24.2(e)(4).

ARTICLE XV

CLOSING

(1) This Agreement is intended to be, and shall be construed to be, a "written agreement" within the meaning of 12 U.S.C. § 1818, and expressly does not form, and may not be construed to form, a contract binding on the United States, the OCC, or any officer, employee, or agent of the OCC. Notwithstanding the absence of mutuality of obligation, or of consideration, or of a contract, the OCC may enforce any of the commitments or obligations herein undertaken by the Bank under its supervisory powers, including 12 U.S.C. § 1818(b)(1), and not as a matter of contract law. The Bank expressly acknowledges that neither the Bank nor the OCC has any intention to enter into a contract. The Bank also expressly acknowledges that no officer, employee, or agent of the OCC has statutory or other authority to bind the United States, the U.S. Treasury Department, the OCC, or any other federal bank regulatory agency or entity, or any officer, employee, or agent of any of those entities to a contract affecting the OCC's exercise of its supervisory responsibilities.

(2) This Agreement is effective upon its issuance by the OCC, through the Comptroller's duly authorized representative. Except as otherwise expressly provided herein, all references to "days" in this Agreement shall mean calendar days and the computation of any

period of time imposed by this Agreement shall not include the date of the act or event that commences the period of time.

(3) The provisions of this Agreement shall remain effective and enforceable except to the extent that, and until such time as, such provisions are amended, suspended, waived, or terminated in writing by the OCC, through the Comptroller's duly authorized representative. If the Bank seeks an extension, amendment, suspension, waiver, or termination of any provision of this Agreement, the Board or a Board-designee shall submit a written request to the Deputy Comptroller asking for the desired relief. Any request submitted pursuant to this paragraph shall include a statement setting forth in detail the special circumstances that warrant the desired relief or prevent the Bank from complying with the relevant provision(s) of this Agreement, and shall be accompanied by relevant supporting documentation. The OCC's decision concerning a request submitted pursuant to this paragraph, which will be communicated to the Board in writing, is final and not subject to further review.

(4) The Bank will not be deemed to be in compliance with this Agreement until it has adopted, implemented, and adhered to all of the corrective actions set forth in each Article of this Agreement; the corrective actions are effective in addressing the Bank's deficiencies; and the OCC has verified and validated the corrective actions. An assessment of the effectiveness of the corrective actions requires sufficient passage of time to demonstrate the sustained effectiveness of the corrective actions.

(5) Each citation, issuance, or guidance referenced in this Agreement includes any subsequent citation, issuance, or guidance that replaces, supersedes, amends, or revises the referenced cited citation, issuance, or guidance.

(6) No separate promise or inducement of any kind has been made by the OCC, or by its officers, employees, or agents, to cause or induce the Bank to enter into this Agreement.

(7) All reports, plans, or programs submitted to the OCC pursuant to this Agreement shall be forwarded via email, to the Examiner-in-Charge, or other such designees as determined by the Examiner-in-Charge.

(8) The terms of this Agreement, including this paragraph, are not subject to amendment or modification by any extraneous expression, prior agreements, or prior arrangements between the parties, whether oral or written.

IN TESTIMONY WHEREOF, the undersigned, authorized by the Comptroller as his duly authorized representative, has hereunto set his signature on behalf of the Comptroller.

//s// Digitally Signed, Dated: 2024.09.12

Mark D. Richardson
Deputy Comptroller
Large Bank Supervision