# FOLLOW THE MONEY

## *Bridging Consumer Protection and Illicit Finance to Stop Scams*

**Adam Rust, Director of Financial Services**

Consumer Federation of America

JANUARY 2026

# INTRODUCTION

Today, fraudsters impersonate trusted relationships and leverage information gathered from multiple sources across the internet. Criminals often pose as representatives of government agencies seeking to collect outstanding debts, as employers requesting payments from employees, or as family and friends in need of emergency funds, among other examples. They ensnare people in romance scams, or lure them with surprise lottery winnings, and sometimes even extort them. These are only examples. New schemes emerge every day. They share one thing in common: they end by duping a victim into sending money.

The number of fraud reports has increased dramatically over the last decade. The Federal Trade Commission (FTC) received 325,519 fraud reports in 2001, more than 1.8 million in 2011, and approximately 6.5 million in 2024.

The converging forces of several technology-driven changes have made fraud and scams more widespread. Twenty years ago, people did not carry mobile devices. Payment systems did not exist to permit individuals to initiate electronic payment orders at any time, from any place, to pay virtually anyone. Commerce occurred online, but digital transactions were almost always made exclusively with network-branded cards rather than through person-to-person (P2P) app transfers. These and other factors were already narrowing the distance between criminals and consumer victims; a worldwide pandemic accelerated them.

The rise in scams reflects another change. There has been a blurring of boundaries between activities traditionally associated with illicit crime – sending funds between criminals– with fraud perpetrated on regular people. Twenty years ago, these activities were distinct, but today they have blended together.

Yet despite this sea change, the agencies charged with policing illicit finance are separate from those focused on protecting consumers. It is urgent and sensible to close this gap. To accomplish this goal, policymakers must change how they work together. As it stands now, they work in silos. While the Consumer


***This graphic shows the overlapping regulatory objectives applicable to preventing criminal organizations from scamming consumers.***

*Source: 2024 National Money Laundering Risk Assessment, Department of the Treasury*

Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) will have visibility into complaints filed by account holders, consumers filing complaints will not know which bank received the funds. They should be able to request this information from payment system operators or the banks themselves. When bank regulators responsible for Bank Secrecy Act (BSA) compliance identify substantive shortcomings at a bank, they should notify the CFPB of risks of scams. As the recipient of Suspicious Activity Reports (SARs), the Financial Crimes Enforcement Network (FinCEN) should maximize the value of this information. As regulators for state-chartered banks and licensed money transmitters, states are also poised to play a part, including for non-bank state-licensed money transmitters.

Scams do not happen by accident. To accomplish their goals, criminals must have a way to receive those funds. While cryptocurrency is well-suited to fulfill their needs, criminals still open bank accounts or take over existing ones. Once under their control, they use those accounts to receive funds. Often, they seek banks with poor anti-fraud defenses, including those that have only recently begun offering online banking.[1] Having identified a vulnerable bank, they proceed to flood it with online account applications. The compromised bank should have rejected the applications for new accounts, prevented criminals from taking over existing accounts, and monitored accounts for suspicious activity. When it didn't, scams could occur.

**When acting as the receiving depository financial institution (RDFI), banks are positioned to prevent scams. They can spot suspicious patterns and should have a clear understanding of who controls the account.**

These approaches also emphasize the critical role financial institutions play when receiving fund transfers. When acting as the receiving depository financial institution (RDFI), banks are positioned to prevent scams. They can spot suspicious patterns and should have a clear understanding of who controls the account. Given that the techniques to spot patterns are readily available, either by direct bank investment or through vendors, using them should be table stakes for facilitating payments.

These policy changes can address a well-documented point of vulnerability in our financial system – partnerships between banks and fintechs – that have been the subject of many enforcement actions. In recent years, regulators have penalized many banks participating in partnership programs for failing to identify criminal actors. Under the Bank Service Company Act, prudential regulators can extend supervision to independent banking-as-a-service (BaaS) providers that coordinate bank-fintech partnerships. Proactively, prudential regulators should update guidance, including the third-party guidance covering bank partnerships, to clarify how BSA compliance customer due diligence (CDD) programs include consumer protections. When financial institutions fail to prevent criminals from using their accounts to commit payment fraud, it constitutes an unfair and deceptive practice. These steps create bridges between BSA and consumer protection.

P2P payment apps – which the FTC categorizes to include non-bank payment apps as well as faster payment apps in a single category - were the second-most common payment method used in transfers cited in complaints received by the agency in 2024.[2] In the second quarter of 2025, more complaints involved P2P app transfers than any other payment channel.[3] Resolving the problem is urgent because the volume and sophistication of scams aimed at tricking victims into sending money are increasing.

This paper examines how regulators can link the prevention of money laundering and scams. It raises questions about the logic of separating consumer protection concerns

from the fight against illicit finance. Is it time, instead, to consider how agencies with these separate remits could work together? Sharing information between regulators and financial institutions will increase effectiveness. Penalizing the financial institutions that fail to prevent criminals from opening accounts will spur investment in compliance. When regulators penalize institutions for permitting illicit finance, they should include relief for consumers in their enforcement actions.

**When regulators penalize institutions for permitting illicit finance, they should include relief for consumers in their enforcement actions.**

***CDD Requirements for Compliance With The Bank Secrecy Act (BSA) and anti-money laundering (AML) are designed to monitor the use of the banking system for criminal activity.***

The BSA calls on financial law enforcement agencies to monitor illicit financial activities by collecting information from financial institutions and sharing it with law enforcement agencies. They seek to identify when drug cartels, terrorists, and human traffickers seek access to American banks. The emphasis is on ensuring that financial institutions conduct the necessary customer due diligence (CDD) to understand who their customers are and how they intend to use their accounts. Historically, CDD efforts have primarily focused on anti-money laundering objectives. They do not consider how scams lead to direct consumer harm. There are three components to CDD:[4]

- Verifying the identity of the person seeking an account or the beneficial owners of the business.
- Understanding the nature and purpose of the customer relationship.
- Monitoring account activity to ensure that use is consistent with the first two steps.

Regulators expect financial institutions to assess the risk posed by each applicant and to seek additional information when proposed account uses raise concerns. For example, many international charities need accounts to send money to high-risk countries, but an escalated review can distinguish their use from criminal activity.

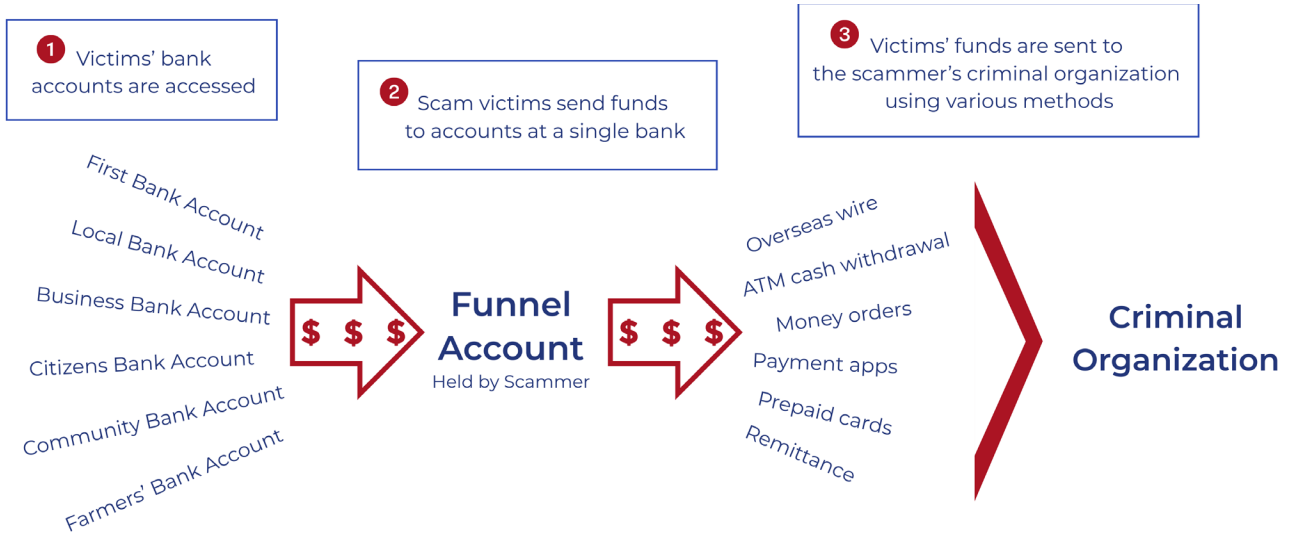
Banks and other financial institutions are expected to collect personally identifying information about their customers to protect the financial system from money laundering and to protect consumers from identity theft and fraud.[5] They have a duty to monitor their accounts for suspicious transactions, review customers, and flag large transactions. When a bank observes suspicious activity, the BSA requires it to file a Suspicious Activity Report (SAR). Transactions exceeding certain dollar thresholds require the bank to file a Currency Transaction Report (CTR). These reports are sent to the Financial Crimes Enforcement Network (FinCEN), a unit within the Department of the Treasury.[6]

Notably, there is a critical shortcoming in a regulatory approach that places such emphasis on reporting and record-keeping. Regulators focus on monitoring but rely on financial institutions to make decisions about their respective risk tolerances. Some institutions will reject risky applicants and business lines, but others will lean into risk.

However, banks have leeway in how they manage fraud prevention. As a principle, banks set their risk tolerances. They have the authority to choose their customers and the lines of business they serve. As a general principle, regulators do not compel banks to open or close accounts.[7] Instead, they review their policies through supervision and hold banks accountable for poor outcomes through enforcement actions. While it has merits, this approach to banking supervision comes with an inevitable downside. It makes it unavoidable that some financial institutions will be vulnerable targets for opportunistic criminals.

It presents an inherent tension between excessive risk aversion – also known as "debanking" – and too much risk-taking – also known as fraud facilitation.

*The Funnel Account: How A Single Bank with Poor Scam Prevention Puts Everyone at Risk of Scams*




## Problem: *The Funnel Account*

A key problem is the "funnel account." Criminals use funnel accounts to receive money. Funnel accounts affect transfers across all faster payments, checks, wires, and Automated Clearing House (ACH) transfers. An FDIC-insured account can serve as a funnel account, but a non-bank P2P wallet can also fulfill this purpose. A single funnel account can be used to receive numerous fraudulent transfers, serving as the hub to accept scams funds from multiple sending banks – referred to as originating depository financial institutions (ODFIs) in transactions. Often, funds are deposited into funnel accounts and then withdrawn as soon as they settle. This problem is only getting worse. The number of SARs identifying a funnel account has increased fourfold since 2020.[8] In the first six months of 2025, nearly 8 percent of bank account applications were made using synthetic identities.[9] With the rise of online banking, the share of applications made online has increased. New account fraud is enabled by stolen identities and made easier by artificial intelligence.[10]

The primary consumer protection law governing payment fraud – the Electronic Fund Transfer Act (EFTA) – will not help scam victims if they authorized a transfer. Unfortunately, EFTA and Regulation E (its implementing regulation) exempt Receiving Depository Financial Institutions (RDFIs) from liability for their role in facilitating scams. Still, poor fraud prevention by even a small number of RDFIs can lead to significant fraud. When criminals exploit a handful of vulnerable accounts to receive and then launder funds, they can create a small network of accounts to funnel funds.

## Problem: *The emergence of innovative payment systems, digital banking, and mobile technology adds risk.*

Technologies are converging, exacerbating the problem of fraud. Outside banking, the near-universal adoption of mobile devices, the risks associated with social media platforms, and the dark web help criminals identify and contact potential victims. In the financial services sector, the rise of mobile banking, online account opening, payment apps, and real-time gross settlement systems all expose the financial system to increased risk. Cryptocurrencies are only adding danger.[11] This is our landscape that permits fraud to flourish, and because its contributing factors continue to enjoy strong adoption, it is likely to become more fraught with peril.

The Patriot Act, passed in 2003, marked the last significant piece of legislation addressing illicit finance. Those rules were made for a different era, before the rise of online banking and the emergence of scams.

## **Problem:** *Because faster payment services are irrevocable and nearly immediate, addressing fraud occurring in them requires unique solutions.*

Sending banks depend on receiving banks to identify high-risk accounts. While standard ACH gives the ODFI several days to request a reversal, there is no such cushion with faster payments. As a result, fraud prevention in faster payments must rely on algorithmic analysis of payment patterns and rapid information sharing between networks and financial institutions. These tools require engagement from both banks and any intermediaries in a transfer.

As key gatekeepers in the exchange of fraud information, faster payment networks such as Zelle must play a role in identifying risky RDFIs. If necessary, they should force worst-practice banks off their systems.

From a business perspective, risky fund-receiving practices reduce the value of investments in faster payment services. Even in 2025, years after the introduction of The Clearing House Real-Time Payment Network and the Federal Reserve's FedNow system, many banks remain hesitant to send funds via faster payments. True, more banks are participating, but too many only receive faster payments. The reticence among banks should tell policymakers something. When so many banks refuse to allow customers to send funds, it suggests they believe many financial institutions lack adequate controls to prevent scams.[12] A perceived lack of safety is undermining the adoption of faster payments.

## **Problem:** *Even when enforcement actions identify failures, they ignore harms to consumers victimized by scams.*

Traditionally, BSA compliance by banks has been viewed primarily as a matter of taking steps to prevent illicit finance. While those priorities are well-founded, they do not address all the consequences of lax compliance. They fail to address another impact of lax BSA compliance: the harm it causes to consumers who are victimized. Weak defenses against illicit finance are unsafe and unsound financial practices that cause significant harm to consumers.

Banks have sought clarity on how regulators assess the risks associated with different types of suspicious activity. Incidents involving structuring, where account holders make transfers just below dollar-amount thresholds that trigger suspicion, are statistically the most common subjects of SARs. Of course, potential events involving the financing of terrorism should be of greater concern. In its 2021 Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, FinCEN addressed those concerns by stating its priorities. Notably, it listed fraud prevention among its eight national priorities. In using the term fraud, FinCEN made clear that the scope included activities common in scams:

> *"Increasingly, fraud schemes are internet-enabled, such as romance scams, synthetic identity fraud, and other forms of identity theft. Proceeds from fraudulent activities may be laundered through a variety of methods, including transfers through accounts of offshore legal entities, accounts controlled by cyber actors, and money mules."*[13]

FinCEN attributed these frauds to international criminal organizations. The activities (imposter scams, confidence fraud, employment schemes, etc.) and the destination of funds (to RDFIs) are consistent with the areas of concern in this paper.

In a 2020 statement on compliance for BSA and AML, FinCEN advised financial institutions to be "vigilant" to guard against scams. It even listed specific types of scams: imposter, investment, product, and insider trading.[14] This statement is only one example. In the prior year, FinCEN issued an advisory urging financial institutions to be on the lookout for fraud

involving criminals posing as charities, disaster assistance providers, and illicit crowdfunding platforms.[15]

FinCEN has stated that SARs can be helpful in understanding how fraud affects consumers. For example, in 2011, it issued an advisory to financial institutions, noting that their information could help combat elder financial fraud. It specifically noted that financial institutions can communicate with federal and state regulators to support fraud prevention efforts.[16]

## **Problem:** *Scams are often run by overseas criminal organizations. Scams are a problem of national financial security.*

Many scams are being carried out by transnational criminal organizations that BSA enforcement is designed to thwart. These organizations conduct scams alongside their other work in human trafficking, drug sales, and weapons smuggling.[17] The profits from scams fund their crimes.[18]

Transnational organizations rely on scams to fund their work. In some cases, scams fund a large share of the GDP of several Southeast Asian countries.[19] There is very little space between scams and international financial crime.[20] The idea that scam prevention should focus on consumer education is naïve, and establishing linkages between the agencies that protect consumers and those that pursue criminals is urgent. It is a problem that requires coordinated work across financial law enforcement and consumer protection agencies.

## **Problem:** *Scams targeting the elderly underscore the need for solutions that protect consumers from such scams and combat illicit financial crime.*

Seniors are a primary target of scammers. All things being equal, they are more likely to have savings, and some will suffer from cognitive impairments, making them more vulnerable to exploitation. In response, FinCEN has prioritized addressing elderly financial exploitation (EFE).

The findings detailed in its recurring Financial Trend Analysis reports show why it is imperative to eliminate boundaries between consumer protection agencies and agencies charged with preventing illicit financial crime.

- Many scam incidents do not lead to SAR filings: It estimated that in 2017, EFE-related SARs filed accounted for less than 2 percent of actual EFE incidents.[21] Disturbingly, the number of EFE-related SARs has increased every year, even though estimates suggest that only a small minority of EFEs result in a SAR filing.[22]
- Scams are sometimes the first step in subsequent money laundering activities. Often, funds received through scams are transferred to other accounts via money mules.[23] These are funnel accounts.
- Preventing account takeover is a critical challenge. FinCEN reported that most elder scam-related filings referenced account takeovers.[24]
- Sharing is inconsistent. The likelihood that an EFE results in a SAR appears to vary widely across institutions. In the 12 months

ending in June 2023, two banks made 33 percent of all SAR filings.[25] Fewer than 5,000 financial institutions filed EFE-related SARs during that period. Given that this number includes money service businesses and other covered non-banks, it is likely that thousands of depository institutions did not file any EFE-related SARs.

- According to FinCEN, most EFEs involved transfers made through money service businesses (MSBs) to scammers operating from Africa and Asia. SARs involving EFEs filed by depositories were much less likely to indicate a foreign recipient, but 47 percent could not identify the location. [26]

While seniors may be the most vulnerable, scammers are constantly seeking victims everywhere.

## **Problem:** *The challenges posed by bank-fintech partnerships.*

Banks must work through conflicting incentives when designing their online account applications. While marketing departments strive to minimize "friction" in the account opening process, banks still need to collect information to make sure the account is legitimate. Naturally, these priorities compete with each other. During onboarding, each new data point introduces additional risk that applicants may not complete their applications.[27] For startup fintechs, often funded by impatient investors, the temptation to reduce friction is strong. For bank partners seeking to attract fintech clients, a similar reason exists to ease the onboarding of new applications. If a fintech perceives that a partner bank's conservative compliance policies will constrain its growth, it will have an incentive to seek a different partner.

*Table 1: List of accounts opened for a fintech partner of Evolve Bank & Trust*

| Phone First 3 | Country Code | Address Type | Permission | City | Country | ZIP | Street | State | Deposit US Bal |
|---|---|---|---|---|---|---|---|---|---|
| 923 | Pakistan | PO Box | Locked | Clovis | US | 93611 | 1187 N. Willow Ave #103-812 | CA | 0.67 |
| 923 | Pakistan | PO Box | Locked | Clovis | US | 93611 | 1187 N. Willow Ave #103-812 | CA | 82.03 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | | WY | 116.17 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 1309 Coffee Ave Ste 1200 | WY | 210.28 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 1309 Coffee Ave Ste 1200 | WY | 110.08 |
| 923 | Pakistan | Reg Agent | Send and Receive | Sheridan | US | 82801 | 1309 Coffee Ave Ste 1200 | WY | 1307.8 |
| 923 | Pakistan | Reg Agent | Send and Receive | Sheridan | US | 82801 | 1309 Coffee Ave Ste 1200 | WY | 1072 |
| 971 | UAE | Reg Agent | Send and Receive | Sheridan | US | 82801 | 1309 Coffee Ave Ste 1200 | WY | 488.36 |
| 798 | Russia | Reg Agent | Closed | Sheridan | US | 82801 | 1309 Coffee Ave Ste 1200 | WY | 9059 |
| 923 | Pakistan | Reg Agent | Closed | Lewes | US | 19958 | 16192 Coastal Hwy | DE | 0.5 |
| 923 | Pakistan | Reg Agent | Closed | Lewes | US | 19958 | 16192 Coastal Hwy | DE | 0.88 |
| 923 | Pakistan | Reg Agent | Closed | Lewes | US | 19958 | 16192 Coastal Hwy | DE | 0.44 |
| 923 | Pakistan | Reg Agent | Closed | Lewes | US | 19958 | 16192 Coastal Hwy | DE | 675.62 |
| 923 | Pakistan | Reg Agent | Locked | Lewes | US | 19958 | 16192 Coastal Hwy | DE | 2175.8 |
| 790 | Russia | Reg Agent | Locked | Lewes | US | 19958 | 16192 Coastal Hwy | DE | 55.03 |
| 791 | Russia | Reg Agent | Closed | Lewes | US | 19958 | 16192 Coastal Hwy | DE | 4.51 |
| 971 | UAE | Reg Agent | Send and Receive | Lewes | US | 19958 | 16192 Coastal Hwy # 14/3 | DE | 856.25 |
| 923 | Pakistan | Reg Agent | Send and Receive | Sheridan | US | 82801 | 30 N Gould St Ste 23609 | WY | 4094.71 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste 23983 | WY | 0.01 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste 24157 | WY | 1227.26 |
| 971 | UAE | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste 24446 | WY | 1 |
| 923 | Pakistan | Reg Agent | Send and Receive | Sheridan | US | 82801 | 30 N Gould St Ste 24614 | WY | 0.84 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste 24632 | WY | 0.14 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste 25211 | WY | 0.02 |
| 923 | Pakistan | Reg Agent | Send and Receive | Sheridan | US | 82801 | 30 N Gould St Ste 4000 | WY | 0.12 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste 5042 | WY | 2840.12 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste 7134 | WY | 3.112 |
| 923 | Pakistan | Reg Agent | Locked | Sheridan | US | 82801 | 30 N Gould St Ste R | WY | 0.91 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste R | WY | 3.07 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste R | WY | 0.09 |
| 923 | Pakistan | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste R | WY | 475.6 |
| 971 | UAE | Reg Agent | Send and Receive | Sheridan | US | 82801 | 30 N Gould St Ste R | WY | 0.07 |
| 971 | UAE | Reg Agent | Closed | Sheridan | US | 82801 | 30 N Gould St Ste R | WY | 28.6 |

The interagency guidance on third-party relationships makes it clear that banks are responsible for the actions of their fintech partners.[28] In recent years, many sponsor banks in fintech partnerships have faced penalties for non-compliance.[29] It underscores a fundamental problem. Banks should be risk-averse, but in partnerships, they must lean into risk to attract clients. Any player in the ecosystem – banks, fintechs, banking-as-a-service companies, and fintech investors – could decide it has a financial incentive to take risks to attract business partners. Decisions to move forward with risk may be inevitable when a "move fast and break things" culture meets the staid world of commercial banking.

For example, Evolve Bank & Trust (Evolve), a partner bank to fintechs, was recently found to have permitted scores of accounts to be opened from a single Wyoming address by applicants with IP addresses in foreign countries, including some on the Office of Foreign Assets Control (OFAC) list. The scenario in **Table 1** shows the status of a set of Evolve accounts that were opened, presumably by criminals using synthetic identities.[30]

Evolve approved these accounts through its partnership with Mercury, a fintech company serving businesses.[31] The document displays the operational capabilities of the accounts at the time of ledger publication ("permission"), including the phone number prefix and country code of the device used to open the account, the address of record for the account (Street), and the current balance (Deposit US balance). Send and receive accounts are fully capable of making fund transfers. Locked accounts are open but cannot send or receive funds. While many are now closed, they were all active at one point, and all still had balances when this ledger was published in a court filing. The same hearing found evidence that Evolve had failed to fulfill the Office of Foreign Asset Control's requirements for seven years.[32]

Criminals have used fintech accounts issued by Evolve for other third-party fintech programs. For example, a Nigerian group used Juno debit card accounts to receive funds from business email compromise scams, tax scams, and romance scams.[33]

In January 2024, the Federal Reserve issued an enforcement action against Evolve for deficiencies in its anti-money laundering, risk management, and consumer compliance programs.[34] The order required Evolve to develop procedures for monitoring and investigating consumer complaints. However, the Federal Reserve's order did not recommend financial redress for consumers. Unwinding the problem has been difficult. The lack of clear record-keeping was the primary hurdle the FDIC faced when attempting to return funds to depositors. However, the attendant issue of how this vulnerability enabled scams has not been addressed.

The problems at Evolve, coming after so many enforcement actions against other partner banks, make clear the need to enhance scrutiny of BaaS firms that are central to many fintech partnerships. The prudential regulators (the OCC, Federal Reserve, FDIC, and NCUA) should tighten supervision of these relationships. The Bank Service Company Act, which covers third-party arrangements that outsource banking activities, provides a basis to argue that the Federal Reserve has this authority. Still, the Federal Reserve should clarify that it does. In some views, the BSCA is underutilized.[35]

***Unfortunately, this is not just a problem for bank-fintech partnerships. Banks of all sizes can still succumb to the temptation to lighten anti-fraud rules in favor of opening more accounts.***

Nonetheless, even larger banks may fall prey to prioritizing growth over prudence. In its 2024 consent order against TD North, Treasury and the OCC wrote that the bank "pursued growth without ensuring that it had established and maintained an adequate BSA/AML program."[36] Ironically, TD had branded itself as "America's most convenient bank."

In its filing, the Department of Justice criticized TD North for failing to monitor Zelle transfers.


From 2017 until August 2020, TD did not screen Zelle transfers for suspicious activity. During that time, TD customers transferred $75 billion through Zelle. All those transactions were unmonitored. Starting in August 2020, TD North deployed two systems to identify high-risk Zelle transfers, but only flagged activity exceeding $10,000 in deposits or $9,000 in transfers over any 5-day period.[37] The Department of Justice noted that such protections were largely irrelevant, as Zelle activity could not exceed $10,000 in any 30-day period. In other words, account monitoring systems were designed to block transfers that would not be permitted under Zelle's rules – a meaningless bar.[38]

In a settlement, TD North agreed to pay $3.1 billion to the OCC, FinCEN, Treasury, and the Federal Reserve to resolve violations. It also agreed to limits on its future growth, dividend payouts, and share repurchases. The bank agreed to enhance its fraud prevention processes, compliance programs, and reporting procedures.[39]

Once again, consumer protections were divorced from a significant BSA enforcement action. The TD North orders did not identify consumer harms associated with Zelle transfers, but their findings show that TD North's practices—by not monitoring Zelle transactions—left the bank blind to the possibility of such harm. Although the impacts on consumers were not revealed in the order, such a possibility should not be discounted, as regulators pursuing violations of BSA rules were not looking for it.

# GETTING TO SOLUTIONS

## Examining the landscape of regulatory authority

The Department of the Treasury has primary responsibility for implementing and enforcing the Bank Secrecy Act. It has delegated the authority to FinCEN. FinCEN has redelegated compliance responsibilities to various federal agencies, including the Office of the Comptroller of the Currency (OCC), the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Internal Revenue Service.[40] The CFPB does not conduct BSA compliance examinations, as the BSA is not a federal consumer financial law. Prudential regulators and FinCEN can bring civil money penalty actions. Additionally, the BSA does not permit a private right of action, and SARs cannot be subpoenaed in civil courts.

The CFPB has authority for 18 consumer financial protection laws, including the EFTA. It can

use enforcement authority to address unfair, deceptive, and abusive acts and practices (UDAAPs). These authorities can overlap. The CFPB brought its 2024 lawsuit against Early Warning Services, Bank of America, JPMorgan Chase, and Wells Fargo using its EFTA authority, but the order involved causes of action that violated prohibitions against UDAAPs."[41] The FTC's role in preventing fraud and scams derives from its statutory power to prohibit unfair or deceptive acts or practices.

States may enforce their anti-money laundering laws by penalizing supervised institutions, such as state-licensed money transmitters or state-chartered banks, through enforcement actions.

Victims have no way to seek remedies for losses resulting from poor know your customer (KYC) or customer identification program (CIP) compliance, or from poor CDD compliance. Even though an RDFI's non-compliance caused harm, it does not have a duty of care for the victim. Private litigants are unable to pursue RDFIs, either, as financial institutions cannot disclose information about an account holder who received funds in a scam to the victim, including in civil court proceedings.[42]

The CFPB's order issued against Block in 2025,[43] which focused on EFTA and unfairness, while state regulators focused on BSA/AML compliance,[44] highlights the interconnectedness of these issues and underscores the opportunity for cooperation between agencies with different mandates. Importantly, the CFPB's order called for consumers to receive $75 million in redress.

**Victims have no way to seek remedies for losses resulting from poor know your customer or customer identification program compliance, or from poor CDD compliance.**

## Solution: *Make better use of SARs*

A key question is how to bridge the scope of BSA/AML work traditionally conducted by FinCEN and the prudential regulators with the CFPB's and the FTC's respective remits. A first step would be to share information for the greater good. The Patriot Act permits law enforcement agencies to request information from financial institutions.[45] But the need is for better information-sharing inside the financial system. If granted permission by FinCEN, banks can share information with other financial institutions. But there are many conditions placed on the process.[46]

For now, most SARs are sent to law enforcement agencies. The Internal Revenue Service, the Federal Bureau of Investigation, the Drug Enforcement Administration, the Department of Homeland Security, and the Department of Justice receive SARs. Institutionally, these agencies are averse to sharing information. Their instinct is to protect information for potential use in court, rather than to provide trend analysis and updates across the financial system. Indeed, in some cases, law enforcement may want an account suspected of illicit use to remain open to better understand criminal organizations' activities.

Clearly, there is utility in using SARs for consumer protection work, and a history of the CFPB accessing them. As it stands, the CFPB receives SARs from FinCEN for information, but cannot use them as evidence in its enforcement work. The CFPB has also used batches of SARs to produce data spotlights on fraud.[47]

While some compliance failures will not have led to scams, others will. Many SARs are filed for transfers between accounts held by criminals, not between a victim and a criminal. Those are important, but they are not relevant to this paper. Likewise, the CFPB does not need reports on violations that have no bearing on consumers' financial security. However, if the data provides a reasonable basis to believe that a SAR could contain relevant information for violations of consumer protection laws, the CFPB should have access to these documents. This information would amplify the impacts of the CFPB's anti-fraud enforcement work.

By many accounts, there is a widely held view that policies for filing SARs require a rethink, but disagreement on the proper course.[48] One current proposal would raise the threshold for filing CTRs to $30,000 for banks, to $3,000 for non-bank money service businesses, limit insight into possible "structuring, and lessen ongoing reviews of suspicious accounts. [49] Separately, in naming a list of regulations that are "no longer necessary," the Treasury Department announced that it would rescind a FinCEN rule establishing civil monetary penalties for certain BSA-related reporting and recordkeeping rules.[50] These changes would move in the wrong direction. The problem today is how SARs are used to identify patterns, prevent fraud, and hold wrongdoers accountable. One challenge is to find the best way to safely share information to maximize its capabilities. But reducing the amount of available data, while certainly less work, removes a tool for preventing financial crime.

Separately, prudential regulators have ceased including "reputational risk" in their examinations.[51] Regulators are falling out of step with common sense. When a bank permits fraud, it undermines its reputation and may erode public trust in banking.

But more importantly, SAR filings should serve as a resource for interagency activity. Reports indicate that only 4 percent of SARs are ever forwarded to law enforcement.[52] That number suggests that SARs are not being used effectively. If SARs become dead letters – filed and never heard from again – it begs the question: why were they filed in the first place? When possible, FinCEN should use this resource to help the CFPB to combat scams. The line between scams and money laundering is blurring. As it is, there are too many roadblocks. For example, banks cannot supply SAR information directly to the CFPB. To address industry concerns about rules prohibiting the disclosure of SARs, BSA regulators would need to issue guidance clarifying that such sharing is lawful.[53] When the CFPB receives SARs from FinCEN, its enforcement teams should be able to use them as evidence in investigations. While acknowledging that some redaction may be appropriate, law enforcement agencies should retain some level of access to SARs.

### **Solution:** *Distribute funds from BSA enforcement to provide remedies for victims of scams.*

There is a victim – or perhaps many victims – behind each scam When considering the reasons this is possible, the significance of RDFIs is especially relevant, given that criminals scour the internet to find banks with lax CDD systems. In underground markets, criminals seek access to stolen accounts that are most likely to evade suspicion, such as those that have been active for over a year or that their legitimate owners have used to make larger fund transfers. Sometimes, criminals open accounts, groom them for months or years by making innocuous deposits and withdrawals to mimic legal use, and then sell them at a premium on the dark web. Some even post pictures of account histories to enhance the desirability of for-sale accounts.[54]

Those accounts may have been used to transfer funds among criminals involved in various illicit money-laundering activities. Some transfers will be used to move money between criminals to operate their illegal enterprises. However, some accounts opened by criminals will be used to perpetrate imposter scams, investment scams, or other scams. The same dynamic applies to accounts that have been taken over: some are used for money laundering, while others are used to receive transfers from fraudulent activity. The latter outcome highlights the importance of incorporating consumer protection components into BSA supervision. When consumers are induced to send funds to a scammer, activities that regulators review for BSA compliance are relevant.

EFTA protects consumers when funds are lost due to unauthorized transfers but leaves victims without recourse if they authorize the transfers. Practically speaking, the current regulatory framework prevents scam victims from receiving relief. Changing enforcement to give victims a share of bank penalties will sidestep one hurdle posed by outdated regulatory distinctions between fraud and scams.[55] While it will not have uniform effects – as it will only aid victims of the most significant failures – it moves in the right direction.

**Solution:** *The funds needed to provide remedies to victims are available. Regulators collect funds when financial institutions fail to comply with BSA/AML laws.*

The resources exist to include consumers in relief. Consent orders and settlements resulting from successful enforcement work often include civil money penalties. However, those funds are paid to government agencies, not to victims.

These penalties are typically added to a list of corrective actions. Those steps could include calls to improve CIP programs; reviews of new products and information technology systems; prompt filing of SARs and CTRs; training for compliance staff; third-party risk management reviews; general reviews of end-to-end compliance; and other remediations.

Regulators could approach relief in two ways. On one hand, they could provide victims with a share of the funds collected in penalties. Alternatively, they could add consumer remedies to penalty assessments. Either works – the key principle is to ensure that victims do not continue to go without meaningful relief.

Of course, providing relief in BSA/AML enforcement actions will not help all victims of fraud. Scams occur everywhere – not just at the financial institutions that receive enforcement orders. However, it will matter in many cases. It could also have a preventive effect. If consumer remedies were required in addition to civil money penalties, it would increase the costs for the outlier, "worst-practice" financial institutions that deploy "know your customer light" policies, along with other shortcuts, that put people at risk. In doing so, it puts more pressure on financial institutions to invest in fraud prevention.

**Solution:** *While often perceived as categorically distinct, BSA and EFTA can both protect consumers from the harms of induced P2P fraud.*

The CFPB's retreat from active supervision and enforcement removes a critical source of pressure on financial institutions to curb induced P2P fraud, even as such fraud continues to rise and artificial intelligence increases its sophistication. Yet the absence of federal leadership does not leave consumers defenseless. States retain authority—and proven tools—to intervene when federal regulators will not.

The CFPB's recent enforcement action against Block illustrates how consumer protection can be pursued from multiple levels. Using its authority under EFTA, the CFPB penalized Block for unfair and deceptive practices, citing

its failure to meet Regulation E's dispute-resolution and fraud-investigation requirements on Cash App. The agency's order imposed $175 million in penalties and required reforms to customer service and fraud-prevention systems.[56]

The New York Department of Financial Services (NYDFS) completed a separate case in April 2025. The case resulted from an event in 2022, when Block discovered that 8,359 of its Cash App accounts were linked to a Russian criminal network.[57] NYDFS gave Block credit for closing those accounts. While that was good, it brought to the surface clear evidence of how accounts support scams.

At the same time, a coalition of 48 state financial regulators reached an $80 million settlement with Block that targeted the same misconduct from a different direction—through the lens of BSA compliance. The state action addressed failures in identity verification, suspicious-activity reporting, and oversight of high-risk accounts.[58] Together, the federal and state settlements demonstrated that BSA obligations can be leveraged not only to combat money laundering but also to achieve concrete consumer-protection outcomes by compelling institutions to enhance fraud detection and onboarding controls. This is not the only example. Just last year, for example, the FDIC's consent order against Piermont Bank required the bank to remediate violations of the Bank Secrecy Act and to review all transactions since 2022 for evidence that it failed to meet EFTA's dispute resolution requirements.[59]

The Block cases demonstrate that BSA and EFTA enforcement can complement one another, and that states need not wait for the CFPB to re-engage before acting. Just as state regulators joined forces in earlier Zelle investigations, they can continue to use their own BSA authority to fill the enforcement void and protect consumers from the ongoing wave of induced P2P fraud. A complementary approach can rely on referrals between agencies. While formal rulemaking could add durability, guidance calling for interagency cooperation to connect the BSA/AML work with consumer protection efforts could also be an effective path forward. It also has the benefit of simplicity and expediency. This approach provides a pathway to deliver relief to scam victims without requiring Congressional action to amend the EFTA.

### **Solution:** *When CDD programs are unusually poor and permit widespread account openings by criminals, it rises to the level of an unfair practice.*

The FTC and CFPB should apply the unfairness standard to address banks with unusually inadequate CDD programs. Under Section 5 of the FTC Act, the FTC has the authority to prohibit unfair practices.

These outcomes should be read to meet the unfairness standard in the FTC Act: Poor CDD programs cause or are likely to cause substantial injury to consumers, consumers cannot reasonably avoid those harms, and those effects are not outweighed by countervailing benefits to consumers or to competition.

Applying the unfairness standard could overcome procedural barriers that have previously limited consumer redress. Using a claim of unfairness for losses suffered by senders would create opportunities that arbitration clauses might otherwise prevent when claims are made against the account holder's bank. Victims who sent money to accounts opened due to RDFIs' failures to vet account applications or to properly police account takeovers (ATOs) have not signed arbitration agreements with RDFIs, nor have they waived their rights to a class action. Recognizing these practices as unfair would create another viable legal pathway to aid consumers harmed by induced P2P fraud.

The prudential regulators could clarify in their exam handbooks that the unfairness standard and UDAP procedures apply to instances where banks fail to prevent illegal account openings that cause consumer harm. Including this information in an exam manual would serve as a critical warning to banks about the penalties for noncompliance. The OCC's handbook, for example, details how examiners should consider consumer complaints for

policies governing deposit products and deposit account management.[60] Similarly, states could apply their unfairness laws to cases involving the institutions they supervise. This method provides another pathway to integrate consumer protections into cases of scams resulting from poor BSA compliance.

## CONCLUSION

Historically, regulatory actions to thwart illicit finance have not overlapped with consumer financial protection. The large money-laundering operations of transnational criminal gangs occurred separately from the scams that used gift cards. But these organizations now make a new business out of tricking people into sending money. They are responding to an opportunity. This sea change calls for a re-examination of the relationship between these two seemingly very different regulatory authorities.

Policymakers can pursue complementary strategies. In principle, financial institutions should be held accountable for building and operating safe, "fraud-resistant" products. Prudential regulators, FinCEN, and other agencies responsible for BSA compliance must consider that non-compliance with BSA requirements is not just a matter of financial stability but also a consumer protection issue. Leveraging complementary authorities – such as prohibitions against UDAPs, compliance with BSA, and the unfairness standard – can reinforce EFTA's protections.

Cases such as those at Evolve and TD North demonstrate how lapses in BSA compliance create the very conditions that enable criminals to defraud consumers. Already, banks pay substantial civil money penalties for BSA/AML violations. However, these orders exclude consumers from relief. There may be cases where this is an oversight. While many BSA violations may not involve defrauding individuals through scams, others likely do. It is crucial to make it possible to consider the question.

New rules should be adopted that would do the following:

Change policies for redress to better support victims and compel financial institutions to improve in the future.

- Regulators should incorporate consumer redress into their enforcement of BSA violations, ensuring that victims are compensated when banks fail to fulfill their obligations. The BSA's requirements—verifying customer identities, monitoring suspicious activity, and filing timely reports—are essential safeguards.[61] When financial institutions – including transfers where they act as RDFIs - fail to meet them, consumer losses should not be ignored.
- While sharing a portion of penalties assessed to banks with consumer victims would be helpful, the best approach would be to require redress in addition to paying penalties. Higher costs for non-compliance can prompt financial institutions to enhance their compliance programs.

Provide clarity to financial institutions:

- Proactively, prudential regulators should update guidance, including the third-party guidance covering bank partnerships, to clarify how BSA compliance with CDD and suspicious activity monitoring programs includes consumer protections. This is a direct way to link BSA to consumer protection.
- Because many independent BaaS companies now perform essential services in banking, the prudential regulators should exert their authority under the Bank Service Company Act to examine them.
- To overcome concerns about violating rules against disclosing SARs, BSA regulators would need to issue guidance to clarify that such sharing complies with the law.[62]
- Regulators should make clear to financial institutions that when they fail to prevent criminals from using their accounts to conduct payment fraud, it rises to meet the standards of an unfair and deceptive practice.

In turn, when financial institutions receive clarity, they should be held accountable to act on it.

In 2018, the prudential regulators and FinCEN issued interagency guidance on how smaller banks and credit unions could share BSA/AML resources. The guidance sought to help banks reduce compliance costs. Suggestions included sharing BSA officers, collaborating on staff training, and engaging third-party contractors for technology services.[63] To date, few institutions have responded.[64]

When evidence shows that a financial institution's CDD processes have repeatedly failed to prevent criminals from using their services to create funnel accounts, the Federal Reserve should conduct a review. If the review finds that the institution's policies and procedures are not adequately robust to detect illicit finance, it should suspend the institution's master account.

Improve information sharing:

- FinCEN should reform how SARs are filed and used. While privacy is essential, regulators should prioritize measures that enable the ecosystem to benefit from SARs by expanding how SAR information can be shared with other banks to facilitate prompt identification of emerging fraud patterns. By implementing more immediate and transparent information-sharing systems, FinCEN should better use SARs to prevent future fraud.
- Legislation to raise thresholds for filing SARs or to limit instances where reports are necessary will reduce the amount of information available to regulators to prevent fraud.
- If it has a reasonable suspicion to believe a SAR could have relevant information for violations of consumer protection laws, the CFPB should have access to these documents and use them as part of exercising its authority to enforce consumer protection laws. This information would amplify the impacts of the CFPB's anti-fraud enforcement work.
- Expedite updates to model risk management systems.

When a bank's systematic failures to prevent funnel accounts result in scams, it should constitute an unfair practice. The FTC and CFPB should apply the unfairness standard to impose penalties on banks when dangerously inadequate CDD programs enable scams. States should do the same and follow suit where authority exists.

**When a bank's systematic failures to prevent funnel accounts result in scams, it should constitute an unfair practice.**

Industry governance can play a part, as well. Financial institutions, their trade associations, and governance standards-setting organizations should promote more fraud prevention and information sharing. As key gatekeepers in the exchange of fraud information, rulemaking bodies governing payment networks, such as Early Warning Systems or Nacha, must play a role in identifying risky RDFIs. If necessary, they should force worst-practice banks off their systems.

The Treasury Department, FinCEN, the Department of Justice, and the prudential regulators, the CFPB and FTC, can protect consumers by acting when banks fail to comply with their BSA obligations. Additionally, federal banking regulators and state agencies should protect account holders at ODFIs who have sent funds to RDFIs where criminals established funnel accounts.

Scams are both a financial crime and a consumer protection issue. The use of payment apps and digital banking will only continue to expand, but without corresponding updates to safeguards, consumers will bear the risk of institutional compliance failures. Financial regulators should adapt their enforcement and supervision to ensure that innovation does not come at the expense of consumer safety and trust in banking.

# ENDNOTES


1. FINRA. (2020, May 5). Regulatory Notice 20-13. https://www.finra.org/rules-guidance/notices/20-13

2. Federal Trade Commission. (2025). Consumer Sentinel Network Data Book 2024. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

3. Federal Trade Commission. (2025, March 10). New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024. Press Releases. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

4. 31 CFR § 1020.220 Customer identification programs for banks, savings associations, credit unions, and certain non-Federally regulated banks. And Federal Deposit Insurance Corporation. (n.d.). Bank Secrecy Act / Anti-Money Laundering (BSA/AML). Banker Resource Center. Retrieved October 25, 2025, from https://www.fdic.gov/banker-resource-center/bank-secrecy-act-anti-money-laundering-bsaaml

5. 31 U.S.C. § 5312(a)(2) The BSA definition of financial institutions is all-encompassing. Depositories are covered, but so are entities such as money transmitters, investment companies, and even pawnbrokers and travel agents.

6. 31 U.S.C. § 5318(g)(1

7. Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, National Credit Union Administration, & FinCEN. (2022, July 6). Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence. https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-18a.pdf

8. David Maimon. (2025, October 21). Fraud In America 2025: The Laundering Network Exploiting Banks. Forbes. https://www.forbes.com/sites/davidmaimon/2025/10/21/fraud-in-america-2025-the-laundering-network-exploiting-banks/

9. Sentilink. (2025). The Sentilink Fraud Report: Identity Fraud Rates and Trends (No. H1 2025). https://insight.sentilink.com/hubfs/The_SentiLink_Fraud_Report_H1_2025.pdf

10. Fraud.com (2023, April 5). 5 reasons behind the increase in digital banking fraud. https://www.fraud.com/post/increase-in-digital-banking-fraud

11. While it is not a topic of this paper, it is must be acknowledged that cryptocurrencies are contributing to substantial risks, as well.

12. David Patrick. (2025). 5 reasons US banks aren't sending Instant Payments (yet). RedCompass Labs. https://www.redcompass-labs.com/insights/5-challenges-us-banks-in-stant-payments-send/

13. Department of Justice, Department of Homeland Security, & US Department of the Treasury. (2018). 2018 National Money Laundering Risk Assessment. https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf

14. Hanna, J. M. (2020, March 18). FinCEN Issues Statement to Financial Institutions on BSA/AML Compliance During COVID-19 Pandemic. https://www.subjecttoinquiry.com/2020/03/fincen-issues-statement-to-financial-institutions-on-bsa-aml-compliance-during-covid-19-pandemic/

15. FinCEN. (2017). Advisory to Financial Institutions Regarding Disaster-Related Fraud (No. FIN-2017-A007). https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a007-0

16. Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation (FinCEN Advisory No. FIN-2011-A003). (2011). https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a003

17. Laila Bera. (2025). Elevating Fraud and Scams as a National Security Threat. Aspen Institute. https://fraudtaskforce.aspeninstitute.org/scams-as-national-security-threat

18. Raman, S., & Carlsen, N. (2025). The World's Underground Bankers. Lawfare. https://www.lawfaremedia.org/article/the-world-s-underground-bankers

19. McClure, T. (2025, December 2). Age of the 'scam state': How an illicit, multibillion-dollar industry has taken root in south-east Asia. The Guardian. https://www.theguardian.com/technology/2025/dec/02/scam-state-multi-billion-dollar-industry-south-east-asia

20. Sims, J. (2025). Policies and Patterns: State-Abetted Transnational Crime in Cambodia as a Global Security Threat. Human Research Consultancy. https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/68264cff-356caba111f2db1e_Policies%20and%20Patterns_16052025.pdf

21. CFPB Office of Financial Protection for Older Americans. (2019). Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends. https://files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf

22. FinCEN. (2022). Advisory on Elder Financial Exploitation (FinCEN Advisory No.

FIN-2022-A022). https://www.fincen.gov/system/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf

23. FinCEN. (2024). Elder Financial Exploitation: Threat Pattern and Trend Information, June 2022 to June 2023 [Financial Trend Analysis]. https://www.fincen.gov/system/files/shared/FTA_Elder_Financial_Exploitation_508Final.pdf

24. FinCEN. (2019). Elders Face Increased Financial Threat from Domestic and Foreign Actors [Financial Trend Analysis]. https://www.fincen.gov/system/files/shared/FinCEN%20Financial%20Trend%20Analysis%20Elders_FINAL%20508.pdf

25. Ibid.

26. Ibid.

27. Terry Badger. (2023, February 10). Fixing the top of the digital funnel. BAI. https://www.bai.org/banking-strategies/fixing-the-top-of-the-digital-funnel/

28. Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, & Board of Governors of the Federal Reserve System. (2023, June 6). Interagency Guidance on Third-Party Relationships: Risk Management. https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html

29. S&P Global. (2024, January 23). Small group of banking-as-a-service banks logs big number of enforcement actions. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/small-group-of-banking-as-a-service-banks-logs-big-number-of-enforcement-actions-80067110

30. Mikula, J. (2024, July 21). Synapse Program Was "Nightmare Fuel" Due To Control Gaps, Ex-Employee Says [Substack newsletter]. Fintech Business Weekly. https://fintechbusinessweekly.substack.com/p/synapse-program-was-nightmare-fuel

31. On December 19th, 2025, Mercury applied for a national bank charter. See https://mercury.com/blog/occ-national-bank-charter-application

32. Ibid

33. Jason Mikula. (2024, July 21). Synapse Program Was "Nightmare Fuel" Due To Control Gaps, Ex-Employee Says [Substack]. Fintech Business Weekly. https://substack.com/home/post/p-146780525

34. Federal Reserve Board issues an enforcement action against Evolve Bancorp, Inc. And Evolve Bank & Trust for deficiencies in the bank's anti-money laundering, risk management, and consumer compliance programs. (n.d.). Board of Governors of the Federal Reserve System. Retrieved September 25, 2025, from https://www.federalreserve.gov/newsevents/pressreleases/enforcement20240614a.htm

35. Kiah Lau Haslett. (2025, January 9). Regulatory Exams of Third-Parties Are Hard to Find, Sometimes "Stale," Critics Say. FinXTech. https://finxtech.com/regulatory-exams-of-third-parties-are-hard-to-find-sometimes-stale-critics-say/

36. United States Department of the Treasury & Office of the Comptroller of the Currency. (2024). In the Matter of TD Bank, N.A. and TD Bank, USA, NA [Consent Order]. https://www.occ.gov/static/enforcement-actions/eaAA-ENF-2024-77.pdf

37. Banks must file a Currency Transaction Report for cash transactions above $10,000.

38. United States of America v. TD Bank, N.A. (United States District Court District of New Jersey October 10, 2024). https://www.aba.com/-/media/documents/extranet/banking-docket/10102024---in-re-bank---doj-information-sheet.pdf?rev=573c8517c7b346c39e50d241cebfe1c5

39. Office of the Comptroller of the Currency. (2024). In the Matter of TD Bank, N.A. and TD Bank USA, N.A. https://www.occ.gov/static/enforcement-actions/eaAA-ENF-2024-77.pdf

40. Internal Revenue Service. (n.d.). 4.26.7 Bank Secrecy Act Penalties. Retrieved November 16, 2025, from https://www.irs.gov/irm/part4/irm_04-026-007

41. Consumer Financial Protection Bureau. (2024). Consumer Financial Protection Bureau v Early Warning Services, Bank of America, JPMorgan Chase Bank, and Wells Fargo Bank, NA. [Complaint for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief]. https://www.consumerfinance.gov/enforcement/actions/early-warning-services-llc-bank-of-america-na-jpmorgan-chase-bank-na-wells-fargo-bank-na/

42. 12 U.S.C. § 5533(b)(2)–(3)

43. Consumer Financial Protection Bureau. (2025, January 16). CFPB Orders Operator of Cash App to Pay $175 Million and Fix Its Failures on Fraud. https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-operator-of-cash-app-to-pay-175-million-and-fix-its-failures-on-fraud/

44. Nawrocki, T. (2025, April 11). Block Hit with $40M Fine Amid Ongoing Compliance Failures. Payments Journal. https://www.paymentsjournal.com/block-hit-with-40m-fine-amid-ongoing-compliance-failures/

45. Patriot Act, Section 314(a)

46. Patriot Act, Section 314(b).

47. Data Spotlight: Suspicious Activity Reports on Elder Financial Exploitation. (2024, December 12). Consumer Financial Protection Bureau. https://www.consumerfinance.gov/data-research/research-reports/data-spotlight-suspicious-activity-reports-on-elder-financial-exploitation/full-report/

48. Claire Williams. (2025, October 9). Exclusive: Regulators move to ease banks' SAR burden. American Banker. https://www.americanbanker.com/news/exclusive-regulators-move-to-ease-banks-sar-burden

49. John Heltman. (2025, October 21). Senate Republicans propose raising SAR threshold to $30K. American Banker. https://www.americanbanker.com/news/senate-republicans-propose-raising-sar-threshold-to-30k

50. FinCEN to eliminate 'redundant' Bank Secrecy Act civil penalty rule. (2025, April 15). ABA Banking Journal. https://bankingjournal.aba.com/2025/04/fincen-to-eliminate-redundant-bank-secrecy-act-civil-penalty-rule/

51. Office of the Comptroller of the Currency. (2025, March 20). OCC Ceases Examinations for Reputation Risk. https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-21.html

52. Aibangbee, Y. (2020, September 22). The Truth About Suspicious Activity Reports. Bank Policy Institute. https://bpi.com/the-truth-about-suspicious-activity-reports/

53. McGuireWoods Government Investigations Group. (2014, January 6). The CFPB and BSA/AML Compliance – Can the CFPB Properly Request a SAR? Subject to Inquiry. https://www.subjecttoinquiry.com/2014/01/the-cfpb-and-bsaaml-compliance-can-the-cfpb-properly-request-a-sar/

54. Maimon, D. (2025, February 26). Investigating Stolen and Forged Treasury Checks. https://resources.sentilink.com/blog/stolen-and-forged-treasury-checks

55. See for example, FedNow. (n.d.). FraudClassifier. https://explore.fednow.org/resources/fraud-classifier.pdf

56. Consumer Financial Protection Bureau. (2025, January 16). CFPB Orders Operator of Cash App to Pay $175 Million and Fix Its Failures on Fraud. https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-operator-of-cash-app-to-pay-175-million-and-fix-its-failures-on-fraud/

57. Howard Bush. (2018, September 11). Reduce false positives, become more efficient by automating anti-money laundering detection. Microsoft Azure Artificial Intelligence. https://azure.microsoft.com/en-us/blog/reduce-false-positives-become-more-efficient-by-automating-anti-money-laundering-detection/

58. Conference of State Bank Supervisors. (2025, January 15). State Regulators Issue $80 Million Penalty to Block, Inc., Cash App for BSA/AML Violations. https://www.csbs.org/newsroom/state-regulators-issue-80-million-penalty-block-inc-cash-app-bsaaml-violations

59. Federal Deposit Insurance Corporation. (2024). In the Matter of Piermont Bank, New York, New York (Consent Order No. FDIC 23-0038b). https://www.fdic.gov/system/files/2024-06/piermont-bank-ny-ny-mod-2019.pdf

60. Office of the Comptroller of the Currency. (2020). Unfair or Deceptive Acts and Practices or Unfair, Deceptive or Abusive Acts and Practices (Consumer Compliance) [Comptroller's Handbook]. https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/unfair-deceptive-act/pub-ch-udap-udaap.pdf

61. 31 C.F.R. § 1020.220(a).

62. McGuireWoods Government Investigations Group. (2014, January 6). The CFPB and BSA/AML Compliance – Can the CFPB Properly Request a SAR? Subject to Inquiry. https://www.subjecttoinquiry.com/2014/01/the-cfpb-and-bsaaml-compliance-can-the-cfpb-properly-request-a-sar/

63. Board of Governors of the Federal Reserve, Federal Deposit Insurance Corporation, National Credit Union Administration, FinCEN, & Office of the Comptroller of the Currency. (2018). Federal Agencies Issue a Joint Statement on Banks and Credit Unions Sharing Resources to Improve Efficiency and Effectiveness of Bank Secrecy Act Compliance (No. News Release 2018-107). https://www.occ.gov/news-issuances/news-releases/2018/nr-ia-2018-107.html

64. Interview with an industry professional. December 19, 2025.