Statement for the Record

Adam Rust
Consumer Federation of America
For the hearing
"Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."
Subcommittee on Financial Institutions
House Financial Services Committee
2120 Rayburn House Office Building
March 5, 2026

Honorable Chair Andy Barr Room 2430
Rayburn House Office Building
Washington, DC 20515

Ranking Member Bill Foster
Rayburn House Office Building Room 2336
Washington, DC 20515

Dear Honorable Chair Barr and Ranking Member Foster:

Thank you for the opportunity to submit this statement and testify before your committee.

The Consumer Federation of America (CFA) is an association of non-profit consumer organizations established in 1968 to advance consumer interests through research, advocacy, and education.

Financial fraud and scams represent one of the most rapidly escalating threats to American consumers and the integrity of our financial system. Today, criminal organizations apply sophisticated scams, evade detection, and adapt their methods to stay ahead of law enforcement. They impersonate government officials to collect fabricated debts, pose as employers directing employees to transfer funds, and exploit personal relationships by masquerading as family members or close friends facing emergencies. They manipulate victims through romance schemes, fraudulent lottery notifications, and targeted extortions. These examples represent only a subset of their tactics, and new ones emerge regularly. While they differ in their methods, they share a common purpose: to compel a victim to send money. No individual is truly insulated from these threats. They affect people from all backgrounds, civilians and servicemembers, old and young, rich and poor, and in every Congressional district.[1]

These are escalating problems demanding attention. The number of fraud reports has increased steadily over the last 25 years. In 2001, the Federal Trade Commission received 325,519 fraud complaints; in 2024, more than 1.8 million; and in 2024, approximately 6.47 million.[2] We know of reports from victims totaling $12.5 billion in losses,[3] but the number is surely greater, as many victims never file a report.

They have increased in part because of converging forces in American life that give criminals more opportunities. Twenty years ago, people did not carry internet-connected mobile devices capable of initiating electronic funds transfers. Most financial arrangements occurred in person rather than over the internet, and bank-fintech partnerships were yet to come. Social media platforms existed, but they were not ubiquitous forums for information sharing. Digital commerce was conducted almost exclusively with network-branded cards, which carried (and continue to carry) fraud protection and institutional scam-prevention technologies. To the extent that our personal data was available online, the scope is only greater now, and constant breaches of private information were still to come. Facebook was exclusively for students until 2005 and did not have a chat function until 2008.[4] All of these forces reinforce each other, creating environments where fraudsters can reach virtually anyone, to the benefit of criminal organizations seeking to steal from people.

The primary law governing consumer fraud protections for electronic funds transfers – the Electronic Funds Transfer Act – was passed almost fifty years ago. It gives consumers rights against unauthorized transfers, but the protection available to victims of scams is at best thin. Transfers authorized by payment

---

[1] Federal Bureau of Investigation. (2025). *Internet Crime Report*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[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). New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[4] Felix Richter. (2019, February 5). How Facebook grew from 0 to 2.3 billion users in 15 years. World Economic Forum. https://www.weforum.org/stories/2019/02/how-facebook-grew-from-0-to-2-3-billion-users-in-15-years/

apps, wire transfers, digital assets, and bank P2P apps are considered authorized. To the extent scam victims receive relief, it is due to voluntary responses by providers, and not by the force of law.

It is within this context that the Committee convenes today.

The Consumer Financial Protection Bureau (CFPB) fights for consumers who are victims of scams and fraud.

The Consumer Financial Protection Bureau plays a critical role in protecting the financial security of American households from scams. In payment, the CFPB's gambit includes authority for the Electronic Funds Transfer Act (EFTA) and Regulation E. The CFPB can also apply its powers to prohibit unfair, deceptive, and abusive acts and practices. Through consumer response, the CFPB takes action when consumers file complaints.

As recently as a year ago, the CFPB was taking meaningful and increasingly assertive steps to address the crisis of scams. In December 2024, the CFPB filed a lawsuit against Early Warning Systems (EWS), the company behind the Zelle network, along with three of its major bank owners. The lawsuit alleged operational failures that left consumers without adequate protection from scams, resulting in an estimated $870 million in consumer losses.

In January 2025, the CFPB ordered Block, the corporate parent of Cash App, to pay $175 million in relief to harmed consumers and to implement substantive improvements to its fraud-prevention infrastructure. The CFPB found that Block violated the Electronic Funds Transfer Act (EFTA) by failing to investigate unauthorized transactions properly and by having inadequate fraud-detection systems.[5]

These actions sent a clear signal that the CFPB was prepared to hold banks and non-banks accountable when payment companies introduced unsafe products to the market. Moreover, the CFPB had shown that it would apply not just its powers under EFTA, but also those against UDAAPs, to help victims. But the attempts to shutter the CFPB make consumers vulnerable to scams and fraud.

Unfortunately, recent attacks on the CFPB have made consumers vulnerable to scams, prevented the agency from supervising payment apps, and absolved companies of accountability.

In March 2025, the CFPB dropped its lawsuit against EWS, Bank of America, Wells Fargo, and JPMorgan Chase. Furthermore, it did so *with prejudice,* meaning that it cannot be refiled.

In May 2025, Congress passed a resolution disapproving of the CFPB's November 2024 rule (the "payment apps rule") that would have subjected larger participant non-bank payment app and digital wallet products to federal supervision. The payment apps rule would have given the CFPB the authority to monitor the payment apps relied on by tens of millions of households to transfer funds. Incredibly,

[5] 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/

Congress chose to remove a layer of oversight only two months after the Federal Trade Commission released new data showing that fraud-related losses on payment apps had tripled from 2021 to 2024.[6]

Because of the reversal of the payment apps rule, the pressures that prevailed on EWS to address Zelle's risk controls are unlikely to be brought to bear on non-bank payment apps and digital wallets. True, the CFPB retains enforcement authority for any violations of EFTA. But in practice, the new administration has eviscerated the CFPB's supervision and enforcement work. The oversight gap will only grow larger over time, as the volume of payment app transfers increases and new entrants add to the number of now federally unsupervised companies. Payment apps continue to be the subject of many consumer complaints. In the 3rd quarter of 2025, payment app complaints crossed a new threshold. For the first time, payment apps were the leading payment type involved in fraud-related complaints tracked by the FTC.[7]

Congress should restore the CFPB's authority to supervise non-bank payment apps and digital wallets and build on the 2024 rule by adding supervision of transfers involving digital assets.

CFPB funding should be restored to its full level

In the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), Congress established an important provision allocating up to 12% of the Federal Reserve's earnings to fund the CFPB. Earlier this year, the CFPB's funding cap was reduced to 6.5 percent of the Federal Reserve's 2009 operating expenses, with inflation adjustments. By slashing the agency's budget, Congress has undercut the agency's ability to fulfill its duties.

During this time, the new administration has attempted to illegally shutter the CFPB. New leadership at the CFPB has attempted to conduct massive reduction-in-force (RIF) orders.[8] It has ordered staff to stop work. To the extent that supervision occurs, it is far more limited. Sixty-seven guidances were withdrawn in a single day.[9] The agency has permanently dismissed 22 enforcement actions. As a result, consumers have lost $3.5 billion in restitution that would otherwise have been paid to remedy the harm they experienced at the hands of the offending companies.[10]

Nonetheless, the American people are still approaching the CFPB, seeking a resolution to problems they have encountered with their financial services provider. The volume of complaints has grown every year since the agency's launch. In 2025, consumers filed more than five million complaints.

Unfortunately, the likelihood that a consumer receives relief is declining sharply. Data from the CFPB's complaint database reveals a dramatic and accelerating drop in the rate at which financial institutions are

---

[6] Federal Trade Commission. "All Fraud Reports by Payment Method: Year 2024." Tableau Public website. Fraud Reports, March 7, 2025. https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[7] Federal Trade Commission. "All Fraud Reports by Payment Method: Year 2025." Tableau Public website. Fraud Reports, December 11, 2025. https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[8] Caitlin Mullen. (2025, April 22). CFPB defends analysis behind 90% job cuts |. *Banking Dive*. https://www.bankingdive.com/news/cfpb-layoffs-job-cuts-vought-paoletta-nteu-berman-jackson-appeals-court/746009/

[9] Gabrielle Saulsberry. (2025, May 12). CFPB rescinds 67 pieces of guidance. *Banking Dive*. https://www.bankingdive.com/news/cfpb-rescinds-67-pieces-guidance-vought/747790/

[10] Senator Elizabeth Warren, Ranking Member. (2026). *New Report Finds Trump's Attack on the CFPB Has Cost Americans $19 Billion in One Year Alone*. United States Committee on Banking, Housing, and Urban Affairs. https://www.banking.senate.gov/imo/media/doc/cfpb_year_in_review_report.pdf

providing relief to complainants. The trend suggests that the companies now believe they face little accountability for ignoring customer complaints.

The data reveals a significant shift since 2024. Then, roughly half of all complaints resulted in a positive resolution for consumers, either monetary compensation or the correction of a problem. Beginning in summer 2025, patterns began to change, and positive outcomes became less common. By November 2025, only five percent resulted in relief. By mid-December, the figure fell below 1 percent.[11]

The CFPB has even pulled back on its commitment to help service members. In its initial RIF, the CFPB fired every staff member in the Office of Servicemember Affairs, save for its division leader. However, that staff member had accepted a voluntary retirement. Military and veterans organizations have expressed their strong support for the agency.[12] Indeed, the CFPB has the primary federal authority to supervise and enforce the Military Lending Act. Luckily, the courts stood up for service members, and the cuts were rejected.

Congress should restore the CFPB's funding to the original 12 percent cap as called for in the Dodd-Frank Act.

Unsafe financial products that harm consumers for reasons they cannot prevent are unfair.
The CFPB brought the 2024 lawsuit against EWS because it has EFTA authority for transfers, but the order involved causes of action that violated prohibitions against "unfair, deceptive, or abusive acts or practices (UDAAPs)."[13]

UDAAPs can occur when any covered financial product or service is offered. In an action using UDAAP, the cause(s) of action must meet the three-part unfairness standard: that the failures caused substantial injuries to consumers; consumers could not reasonably avoid the harms, and countervailing benefits to consumers or competition did not outweigh the injury.[14]

Companies should be accountable when they rush dangerous products to market – in any market. According to the CFPB, when EWS introduced Zelle, it designed the network for sending and receiving payment messages; however, it could have incorporated stronger fraud prevention capabilities into the software. For example, EWS could have embedded fraud-detection tools within the system's operating software. If it had done this, the network would have been safer. The CFPB held both the network and its three largest bank participants accountable for offering an unsafe product.

---

[11] Adam Rust. (2025, December 22). Trump's CFPB to Nearly a Million Americans: Goodbye, We Prefer Not To Help You · Consumer Federation of America. *Consumer Federation of America*. https://consumerfed.org/trumps-cfpb-to-nearly-a-million-americans-goodbye-we-prefer-not-to-help-you/

[12] Brief of Military and Veterans Organizations as Amici Curiae in Support of Petitioners, No. 22-448 (Supreme Court of the United States). Retrieved https://www.moaa.org/uploadedfiles/22-448-amicus-brief-of-military-and-veterans-organizations.pdf

[13] 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/

[14] 12 U.S.C. §§ 5531(a), 5536(a)(1)(B)

The complaint described six ways the network and the three bank defendants failed to prevent, detect, or limit fraud:[15]

- Maintaining inadequate systems for authenticating, verifying, and registering applicants to ensure "bad actors" were excluded from the network. For example, EWS permitted "token flipping," where users could register multiple Zelle tokens (with different phone numbers or email addresses) with a single bank. EWS allowed transfers to accounts whose email addresses or phone numbers (tokens) were not linked to a deposit account before the time of the payment order.
- Not giving consumers enough information about the recipients' identity. When launched, Zelle rules required only that banks indicate the recipient's first name, making it harder for a sender to recognize a problem.
- Failing to share some risk-related information with participating FIs that may have warned them to pause or block transfers. While rules required participants to report when an account was closed due to unauthorized fraud, they did not mandate the sharing of information related to induced fraud.
- Failing to suspend or block bad actors from participating in the network.
- Not requiring timely fraud information-sharing among participating FIs. The CFPB found that while network rules required FIs to report unauthorized frauds promptly, in practice, network participants were allowed to delay reporting until "long after it occurred."
- Failing to ensure participants followed network rules.

The events in this narrative meet the unfairness standard: consumers were harmed ($870 million in losses), they could not have prevented the incident (EWS introduced Zelle without safeguards), and there was no countervailing benefit to consumers or competition.

These shortcomings underscore the need for a governance layer in any payment system. Any network that moves consumer funds must be built with a governance layer that includes fraud detection, risk management, and accountability mechanisms. EWS launched Zelle without one, and as a result, account holders lost hundreds of millions of dollars.

Supervision and enforcement prompt companies to make their services safer.

Enforcement actions of the kind brought against EWS require years of investigation, development of legal theories, and ongoing engagement. It is therefore significant that Zelle introduced Zelle Risk Insights (ZRI) in the summer of 2023, during the period when the CFPB's scrutiny of the network was advancing. From a regulatory lens, this outcome is not incidental. It reflects the direct relationship between unsafe product design and unfair consumer outcomes. The Zelle experience demonstrates that supervision and enforcement are not bureaucratic formalities. They are the forces that compel companies to build safer products and bear responsibility when they do not.

[15] Consumer Financial Protection Bureau. (2024). CFPB v. Early Warning Services, LLC; Bank of America, N.A.; JPMorgan Chase, NA.; and Wells Fargo Bank, N.A. [Complaint for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment and Other Relief]. https://files.consumerfinance.gov/f/documents/cfpb_Zelle-Complaint_2024-12.pdf

ZRI advanced Zelle from a simple messaging system to a risk-sensitive platform. For the first time, network rules held participating banks accountable for using fraud-detection information. It created systems for flagging high-risk accounts, additional identity-verification overlays, and a new impostor-scam refund system.

These are all positive changes – but they cannot be evaluated in isolation from the regulatory context in which they were made. The evidence strongly suggests that these improvements were a direct response to the CFPB's supervision and enforcement work, rather than to a voluntary industry initiative.

If the CFPB's investigation into Zelle drove EWS to make reforms, it would not be the first instance where enforcement led to better outcomes for consumers in the broader market. During the last administration, the CFPB and prudential regulators cracked down on aggressive bank overdraft and non-sufficient funds (NSF) fee harvesting. The CFPB completed enforcement actions against banks in 2017, 2020, 2022, 2023, and 2025.[16] During this time, many banks began to reform their policies. By 2024, the CFPB's work had led to proactive savings of $4 billion per year in overdraft and NSF fees that might have otherwise been paid.

For policymakers, developments in overdraft and faster payment markets that arose from investigations should demonstrate why the goal of a safe financial ecosystem hinges on a strong financial regulator to oversee markets, conduct investigations, and enforce consumer protection.

Congress should pass legislation restoring the CFPB's ability to supervise non-bank payment apps and digital wallets.

Crypto kiosks are a dangerous vector for scams.

There are now over 30,000 crypto kiosks across the United States. Without state intervention, these kiosks lack consumer protection. In 2024, the FBI received almost 11,000 complaints about crypto kiosks, resulting in nearly $250 million in losses. Adults over the age of 60 suffered approximately 85 percent of those losses.[17] Losses increased tenfold between 2020 and 2023.[18] Since a very high share of scam losses are never reported, these numbers reflect only a fraction of total harm.[19] CFA supports legislation to curb the abusive practices of crypto ATMs:

- Set mandatory daily transaction limits
- Limit fees to $5 per transaction of 15 percent, whichever is lower.
- Require paper receipts for all transactions
- Post clear, visible scam warnings at every kiosk
- Require mandatory holds on transfers to allow time to reverse fraudulent or coerced payments.

---

[16] Consumer Financial Protection Bureau. (2024, September 17). CFPB Takes Action to Stop Banks from Harvesting Overdraft Fees Without Consumers' Consent. https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-stop-banks-from-harvesting-overdraft-fees-without-consumers-consent/

[17] AARP. (2026, January 28). AARP Backs Legislative Action to Stop Crypto Kiosk Scams. https://www.aarp.org/states/washington/aarp-backs-legislative-action-to-stop-crypto-kiosk-scams/

[18] Federal Trade Commission. (2024). Bitcoin ATMs: A payment portal for scammers [Data Spotlight]. https://www.ftc.gov/system/files/ftc_gov/pdf/bitcoin_atms_spotlight.pdf

[19] Anderson, K. B. (2021). To Whom Do Victims of Mass-Market Consumer Fraud Complain? (SSRN Scholarly Paper No. 3852323). Social Science Research Network. https://doi.org/10.2139/ssrn.3852323

- Subject all kiosk operators to state licensure.

By early 2026, seventeen states had passed laws regulating crypto kiosks. In announcing a lawsuit against a crypto kiosk operator, District of Columbia Attorney General Brian L. Schwalb revealed that the agency's investigation found 93 percent of the company's transactions were fraudulent.[20]

These measures will protect consumers from scams. They will also suppress the use of crypto kiosks for illicit finance.

Policymakers should strengthen the connections between consumer protection agencies and those fighting illicit finance.

A critical gap exists in how Bank Secrecy Act (BSA) enforcement has traditionally been conceptualized in light of emerging large-scale international scam operations. Even when regulators identify failures to prevent illicit finance, the resulting enforcement actions largely overlook the direct harms experienced by consumer victims. BSA compliance has focused on stopping money laundering, terrorist financing, human trafficking, drug sales, and international government corruption. No one argues that those are essential purposes. When illicit finance flourishes, it harms people in tragic ways.

But the organizations investigated for illicit financial crimes have now opened a new line of business: scamming regular people. In several Southeast Asian countries, scams fund a large share of national economic activity.[21] There is a consistent overlap in which scams are one component of criminal operational portfolios.[22]

FinCEN has itself signaled that this broader view is warranted. In its 2021 Anti-Money Laundering and Countering the Finance of Terrorism (AML/CFT) National Priorities report, FinCEN listed fraud as one of eight national priorities. In listing fraud, it made clear that the term encompassed common scam tactics: impostor schemes, confidence fraud, employment scams, and related methods.

> *"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."*[23]

And, critically, it attributed the work to the same organized criminal networks engaged in other transnational crimes. The activities FinCEN identified, and the flow of funds associated with them to US

---

[20] Attorney General Brian L. Schwalb. (2025, September 8). Attorney General Schwalb Sues Crypto ATM Operator for Financially Exploiting District Residents. https://oag.dc.gov/release/attorney-general-schwalb-sues-crypto-atm-operator

[21] 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

[22] 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/68264cff356caba111f2db1e_Policies%

[23] FinCEN. (2021, June 30). Anti-Money Laundering and Countering the Financing of Terrorism National Priorities. https://www.fincen.gov/system/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

depositories and money transmitters, are precisely the actions that call for closer ties between consumer protection agencies and those charged with stopping illicit finance.

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

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.[24]

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: FinCEN 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.[25]

Scams are sometimes the first step in subsequent money laundering activities. Often, funds received through scams are transferred to other accounts via money mules.[26] These are funnel accounts.

Preventing account takeover is a critical challenge. FinCEN reported that most elder scam-related filings referenced account takeovers.[27]

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.[28] 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.

---

[24] 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

[25] 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

[26] 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

[27] 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

[28] Ibid

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.[29]

The fraud/scam distinction in EFTA and Reg E must be reevaluated

The liability framework for scams requires fundamental reform. At the heart of the problem is an outdated legal distinction embedded in the Electronic Fund Transfer Act (EFTA) and its implementing rule, Regulation E. Under current law, consumers are protected when funds are taken from their accounts without their consent. However, consumers receive no equivalent protection when they are deceived or coerced into initiating a transfer themselves. Because the account holder technically authorized the payment, these transactions are classified as "scams" and fall outside existing consumer protections.

This distinction, once perhaps administratively coherent, has become increasingly disconnected from the reality of modern criminal tactics. Sophisticated fraud schemes routinely manipulate victims into authorizing payments under false pretenses. The resulting transfers are "authorized" only in form.

The methods by which criminals conduct fraud and scams have evolved since the 1970s. When the EFTA was passed in 1978, virtually all electronic funds theft involved stolen automated teller machine (ATM) cards or compromised personal identification numbers (PINs). At this time, almost all losses were due to unauthorized transfers. When the Federal Reserve issued Regulation E to implement EFTA in 1979, it defined an unauthorized payment as one initiated by someone other than the consumer. They focused on the critical risks of the time – stolen PINs and lost or stolen ATM cards.

In 1981, the Federal Reserve introduced a new wrinkle: transfers initiated by the account holder are considered unauthorized payments if the consumer is “conned or forced to furnish another person with an access device for use in an ATM.”[30] A few months later, the commentary was updated to state that when a consumer is “induced by fraud to furnish another person with an access device” to make an ATM withdrawal, the payment is also unauthorized. Fed staff reasoned that criminals might force people to withdraw funds at ATMs. In 1983, this example was provided in a staff commentary.[31]

These commentaries are the first instances in which regulators acknowledged that criminals might coerce consumers to initiate an EFT. Congress’s conclusion in 1981—that electronic funds transfers made through inducement are also unauthorized—shows that today’s inducement schemes also deserve reclassification as unauthorized payments.

Any durable legislative or regulatory solution must eliminate this distinction and extend meaningful protections to consumers who are induced through deception or coercion to send funds, regardless of whether the account holder technically initiated the payment.

---

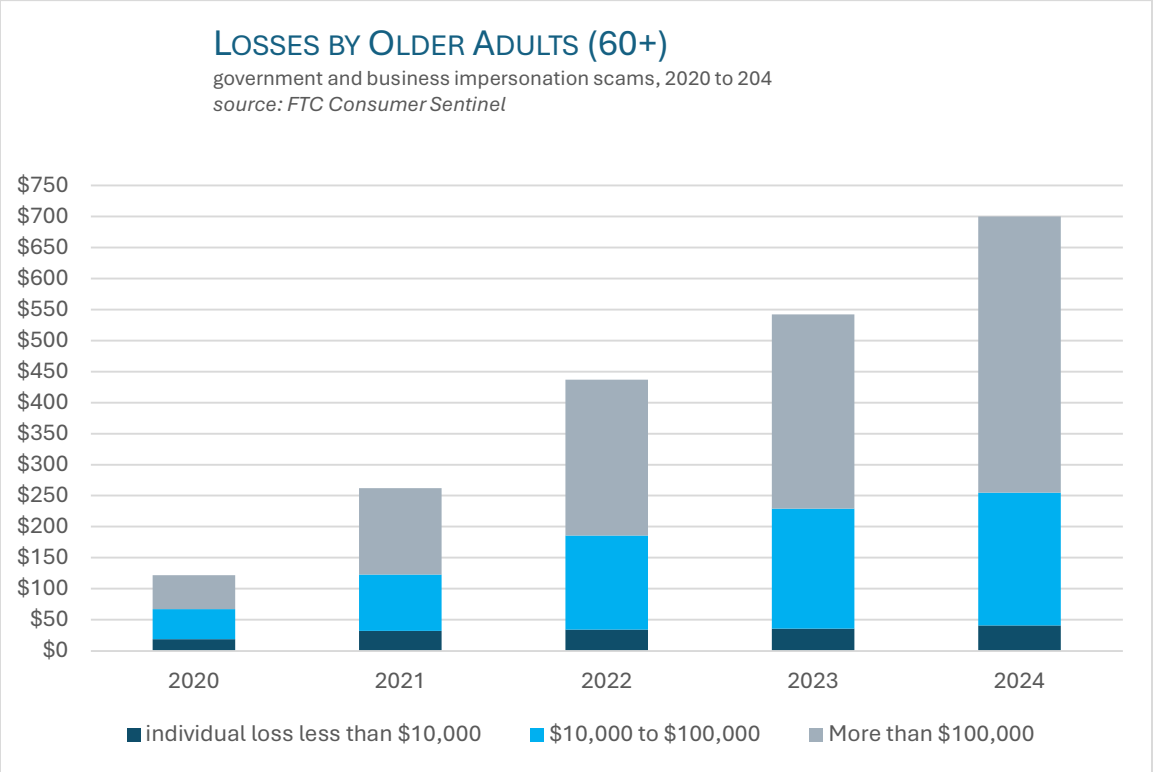
[29] Ibid

[30] Technical Amendments and Official Staff Commentary Update, 48 Fed. Reg. 4667, 4668 (Feb. 2, 1983).

[31] Official Staff Commentary Update, 50 Fed. Reg. 13180, 13181 (April 3, 1985) ("Q 2-28: Unauthorized transfers – forced initiation. A consumer is forced by a robber (at gunpoint, for example) to withdraw cash at an ATM. Do the liability limits for unauthorized transfers apply? A. Yes. The transfer is unauthorized for purposes of Regulation E. Under these circumstances, the actions of the robber are tantamount to the use of a stolen access device.").

Scams harm some of our most vulnerable populations

The rise in scams disproportionately affects seniors. High-loss scams start with similar narratives: someone is using your account, your information is being used to commit crimes, or there is a security problem with your computer. They end tragically. According to a recent FTC report, the number of older adults who lost more than $10,000 in a scam increased fourfold from 2020 to 2024. Losses of more than $100,000 increased sevenfold, and total sums lost increased eightfold.[32]



The criminal coerces the victim to authorize a payment, a significant problem for existing laws, as authorized funds transfers fall outside of EFTA protections.

Owing to their use of smartphones, young people are more likely to fall prey to sextortion schemes. The National Center for Missing & Exploited Children (NCMED) said that an overwhelming share of cases are initiated online, most often through Instagram and Snapchat. The number of reports jumped dramatically during the pandemic. NCMEC says it receives more than 1,000 reports per week.[33]

As well, servicemembers are vulnerable to scams. During a permanent change of duty station, service members must find new housing. While junior personnel may be relocated to a new barracks room, others will need to secure a private residence. When relocating, service members rely on payment apps at rates

[32] Division of Consumer Response and Operations Staff. (2025). False alarm, real scam: How scammers are stealing older adults' life savings. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings

[33] National Center for Missing and Exploited Children & Thorn. (2024). *Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data*. https://www.thorn.org/research/library/financial-sextortion/

far more frequently than civilians. As a result, criminals are now targeting service member accounts. To make matters worse, some payment apps limit customer service hours, making it harder for servicemembers stationed overseas in different time zones to resolve problems. The number of complaints filed by servicemembers about payment apps has increased steadily in the last few years, and many have been related to fraud and scams using payment apps.[34] Service members report being unable to access funds when their accounts are frozen.[35]

Expand EFTA to include protections for consumers who are scammed into sending wire transfers.
While wires are the preferred payment rail for corporations making large-value transfers, they are still used by consumers on occasion. Moreover, wires are often used in some of the largest scams perpetrated against regular people, such as investment scams resulting in losses of hundreds of thousands of dollars.

Wire transfers are classified as out of scope of EFTA.[36] Instead, the Uniform Commercial Code Article 4A governs wire transfers. Article 4a absolves banks of liability as long as they followed "commercially reasonable security procedures," even if the sending customer was scammed.

Through staff commentaries, the Federal Reserve has concluded that EFTA and its implementing regulations do not apply to funds transferred through Fedwire. However, in 2024, the CFPB filed a statement of interest in New York v. Citibank, N.A., making the point that EFTA should apply to wires sent by consumers.

Share liability between sending and receiving financial institutions
Policymakers must apply liability to the "bank of the criminal" and the "payment app of the criminal."

Regardless of the narrative employed and the method used to contact the victim, scammers must have a place to receive funds. While cryptocurrency and Bitcoin ATMs are emerging as popular tools for this purpose, criminals still need to use depositories and payment apps. As long as consumers place their funds in either, scammers will need accounts inside them.
Scammers can gain access to an account in one of three ways: by applying for one directly, typically using a synthetic identity; by taking over an account; or by using a money mule to move funds on their behalf. In each case, the FI is the first line of defense against scams. Once they have gained a foothold, scammers use the account to receive proceeds from scams and then move those dollars to another location.

Most often, they search for and target FIs with weak fraud detection systems. For example, they may see that a bank has only recently introduced online or app-based banking services. Criminals share information, so they may quickly flood an FI with applications after the first successful compromise. The

---

[34] *CFPB Report Identifies Issues with Increased Servicemember Use of Digital Payment Apps*. (2023, June 20). Consumer Financial Protection Bureau. https://www.consumerfinance.gov/about-us/newsroom/cfpb-report-identifies-issues-with-increased-servicemember-use-of-digital-payment-apps/

[35] Consumer Financial Protection Bureau. (2022, November 11). *Consumer Complaint Database* [Consumer Complaint, Scam]. https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/6190058

[36] 15 U.S.C. § 1693a(7)(B)

FI's failure to reject fraudulent applications, prevent account takeovers, and monitor accounts for suspicious activity is not a peripheral compliance lapse. It is the condition that makes a scam possible. Weak customer due diligence (CDD) controls directly enable consumer harm.

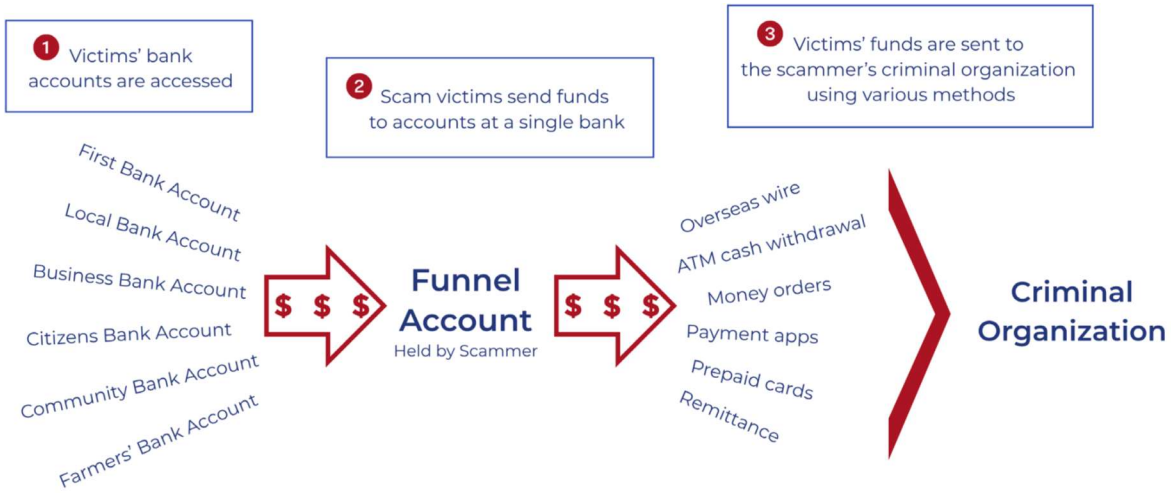
The dynamic places receiving FIs at a critical place in the scam chain. The "FI of the criminal" has a unique line of sight into suspicious behavior. They should know who holds the account and its declared uses. As such, they are better situated to see suspicious activity than senders. The tools required to conduct these reviews need not be developed in-house. They are widely available through contracts with third-party vendors.

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

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 scam funds from multiple sending banks.

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.[37] In the first six months of 2025, nearly 8 percent of bank account applications were made using synthetic identities.[38] 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.[39]



[37] 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/

[38] 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

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

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.

To force investment across the entire payment ecosystem, incentives should be put in place to increase financial institutions' motives to identify and pause suspicious activity.

Policy approaches that call for shared liability are sensible and would be effective. Returning to the case of ZRI, one of the critical elements of its update was the requirement that participating institutions contribute to and use shared fraud-detection information.

In fact, it is not unreasonable to see a future in which the distinguishing features of payment channels are security, speed, and cost. Chartered financial institutions and state-licensed money transmitters will face new competition from blockchain-based settlement, driven forward by agentic AI shopping. The cost of routing a transaction through a Layer 2 blockchain could be very low, nearly immediate on a 24-7 basis, and also very risky. At the moment, it appears that most bank-routed transactions will settle more slowly and at a greater cost.

Shared liability will place greater scrutiny on KYC-lite practices, including those involving bank-fintech partnerships.

All financial institutions face a tension in attracting new accounts. The imperative to grow, along with the desire to see returns on marketing costs, makes it imperative to minimize "friction" in processes for opening new deposit and loan accounts. Each new data point in an application form inevitably leads to more abandonments and fewer completions.[40] Compliance risks push in the opposite direction, requiring FIs to collect more information to verify customer identity. Together, these pressures act in conflict. Too often, some FIs succumb to the temptation to perform "KYC-lite."

This tension is particularly acute in the fintech sector. In the last six years, prudential regulators have issued enforcement actions and settlements with a high share of partner banks.[41] In 2023, enforcement actions were issued to Cross River Bank, Metropolitan Commercial Bank, Vast Bank, B2 Bank, First Fed Bank, and Choice Financial Group. Blue Ridge Bank, Lineage Bank, Sutton Bank, Piermont Bank, and Evolve Bank & Trust received orders in 2024.[42] Most involved AML compliance failures.

For a number of reasons, fintech accounts are in the crosshairs of criminals. Not least, they operate exclusively online and are frequently very new. But fintech companies also bring healthy risk appetites to the table. These companies, and especially early-stage firms operating under pressure from impatient

---

[40] 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/

[41] 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

[42] Son, H. (2024, July 2). How thousands of Americans got caught in fintech's false promise and lost access to bank accounts. CNBC. https://www.cnbc.com/2024/07/02/synapse-fintech-fdic-false-promise.html

investors, have strong financial incentives to minimize friction. In turn, partner banks face corresponding incentives. To attract business from fintechs, they may feel competitive pressure with competitor partner banks to offer streamlined compliance standards.

Federal interagency guidance on third-party risk is clear and unambiguous: banks are responsible to ensure their non-bank partners follow the rules.[43]

Unfortunately, too large a share of bank activity now occurs outside the banking perimeter. While some banks have BaaS programs inside their bank holding companies, other banking-as-a-service (BaaS) firms operate outside prudential supervision. Independent banking-as-a-service (BaaS) companies must face greater regulatory scrutiny.

The failures at Synapse, an independent BaaS firm, illustrate the problem. Working in conjunction with a roster of consumer and small business fintechs and four bank partners, Synapse failed to properly ledger consumer account balances. Following the company's bankruptcy, a court-appointed trustee estimated that between $65 and $96 million in customer funds were unaccounted for, affecting more than 100,000 consumers.[44] These funds were owed to consumers at a variety of fintech apps, but neither Synapse nor its bank partners could ascertain the exact amounts due to each depositor.

Evolve Bank & Trust was also central to the failures at Synapse. A partner bank to fintechs, Evolve 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.

Evolve approved these accounts through its partnership with Mercury, a fintech company serving businesses. 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.

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.[45]

---

[43] 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/

[44] Penny Crosman. (2025, August 8). CFPB to hold Synapse responsible for missing customer funds. American Banker. https://www.americanbanker.com/news/cfpb-to-hold-synapse-responsible-for-missing-customer-funds

[45] Ibid

The prudential regulators should apply their authority under the Bank Service Company Act to supervise independent BaaS firms. Some contend that this power is underutilized.[46] The Synapse event should add urgency among prudential regulators to strengthen its use.

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.[47]

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.[48] While it will not have uniform effects – as it will only aid victims of the most significant failures – it moves in the right direction.

When the UK Payment System Regulator implemented a new code requiring shared liability for scams, the number of complaints fell.

Accountability is essential to making our payment systems safer. This principle must be applied across the payment journey. Currently, consumer protection focuses primarily on the financial institution that sends funds. Bank and non-bank senders must have responsibility, but so should the institutions on the other side of the payment as well.

---

[46] 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

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

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

Other countries have moved forward with updating protections against induced fraud. In October 2024, the United Kingdom's (UK) Payment Systems Regulator implemented the Contingent Reimbursement Model to hold banks and building societies accountable when criminals trick account holders into sending funds. Most cases result in reimbursements under a framework where Originating Depository Financial Institutions (ODFIs) and Receiving Depository Financial Institutions (RDFIs) share liability.[49]

The onset of this new policy has been a success. Notably, it did not provoke a surge in unjustified fraud claims by people posing as victims. In 2023, UK consumers filed 56,000 scam ("authorized push payment") per quarter on average. In the first three months after the CRM's introduction, the number of scam complaints fell by almost 18 percent, to 46,000.[50] The UK's latest report, covering the first two quarters of 2025, continues to show a decline in confirmed cases.[51]

Pass legislation to provide protection for victims of scams, expand liability to receiving institutions, and take steps to ensure the CFPB can hold financial companies accountable.

Just as it is important to involve government across agencies, it is also important to compel action from financial institutions across the payment journey.

At each stage of the payment journey, institutions face challenges in preventing scams. For sending-side institutions, it may be challenging to overcome an account holder's desire to send funds to a scammer. For a receiving institution, deploying the technology needed to thwart application and account takeovers (ATOs) by criminals will require vigilance and expense. The networks that serve as connectors, which may also control directories, may not understand activities occurring outside of their systems.

Nonetheless, all of these actors can play an important role in sharing information and flagging suspicious activity. These facts are relevant for depositories and non-banks alike.

For this reason, it would be a critical error to absolve any institution of responsibility for a transfer that results in a scam event. Proposals to exempt depositories or non-banks from liability, on either side of a payment order, will disincentivize investment in scam prevention.

For this reason, CFA supports the *Protecting Consumers from Payment Scams Act*. This act will ensure that losses resulting from fraudulent inducement will receive the same level of protection as funds lost from an unauthorized electronic transfer.

Additionally, the Act wisely shares liability between sending and receiving institutions. In doing so, it follows the lead from the United Kingdom, where the introduction of shared liability led to fewer scams.

---

[49] UK Payment Systems Regulator. "Fighting Authorised Push Payment Fraud: A New Reimbursement Requirement." Policy Statement. Response to Consultation, June 2023. https://www.psr.org.uk/media/iolpbw0u/ps23-3-app-fraud-reimbursement-policy-statement-final-june-2023.pdf.

[50] David Geale. (2025). The story so far: A snapshot of what we've seen since our APP scams reimbursement requirement went live [News and Updates Thought Pieces]. UK Payment Systems Regulator. https://www.psr.org.uk/news-and-updates/thought-pieces/thought-pieces/the-story-so-far-a-snapshot-of-what-we-ve-seen-since-our-app-scams-reimbursement-requirement-went-live/

[51] UK Finance. (2025). Half-Year Fraud Report 2025. https://www.ukfinance.org.uk/system/files/2025-10/Half%20Year%20Fraud%20Report%202025_0.pdf

And further, the Act expands protections for consumers who lose money to scams in which they agree to wire funds. Some banks have now programmed their apps to process wire transfers, and at a discount compared to ordering a wire at a branch. These policies contradict depositories' claims that they strive to prevent their customers from paying criminals in scams.

Also, the Act includes in the definition of an "error" the mistakes made by consumer senders when they are tricked by a criminal. This step will ensure that consumers can seek resolution and recover funds through established processes for unauthorized transfers.

Lastly, to ensure that regulators have the authority they need to address current and future challenges, the Act empowers the CFPB to issue new rules to enforce the Act's provisions.

Social media platforms and telecoms are weak points in systemic defense against scams.
A significant share of scam activity originates from social media platforms.[52] Many scammers contact people through their smartphones. Both systems connect directly to the payment system. Meta has projected that over 10 percent of its 2024 sales revenue came from scammers who purchased ads to attract victims or sell false goods.[53]

Some countries have passed laws holding telecommunications companies and social media platforms accountable for scams conducted on their platforms.

For the moment, methods to address these scam gateways are voluntary and not consistent. JPMorgan Chase has introduced a system that warns account holders when it detects that a Zelle purchase request originated from a social media channel.[54] However, Chase is an exception.

Policymakers should revise rules that protect platforms from scam activity.

Moreover, it appears that sharing liability had beneficial effects on the resilience of the payment ecosystem as a whole. Elsewhere, shared liability policies have gone further to hold other actors involved in the chain of scams responsible. In Singapore, telcos share some liability in cases where their breaches result in fraud losses.[55] In Australia, financial institutions have liability, but accountability has also been extended to telcos and digital platforms. Telcos must block SMS messages with phishing links, monitor their systems for suspicious activities, and conduct investigations to block scam calls. Digital platforms must enhance identity verification for new accounts, freeze suspected scam accounts, prevent scammers from advertising, and remove content when necessary.[56]

In the United States, the bipartisan *Safeguarding Consumers from Advertising Misconduct Act* would hold social media platforms accountable to apply some of the same policies to digital platforms as those

---

[52] Au-Yeung, J. H. and A. (2025, May 15). Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook. Wall Street Journal. https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8

[53] Vanian, J. (2025, November 6). Meta reportedly projected 10% of 2024 sales came from scam, fraud ads. CNBC. https://www.cnbc.com/2025/11/06/meta-reportedly-projected-10percent-of-2024-sales-came-from-scam-fraud-ads.html

[54] Chase. (n.d.). Help Protect Yourself From Social Media Scams. Privacy and Security. Retrieved March 1, 2026, from https://www.chase.com/digital/resources/privacy-security/security/social-media-scams

[55] Neira Jones. (n.d.). No Weak Links: The Case for Shared Liability in Fraud and Scam Prevention. BioCatch. Retrieved March 1, 2026, from https://www.biocatch.com/blog/case-for-shared-liability-fraud-prevention

[56] Australian Government Treasury. (2025). Scams Prevention Framework – Protecting Australians from scams. https://treasury.gov.au/sites/default/files/2025-01/p2025-623966.pdf

already adopted in Australia. This law would dramatically strengthen defenses against purchase scams. This Act is a step in the right direction, but financial institutions and consumers need stronger action from Congress.

To increase safety and enable faster payments, regulators should update EFAA to allow receiving FIs to delay account crediting when they detect suspicious activity.

The virtue of real-time gross settlement is also the source of its risk. Because of speed and irrevocability, a faster payment service provides an attractive opportunity to a fraudster. While most other payment methods can be canceled, a faster payment is completed in seconds, and the payee may withdraw it as soon as it is received.[57] Once a consumer discovers they sent the funds to the wrong recipient, it is too late to cancel the order. The scammer's financial institution will have accepted the funds and credited them to the account holder's account. The account holder may even have transferred them to another account at a different financial institution. If funds settled at the speed of a batched ACH transfer—a same-day or the traditional multi-day version—the same vulnerability would not exist because there would be time for a payment order to be canceled.

Effective solutions can be applied to improve defenses. With an application programming interface (API) call, a sending bank can request the receiving bank to check if the receiving account has any of the suspicious factors listed earlier. These "accept/reject" requests are standard technology now. In almost all cases, the time between the request and the response is less than five seconds. Usually, response times are under 1 second.

They can also create analytics to flag suspicious transfers – even if the account is new. For example, if the note in a payment memo line reads "for a puppy," there is a logical reason to reject the transfer. By some accounts, fake puppy scams make up almost one-fourth of all online purchase scams.[58] Similarly, if information gleaned through an application suggests that an account will only be funded twice per month and solely through a direct deposit, it should raise flags when it immediately begins to receive many non-payroll deposits. These are practical, empirically-proven, common-sense approaches.

But in cases where near-real-time analytics flag concerns about scams or fraud, the FI needs to be able to delay account crediting.

To further enhance the ability for FIs to apply their fraud detection systems to help scam victims, the Expedited Funds Availability Act and Regulation CC should be updated to specify that FIs can delay crediting an account when they see suspicious activity.

This clarity would not alter consumers' important rights to challenge account freezes or closures. A consumer should be able to contest a bank's decision to freeze or close their account. When a consumer attempts to access the funds but is denied access, the action should be treated as an error. With that protection, a consumer would receive their necessary error-resolution rights, and the bank would be held

---

[57] Federal Reserve. "Fraud and Instant Payments: The Basics." *Instant Payments Education* (blog), 2024. https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html.

[58] Better Business Bureau. "BBB Study Update: Average Losses in Puppy Scams Rising, Even as Cases Fall." *Latest News* (blog), December 6, 2022. https://www.bbb.org/article/investigations/27895-bbb-study-update-average-losses-in-puppy-scams-rising-even-as-cases-fall. As an aside, French bulldogs, Yorkies, and Dachshunds are especially risky, leading to almost one-third of puppy scams.

to the investigation standards set out in the EFTA.[59] Once the consumer filed a complaint with the bank about a denied transaction, the institution would have to investigate the payment, and if it could not provide a resolution within 10 days, release the frozen funds or reopen the closed account. In essence, it is possible to balance consumer protections with priorities for scam detection.

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.

Giving this flexibility to receiving FIs would advance the adoption of faster payments. While many depositories now participate in a faster payments system, many are "receive-only." Institutions choose not to send funds because of a perceived risk that some recipients lack adequate safeguards to detect scam activity.[60] Those receive-only FIs believe that sending an irrevocable real-time payment could put their customers at risk of scams.

Digital identification systems must observe critical privacy safeguards.

Proposed bipartisan legislation would provide support for states to consider plans for mobile digital identification. By creating a tokenized system for data sharing with strong user-determined permissioning, customers and their FIs would have a powerful tool to verify the identities of recipients of fund transfers.

Fundamentally, any system for tokenizing digital identification must also protect consumers from government surveillance. The use of such a tool must be at the consumer's discretion, not conditioned by other factors, and revocable. There are genuine concerns about "phone home" capabilities embedded in digital state-issued identification that would undermine personal privacy.[61] Unfortunately, the federal government is currently instituting practices that compromise consumer privacy rights to a degree never before seen. For this reason, it makes sense to address aggressive privacy invasions by federal law enforcement first, before operationalizing government-issued digital identification. The American public should not have to choose between a system that makes their PII vulnerable to scammers or one that permits intrusive government surveillance.

SARs are an essential tool for identifying suspicious activities. Rather than reduce the number of filings, policymakers should seek ways to improve their utility for law enforcement and consumer protection agencies.

While some policymakers would like to raise the thresholds for filing SARs, meaningful reform will require leaders to look beyond reducing SAR filing volume and instead consider how to make data-sharing regimes more effective. Indeed, if policy focuses on the narrow goal of reducing the number of SARs filed, then policymakers may handicap one of the best tools available to financial companies and

[59] 12 CFR 1005.11(c)(1).

[60] John Adams. (2024, February 1). Why aren't more banks sending real-time payments? American Banker. https://www.americanbanker.com/payments/news/why-arent-more-banks-sending-real-time-payments

[61] Jay Stanley. (2025, June 2). Digital Identity Leaders and Privacy Experts Sound the Alarm on Invasive ID Systems. American Civil Liberties Union. https://www.aclu.org/press-releases/digital-identity-leaders-and-privacy-experts-sound-the-alarm-on-invasive-id-systems

regulators to prevent fraud and scams.[62] It's the actionability of the data in the SAR, and the utility of systems to support law enforcement activities efficiently, that must be addressed.

The key question, from the perspective of providing relief to scam victims, is how to improve reporting to better highlight the activity affecting regular people. If data collected from SARs can help law enforcement agencies (LEAs) better analyze scam trends, it will improve scam detection and prevention and support ongoing investigations. This is an efficient step to put existing resources to use for additional problems.

LEAs can access SARs through the FinCEN web portal. With the portal, they can query data by using FinCEN Query or download data in bulk to run on separate systems. LE agencies must apply for access to the FinCEN portal. If FinCEN approves the request, it executes a memorandum of understanding (MOU) with the agency. Last month, the Office of the Inspector General reported that FinCEN had approximately 450 active MOUs with external agencies and 14,000 external users.[63]

The ability to obtain bulk data is critical for any user seeking to apply SARs to analytical platforms. Once uploaded, platforms can conduct data mining and other analyses to permit greater utilization of SARs. But those LEAs face hurdles because uploading is time-intensive. Many key data points are buried in narratives, requiring costly machine-learning techniques to extract them. An updated SAR form could require the critical fields in a structured format, reducing burdens on both private institutions and LEAs.

SARs can become the signals that connect filings across accounts and institutions lead to new cases. But SARs themselves are not legal evidence. LEAs use SARs, in part, as tips on where to issue subpoenas. As the Chief of the IRS's Criminal Investigation unit recently wrote, "BSA data is often the first signal that something isn't right. These filings become essential puzzle pieces in identifying patterns, following financial trails, and building cases that protect taxpayers." The IRS conducted 3.9 million searches of BSA filings in 2025. That data was the basis of a new investigation in more than 2 of every 3 instances. The same report noted that SARs were used to initiate cases under 12% of the time, but SARs were queried on targets in over 80% of their cases, suggesting connected activity is a critical area done well.[64]

For this reason, it is important for policymakers to consider ways to reshape how SARs data is collected, stored, and shared.

Migrate data from unstructured "narratives" to structured formats. Some of the most useful information is filed in non-structured data fields. Filers use these sections to explain details that are not easily conveyed elsewhere in the form. To their credit, the narratives often contain valuable descriptions of activity. Often, filers put the most useful information in the narrative section. Nonetheless, for analysts seeking to identify trends from large numbers of filings, information stored in non-structured fields is

---

[62] Kelly Phillips Erb. (2026, February 27). Following The Money: How Financial Data Helps Solve IRS Criminal Cases. Forbes. https://www.forbes.com/sites/kellyphillipserb/2026/02/27/following-the-money-how-financial-data-helps-solve-irs-criminal-cases/

[63] Office of the Inspector General of the Department of the Treasury. (2026). Audit of FinCEN's Management of BSA Data—User Access and System of Records Notice (OIG-26-015). https://oig.treasury.gov/system/files/2026-02/Audit-of-FinCEN%27s-Management-of-BSA-Data---User-Access-and-SORN-%28OIG-26-015%29---SECURED.pdf

[64] Internal Revenue Service. (2026, February 24). *IRS-CI data shows BSA filings are used in nearly all its investigations*. Press Release. https://www.irs.gov/compliance/criminal-investigation/irs-ci-data-shows-bsa-filings-are-used-in-nearly-all-its-investigations

hard to use. Unfortunately, this information is difficult to access because it is not in a structured, searchable format. With better structure, law enforcement can more effectively use existing data.

SARs should have a clear identifier for activity involving scams.

Policymakers should design data collection to help LEAs see scam activity. With a simple "check box" to identify a scam event, consumer protection agencies could rapidly search SARs to identify scam victims. The inclusion of the box would help LEAs and lead to better outcomes for victims. Already, systems like FedNow's FraudClassifier and ScamClassifier capture useful data on fraud and scam transactions. Relatedly, SARs should include contact information for scam victims to facilitate LEAs and consumer protection agencies' ability to help victims and potentially provide remedies.

Do not raise thresholds for currency transaction reports (CTRs).

Notably, the IRS reports that the median size of a CTR used in a 2025 investigation was $12,543, underscoring the importance of not raising filing thresholds.[65]

It is also the case that raising thresholds would close off the line of sight for LEAs to some categories of scams. For example, most transactions in teen sextortion cases are for only a few hundred dollars. The most common payment types in these events were, in order: gift cards 25.6%, PayPal 17.8%, Venmo 9.4%, Zelle 7.5%, Apple Pay 4.8%, and cryptocurrency at 2.9%.[66] Laws curb teens' access to traditional bank accounts, but there are still loopholes, such as gift cards, teen accounts, and accounts held by parents. Teens authorize transfers under coercion that criminals will distribute explicit images.[67] Criminals on the dark web are not seeking to raise thresholds for information sharing. Our law enforcement agencies should not raise them, either.

Clarify to banks that they can release bank account information to law enforcement agencies. For their investigations, LEAs need to know where the money was sent. It is essential to include the routing and account numbers for destination (funnel) accounts. This privilege does not infringe the privacy rights of victims who sent funds, unlike if an FI released this data to a private individual. With this information, LEAs will have more resources to track patterns. Again, it is important to identify the vulnerabilities in the payment ecosystem, starting with the "bank of the criminal." Anecdotally, some banks appear to believe they cannot release this information. Regulatory clarity is needed. Otherwise, LE needs to issue a subpoena to the SAR filer, wasting precious time.

Conclusion

Financial fraud and scams are among the most serious and rapidly evolving threats to American consumers. The stakes could not be higher. Reported losses now exceed $12.5 billion annually, and the true toll is far greater. Seniors are losing their life savings. Service members stationed overseas cannot access frozen funds. Teenagers are being extorted. And the criminal organizations behind these schemes

[65] Ibid

[66] Jimenez, A. (2024, November 21). Teen Sextortion Victim Payments. Dynamic Securities Analytics, Inc. https://securitiesanalytics.com/teen-sextortion-victim-payments/

[67] ibid

are growing more sophisticated, better resourced, and increasingly intertwined with broader networks of transnational illicit finance.

The good news is that the tools to fight back exist. Supervision works. Enforcement works. Shared liability works. The evidence from Zelle's belated safety improvements, from the reduction in overdraft fee harvesting, and from the United Kingdom's successful implementation of the Contingent Reimbursement Model all point to the same conclusion: when regulators hold institutions accountable, the financial system becomes safer for everyone.

But sadly, in the last year, policy has had the opposite effect. By sidelining the CFPB and preventing it from supervising payment apps and digital wallets, the Administration and Congress have reduced our defenses against scams.

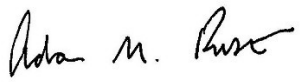
The Consumer Federation of America urges Congress to take the following actions:

- Restore the CFPB's funding to the 12 percent cap established in the Dodd-Frank Act and reverse the dismantling of the agency's supervision and enforcement capacity.
- Reestablish the CFPB's authority to supervise non-bank payment apps and digital wallets, including products that facilitate digital asset transfers.
- Pass the Protecting Consumers from Payment Scams Act to extend EFTA protections to consumers induced through deception or coercion, share liability between sending and receiving financial institutions, and expand coverage to wire transfers.
- Support regulation of crypto kiosks, including transaction limits, mandatory holds, fee caps, and scam warnings.
- Pass the Safeguarding Consumers from Advertising Misconduct Act to hold social media platforms and telcos accountable for their roles in facilitating fraud and scams.
- Improve the structure and utility of SARs so that law enforcement and consumer protection agencies can more effectively identify scam victims, track criminal networks, and build cases.
- Resist efforts to raise CTR thresholds, which would blind regulators to the low-dollar transactions that characterize many of the most harmful scams.
- Advance legislation to hold social media platforms and telecommunications companies accountable for the role their networks play in facilitating scam activity.
- Update the Electronic Funds Availability Act and Regulation CC to give receiving financial institutions the flexibility to delay account crediting when they detect suspicious activity, without diminishing consumers' core rights to challenge such actions.

The costs of inaction are not abstract. Every month that passes without meaningful reform is another month in which criminal organizations operate with impunity, consumers lose money they cannot recover, and financial institutions face little incentive to invest in prevention. The legal framework governing electronic payments was designed for a world that no longer exists. Congress has both the authority and the responsibility to bring it into the present.

It is time to advance reforms that protect American consumers, strengthen the integrity of our payment systems, and ensure that those who profit from moving money bear a fair share of the responsibility for doing so safely.

Sincerely,



Adam Rust
Director of Financial Services
Consumer Federation of America
arust@consumerfed.org