
Testimony of Patrick McDade

Senior Vice President, Fraud Risk and Technology Risk Management,
Head of Internal Investigations

EverBank N.A.

U.S. House Financial Services Committee

Financial Institutions Subcommittee

Hearing Entitled “Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions”

March 5, 2026

Chairman Barr, Ranking Member Foster, and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Patrick McDade, and I am Senior Vice President, Fraud Risk and Technology Risk Management, Head of Internal Investigations at EverBank.[1] Prior to joining EverBank, I spent over a decade as a state and federal prosecutor, bringing an understanding of regulatory expectations, corporate governance, and financial crime expertise to my role at the bank.

In addition to my role at EverBank, I also serve as the Chair of the Consumer Bankers Association (CBA)[2] Fraud Management Committee. The CBA Fraud Management Committee provides senior leaders of fraud and scam prevention at the nation's leading retail banks an open forum to discuss best practices, emerging trends, and provide expertise related to advocacy in the federal legislative and regulatory environment.[3] On behalf of the CBA Fraud Management Committee, I also served as a delegate to the Aspen Institute's National Taskforce on Fraud and Scam Prevention.

CBA's broad membership – representing America's leading Main Street banks - have been raising the alarm for years about the rise in fraud and scams that are inflicting deep financial and emotional harm on American consumers and small businesses. Banks invest billions of dollars and thousands of hours to combat fraudsters and scammers each year.[4] This includes constant education campaigns to warn customers about new and emerging threats.

Successfully combating fraud and scams requires a robust understanding of the key differences between the two illicit activities, as their unique features should dictate the methods used to counter each of them. Bank fraud generally involves an attempt to obtain money that is owned by or under the custody or control of a financial institution by false pretenses or misrepresentation, or at a more basic level, attempts to defraud a financial institution See: (18 US Code Sec. 1344). This generally refers to situations in which a fraudster tries to borrow, withdraw, or move money from a bank account without the authority to do so. In modern times this often involves trying to use a computer system to access a customer's account without authorization or impersonate a customer through the phone channel. Bank fraud is best prevented

[1] EverBank N.A., formerly known as TIAA Bank, is a nationwide specialty bank servicing clients across the United States with a focus on delivering high-value products competitive deposit, lending, and commercial solutions.
[2] The CBA is a member-driven trade association, and the only national financial trade group focused exclusively on retail banking—banking services geared toward consumers and small businesses. As the recognized voice on retail banking issues, CBA provides leadership, education, research, and federal representation for its members. CBA members operate in all 50 states. They include the nation's largest bank holding companies as well as regional and super-community banks. Eighty-three percent of CBA's members are financial institutions holding more than $10 billion in assets.
[3] https://consumerbankers.com/committee/fraud-management-committee/
[4] https://www.pymnts.com/fraud-prevention/2023/banks-and-payment-firms-tap-ai-to-combat-fraud-amid-surge-in-sophisticated-financial-crime/

with controls that detect when a misrepresentation occurs, and banks with online presences have established strong control environments to detect and prevent these types of fraud attempts, securing the customers' assets and protecting the integrity of the financial system.

Scams, on the other hand, involve criminals deceiving customers directly, often through phone, text, or online communication and convincing the bank's customers to send money out of the bank under false pretenses. Notably, scams generally occur outside of the bank's control environment and the first time the bank becomes aware of the transaction is when the customer requests that their money be moved. Like bank fraud, scams, are best prevented where the deception occurs – in the phone, text, or online channel where the scammer tries to convince the customer to send them money. Today, the primary tool we have to help our customers recognize and prevent scams is to raise consumer awareness of these activities beyond their banking channels and that target the fraudulent conduct occurring in those external channels.

This distinction between fraud and scams is critical and is one reason that CBA has called for consistent standards for how various fraud or scams are classified. On fraud, banks continue to deploy significant controls to prevent and detect fraud, deploying behavioral biometrics, artificial intelligence models, real-time transaction screening, two-factor authentication, digital ID verification, dark web monitoring, and 24/7 investigative teams. The results matter: Most fraud attempts are stopped before customers ever see them.

Banks invest heavily to fight fraud, working together with government and fraud prevention experts leverage data and signal to detect and prevent billions of dollars of fraud within bank-managed channels. When fraud touches the bank, we can see it, detect it, and stop it.

Scams are fundamentally different. Scams occur when criminals manipulate victims into willingly authorizing payments. Banks are required to direct authorized payments where the customer wishes them to go. These are not bank system breaches that the banks are capable of detecting and preventing, but are social engineered operations aimed at the customer or small business where the deception and related data and signals happen entirely outside the regulated banking system. Only when the customer authorizes a payment does the bank get involved, and then it is often too late.

Unfortunately, both fraud and scams have continued to become more sophisticated and more pervasive year-over-year. Criminals are leveraging data from decades of breaches and stolen information to carefully target potentially vulnerable scam victims. They are imitating legitimate individuals, companies, and financial institutions to gain the trust of our customers. They are eroding trust in reputable institutions, inflicting financial and emotional harm on our customers, and exploiting some of the most vulnerable members of our society.

Scams are largely driven by criminals operating on social media platforms, online marketplaces, messaging apps, telecom networks, and fraudulent digital advertising channels among other places. New technology has birthed new forms of scams, especially in the AI era. These criminal enterprises relentlessly bombard consumers outside of bank-managed channels, with sophisticated scams through endless phishing emails, spam texts, fake "Amazon shipment" notifications, long-term interpersonal engagements on social media platforms, and more. Continuing technological evolutions are making it harder for even the most diligent consumers to effectively be on their guard. Scammers are using AI to assemble detailed profiles on potential scam victims, obtaining details they use to establish trust. More advanced applications like AI-generated voice cloning and video impersonations, once confined to the realm of science fiction, are now a fraud and scam reality. Although many of the schemes are not new, modern scams evolve every day. Unfortunately, as the deception happens so far upstream, banks are often the last line of defense with scams, not the first. By the time a bank is involved, the customer is already convinced that they need to send money to the scammer, and the bank is trying to put the puzzle together while the customer insists that the money be sent right away.

CBA members – and the banking industry as a whole - are working day and night to combat the swift and nimble nature of these criminals. To win the fight, however, and actually stop fraud before it even reaches a bank or a bank's customer, there are several opportunities for policymakers to make a meaningful difference. The steps this Committee and specific members have taken in a bipartisan manner demonstrate policymakers' aim to tackle this consumer crisis. A number of legislative proposals have been introduced and will be extremely meaningful to address the numerous complicated facets of scams. But even more will be needed, including Administrative and agency actions to create an even greater unified approach across government and the private sector to educate consumers, to investigate and mitigate scams, and prosecute bad actors. Overall, the efforts by Congress and the Administration should be aimed at: strengthening coordination; enhancing information sharing; modernizing regulatory tools; a unified approach to scam awareness education and; protecting consumers when and where the scam occurs, before it ever reaches their bank accounts.

In my testimony I will:

- Provide an overview of the alarming scale of the fraud and scam epidemic
- Outline the differences between fraud and scams that impact the toolsets used to address each
- Explore why scammers are winning
- Highlight what banks are doing to protect customers
- Emphasize the need for a whole-of-government strategy to combat fraud and scams
- Recognize positive federal legislative and regulatory developments
- Offer recommendations and a roadmap for policymakers to better support the private sector and federal government in stopping fraud and scams

EverBank and the Consumer Bankers Association's membership more broadly remain committed to working with this Committee to increase public and private sector coordination, better protect consumers, and address the root causes of fraud and scams.

**A National Crisis: The Alarming Scale of the Fraud and Scam Epidemic in the U.S.**

According to recent Federal Trade Commission (FTC) data, consumers reported losing approximately $12.5 billion to fraud in 2024, which represents a twenty-five percent increase from the previous year. This trend is just due to a spike in reporting, we are seeing a significant rise in the percentage of Americans who have fallen victim to fraud or scams, jumping from twenty-seven percent thirty-eight percent from 2023 to 2024.[5]

But, as noted earlier, scams have become far more pervasive for consumers—and as the FTC reports what acts comprised those $12.5 billion in losses, the top five are all scam activity, including: 1) imposter scams; 2) online shopping and negative review scams; 3) business and job opportunity scams; investment scams; and internet service scams.

As the FTC reports, "big losses follow scams that start with a call or on social media"[6] This economic damage is inextricably linked to the profit incentives of the digital platforms where these schemes frequently originate.

An internal report from one of the most prominent online platforms estimated it generated 10% of its revenue, or $16 billion, by allowing fraudulent advertisements and scams to proliferate on their websites.[7] That same platform is also accountable for close to half of the reported scams on the peer-to-peer payment platform Zelle, leading to millions in losses for customers.[8] While certain online platforms profit, the banking industry faces the burden of managing the fallout.

Scammers often operate across international borders and exploit digital platforms with limited identify verification. The challenge is further complicated by a fragmented reporting infrastructure that obscures the true extent of the crisis. While the Federal Bureau of Investigation (FBI) received nearly 589,400 scam related complaints in 2023 totaling over $10.55 billion dollars in losses, a recent Government Accountability Office (GAO) report reveals a systemic lack of coordination among federal bodies to investigate or assist victims of scams. Of the thirteen federal agencies involved in countering these threats, only eight currently maintain the capacity to receive scam complaints from the public, leaving a significant portion of the regulatory landscape unable to effectively track or respond to the evolving needs of consumers.[9]

---

[5] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
[6] https://www.ftc.gov/system/files/ftc_gov/images/csn-scammy-snapshot-2024.png
[7] Horwitz, J. (2025, November 6). Online Platform is earning a fortune on a deluge of fraudulent ads, documents show. Reuters.
[8] https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8#selection-2405.0-2405.60
[9] https://www.gao.gov/assets/gao-25-107088.pdf

When scammed, victims face difficulty navigating all the service providers, law enforcement agencies and multiple jurisdictions that may be involved. Banks, realizing that they are not capable of detecting and stopping scams on their own and face regulatory obstacles when trying to, struggle to join with other industries to share information and pool resources. Law enforcement agencies have tools to counter the swift actions of illicit actors working globally, but they require new mandates, immediate access to data and signals, and resources to evolve new ways to work across silos of expertise and legal authority.

**Fraud and Scams Are Related, but Distinct, Illicit Activities that are Addressed through Different Toolsets**

Fraud and scams are often conflated in discourse of this threat, as both have the same net result: funds ultimately come into the possession of illicit actors and can then subsequently be used for other nefarious purposes. However, it is vital to distinguish between the two because the remedies required for stopping the two are different.

Bank fraud generally involves an attempt to obtain money that is owned by or under the custody or control of a financial institution by false pretenses or misrepresentation, or at a more basic level, attempts to defraud a financial institution See: (18 US Code Sec. 1344). This generally refers to situations in which a fraudster tries to borrow, withdraw, or move money from a bank account without the authority to do so. The term “scams” covers instances in which individuals are manipulated into authorizing transfers themselves, a category sometimes referred to as “authorized push payment fraud.”

These methodologies leverage some of the same tactics, such as social manipulation and technical exploitation to bypass traditional safeguards, but there are tangible differences. For example, interpersonal and social deceptions such as romance scams, often termed “pig butchering,” represent a form of long-term engagement where bad actors cultivate false intimacy over months to induce victims into making authorizing investments or emergency transfers. Here these methodologies are used to facilitate a “scam,” to convince the victim to push out funds to the criminal themselves.

However, similar tactics are employed in job scams where synthetic professional identities are used to harvest personal data and bank details from unsuspecting job applicants under the guise of legitimate remote employment. The same methodologies are also used for the purpose of fraudulently gaining access to a victim’s account. Furthermore, despite the decline of physical paper in commerce, check fraud remains a significant risk involving either fake checks designed to trigger advance fee repayments or check washing where stolen mail is altered to divert funds. The rise in remote deposit capture and using cell phone photos to deposit checks through apps creates further difficulties as banks do not have the physical check to examine when determining

whether an instrument is altered or forged. This sits alongside broader bank transfer fraud which leverages both fraud attacks on banks' digital controls and social engineering to bypass standard verification protocols.

This distinction matters because the tools most effective in combating fraud and scams will necessarily differ based on these features. With respect to fighting fraud, since the illicit activity centers on impermissibly gaining access to a victim's account, the necessary tools are those that ensure authorized access, with particular emphasis on confirming the identity of the person attempting to access the account. Through tools such as password protection, multi-factor authentication, biometrics, device risk assessment, and other advanced fraud detection methods, banks are well positioned to determine whether a transaction was truly initiated by the consumer and often can verify whether the funds are being sent to a like-named account.

With respect to fighting scams, however, the necessary toolset is entirely different and extends beyond the control environment of banks. The key issue is that, in a scam, the consumer knowingly and intentionally authorizes payment to a particular account. In many cases the customer is quite insistent that the payment be processed immediately, and the bank has very limited information as to why the customer is sending the payment to a particular destination. Banks do not have access to the upstream communications — such as emails, social media messages, text messages, video calls, or phone calls — that would provide insight into the nature and validity of the relationship prompting the consumer to initiate the transaction. The fraud detection signals exist as a part of these upstream communications, and the bank does not have access to those signals. This issue is further exacerbated as an increasing number of transactions occur outside traditional bank-enabled channels, such as through fintech enabled rails or Bitcoin ATMs, that bypass conventional protections, leaving consumers more vulnerable. Accordingly, the tools needed to combat scams must target these upstream channels through which scams are perpetrated and promote consumer education aimed at helping individuals identify and avoid such schemes. The time to detect or prevent the scam is when the deception occurs, during upstream communication. Scam education can prevent deception which is why banks work hard to educate their customers. Otherwise, the deception signals related to upstream communication are essential to disrupt the scam and banks do not have access to those signals.

**How Scammers are Winning, and Why Banks Cannot Stop Them Alone**

To build a truly effective defense, we must understand why scammers are currently succeeding at such a high rate. The average American is facing a constant, multi-front attack that happens largely outside the safety of bank-monitored channels. These criminals use a relentless stream of phishing emails, scam texts impersonating business and financial institutions, fake shipping alerts, follow-up phone calls, social media messages, and fake websites and social media profiles and advertisements to target people where they live and work.

The threat vectors for scams in particular is almost exclusively present on non-financial platforms where the warning signs are often obvious but go unaddressed. We see this in online platforms and marketplaces where the exact same car is listed for sale in every state at once, or on social media or dating sites where synthetic profiles send the same automated messages to thousands of potential targets. Perhaps most concerning is the rise of social media streams and pages that are openly dedicated to teaching people how to commit fraud or scams, yet these platforms often provide no clear way for the public to report the content or for the authorities to effectively shut them down.

This problem is significantly worsened by the rapid pace of technological change, which makes it difficult for even the most careful consumers to stay protected. For example, AI-powered voice cloning and image impersonation, which used to be the stuff of science fiction, is now a common tool for scammers to impersonate loved ones or officials to induce a consumer into sending funds. These criminal organizations operate across international borders and target every piece of technology we rely on, from our smartphones to our personal computers, to trick people into moving money out of the regulated financial system and into the hands of bad actors.

**How Financial Institutions are Working Proactively to Safeguard Consumers**

Financial institutions are deeply committed to safeguarding their customers, especially individuals who may be more vulnerable, such as older adults. This commitment extends far beyond simply meeting regulatory requirements. It reflects a genuine dedication to protecting customers' financial security, promoting their overall wellbeing, and ensuring they can engage with and conduct their financial services needs confidently and safely. Financial institutions utilize the unique tools and train passionate fraud detection and investigation teams to prevent and mitigate fraud, as well as the tools at their disposal to mitigate scams, though given the unique nature of scams, banks are only able to diminish certain risk vectors that are actually within their control.

Mid-sized and regional financial institutions like EverBank invest resources and time in specialized training for staff, purchase and integrate fraud prevention technology and implement programs designed to identify and assist at risk consumers, helping them to not fall victim to scams. Some of the techniques we use include:

- Conducting risk assessments on transactions and their destinations across payment channels
- Using behavioral biometrics to detect and prevent account takeovers

- Reporting bad actors and sharing information with consortiums and credit bureaus to mitigate scams
- Investing resources in both people and technology to combat innovative scams
- Targeted customer training for scam and fraud scheme awareness
- Collaborating with law enforcement agencies to provide fraud and scam training
- Implementing two-factor authentication
- Developing a robust taxonomy for reporting and classification to address issues effectively and at scale
- Using advanced analytics to identify and combat account takeovers
- Utilize targeted in-app messaging to inform and educate consumers
- Investigating the dark web for compromised accounts proactively to protect customers.

While not all banks have the resources of some of the largest financial institutions, we do still leverage sophisticated third-party fraud tools to protect our clients. However, banks like EverBank are often more reliant on manual processes and skilled fraud detection and investigation associates to combat fraud and scams. These fraud-fighters work directly with our customers and other financial institutions to decision fraud alerts, investigate cases, and work to recover money that was moved between institutions due to fraud or scams. By taking proactive steps, including monitoring unusual account activity, educating customers about common and emerging fraud and scam techniques, and creating policies that prioritize customer protection, banks demonstrate a sincere desire to support the Main Street communities and protect the customers they serve. Ultimately, these efforts reinforce trust, strengthen long-term customer relationships, and help create a safer financial environment for everyone across the banking ecosystem.

Many institutions the size of EverBank also leverage the resources provided by trade associations such as CBA. As previously noted, CBA's Fraud Management Committee has become a resource for member banks to discuss and share mitigation efforts, discuss types of attacks, and data trends across different institutions. Some examples about how effective this Committee has been for the industry, and the consumers we serve, examples of the action's banks are taking to fight fraud and scams, and protect their customers, include:

- Sharing best practices to combat specific scams and fraud schemes
- Identifying and sharing new fraud trends
- Establishing contacts at other banks to expedite fund recovery
- Engaging with fraud service vendors to share knowledge and improve tools
- Meeting with other industry groups such as Telecoms to share knowledge and establish best practices
- Engage with industry groups such as EWS, NACHA, to suggest improvements to protect our institutions and customers

- Bring in experts to educate the membership on new trends and emerging threats
- Sharing customer communication and training methods
- Investing resources in both people and technology to combat innovative scams to identify and combat account takeovers

While this list is not exhaustive, it demonstrates the commitment of financial institutions across the country in combating fraud and scams daily.

**CBA Strongly Supports a Whole-Of-Government Approach to Combat Fraud and Scams**

There is a desperate need for a greater collective approach to addressing the root causes of fraud and scams, before they ever reach a bank or, for that matter, a bank's customer.

In July 2024, CBA convened a roundtable with participants representing the federal government, private sector entities, non-profit consumer organizations, and industry trade associations from the banking and telecommunications sectors to discuss the need for a national strategy for combating fraud and scams. CBA also contributed to the publication of a discussion paper exploring how industries could work together and with government to prevent fraud and other harms against consumers and businesses, "Stopping Scams Against Consumers: Roadmap for a National Strategy."[10] These efforts were followed by the Aspen Institute Financial Security Program (Aspen FSP) announcing the formation of a National Task Force for Fraud & Scam Prevention - an initiative that brought together leading stakeholders from government, law enforcement, private industry, and civil society to develop a nationwide strategy aimed at helping prevent fraud and scams.

CBA simultaneously worked with our Fraud Management Committee and through the Aspen Institute's National Task Force for Fraud & Scam Prevention, of which I served as a delegate, to develop important industry and government wide recommendations regarding fraud and scams.[11]

Although the banking industry is working day and night to combat the swift and insidious nature of these criminals, to win the fight, and actually stop scams before they even reach a bank, there are several important steps policymakers can take. One of the most important things the federal government can do today is establish a whole-of-government strategy—one that creates a unified set of definitions and terminology for categorizing different frauds and different scams. A singular and approachable means for ensuring victims can report scams, with tracking and information systems that cut across agencies to deliver critical information to various agencies, law enforcement, and as appropriate, industry participants, such as banks.

[10] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4897644
[11] https://fraudtaskforce.aspeninstitute.org/phase-one-outputs

While much of the recommendations below focus on Congressional actions and recommendations, the Administration could also take meaningful steps in the near term, in tandem with Congress' actions, to initiate near-term and longer-term changes. For example, the Administration could issue an Executive Order (EO) establishing a formal, government-wide framework for combating fraud and scams. Such an Executive Order would not replace legislative action, nor would it alter Congress's important oversight role. Rather, it would provide immediate structural alignment across agencies while longer-term statutory reforms are developed and considered.

Any EO should identify an agency to lead this whole-of-government approach, and accelerate many of the bipartisan objectives already under consideration by Congress, including:

- Creating a nationally coordinated fraud scam awareness campaign, similar to the Smokey the Bear campaign to prevent forest fires or the "Take Five to Stop Fraud" campaign in the United Kingdom
- Directing the development of a unified federal fraud and scam taxonomy and standardized definitions across agencies
- Establishing a centralized inter-agency reporting and data-sharing infrastructure to streamline complaint intake and trend analysis
- Clarifying safe harbor protections to enable responsible cross-sector information sharing among financial institutions, telecommunications providers, and online platforms
- Formalizing coordination between financial regulators, law enforcement, the Federal Trade Commission, Treasury, the Department of Justice, and telecommunications regulators
- Requiring periodic public reporting on scam typologies, enforcement actions, and loss trends
- Elevating fraud and scam prevention as a core national consumer protection priority

Given the fragmented reporting structure identified by the Government Accountability Office and the cross-sector nature of scam activity, executive coordination is both practical and urgently needed.[12] Moreover, a formal whole-of-government directive would send a strong signal to criminals – both domestic and transnational – that the United States is aligning its enforcement, regulatory and supervisory tools to address scams at their source.

**Emerging Positive Federal Opportunities to Combat Scams**

Congress and members of this Committee should be commended for coming together in a bipartisan way to work collaboratively in the fight against fraud and scams.

[12] https://www.gao.gov/products/gao-25-107088

*Positive Legislative Developments*

Ongoing efforts in Congress are encouraging, particularly through bipartisan and bicameral measures such as the Guarding Unprotected Aging Retirees from Deception (GUARD) Act[13] and the Taskforce for Recognizing and Averting Payment Scams (TRAPS) Act.[14] These bipartisan bills, led by Representative Zach Nunn (R-IA) in the House, provide essential, targeted protections for elderly populations and aim to streamline interagency communication through the formation of specialized anti-fraud task forces.

More recently, the Financial Services Committee has continued to lead the charge through hearings and roundtables. This past October, under the leadership of Subcommittee Chairman Dan Meuser (R-PA), the House Financial Services Oversight and Investigations Subcommittee held an important hearing that provided a great platform to identify exactly how scammers are executing their schemes. Roundtables with industry participants have continued to build on this work.[15]

Further, additional bipartisan and bicameral legislative solutions such as the Safeguarding Consumers from Advertising Misconduct (SCAM) Act have been introduced.[16] This legislation, also led by Subcommittee Chairman Dan Meuser (R-PA) in the House, represents a concrete step toward addressing the origin of many schemes by directing the FTC to establish identity verification and safety protocols for advertisers on online platforms. This measure is particularly vital given that fraudsters often leverage deceptive advertisements to facilitate fraudulent product sales outside the banking environment, often resulting in the permanent flight of capital from the regulated financial system.

CBA strongly supports these legislative proposals, roundtables, and hearings.

CBA is also pleased that several thoughtfully drafted pieces of legislation have been included for discussion in this hearing. This includes proposals to establish a safe harbor for banks related to information sharing, to require federal bank regulators to conduct a study about the technology being used, and needed, by banks to combat frauds and scams, and to consider updates to the Regulation CC framework.

*Positive Congressional Appropriations Developments*

[13] https://www.congress.gov/bill/119th-congress/house-bill/2978
[14] https://www.congress.gov/bill/119th-congress/house-bill/4936
[15] https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=410851
[16] https://www.congress.gov/bill/119th-congress/house-bill/7548

The most recent Financial Services and General Government Appropriations bill represents a particularly significant step in the fight against fraud.

As CBA has been calling for a whole-of-government approach to fraud and scams, the package contains language directing the Department of Treasury, in consultation with all members of the Financial Stability Oversight Council (FSOC) and the Federal Trade Commission (FTC), to submit a national strategy or plan that leverages and augments local, State, and Federal resources within the financial sector to mitigate and prevent online scams.[17] We commend the Representative and Senators for recognizing the continued rise in prevalence and damage to the American consumer that we have called attention to as an industry for so long. We look forward to Treasury carrying out this language and are happy to provide any resources necessary to aid in its development.

Additionally, CBA commends the inclusion of language directing FinCEN to submit a report encapsulating many different vectors of fraud data such as the volume of scams, the number of individuals scammed, the dollar amount lost to scams, and which type of scam was employed.[18] Having this data in one clear concise report will give key insights into trends the aforementioned GAO reports state are clearly missing in its current dataset.

Despite these successes in the appropriations process, significant legislative work remains to be done.

*Positive Executive Branch and Regulatory Developments*

The Administration is also taking steps against the evolving fraud landscape, marked by a significant increase in engagement from the Department of the Treasury and other prudential regulators. The recent issuance of a Request for Information (RFI)[19] regarding potential actions to address payments fraud represents a critical opportunity for industry participants to shape a more cohesive regulatory framework. In submitting formal comments, CBA emphasized that any solutions must facilitate a robust cross sector and public-private collaboration. This approach ensures that all relevant stakeholders, including those in the telecommunications and social media sectors where scams often originate, bear the necessary obligations to monitor and disrupt fraudulent activity at its source.[20]

The Executive Branch has further intensified its enforcement through the Department of Justice's creation of the Scam Center Strike Force. This initiative represents a targeted response to the

[17] Joint Explanatory Statement, Public Law 119-75
[18] Joint Explanatory Statement, Public Law 119-75
[19] https://www.federalregister.gov/documents/2025/06/20/2025-11280/request-for-information-on-potential-actions-to-address-payments-fraud
[20] https://consumerbankers.com/comment-letter/cba-responds-to-prudential-regulator-rfi-on-payments-fraud/

proliferation of Southeast Asian scam compounds that orchestrate complex pig butchering and cryptocurrency investment schemes against Americans. By actively dismantling these criminal organizations, the Strike Force provides a vital mechanism to counter groups that have historically operated with immunity.

In addition to these strategic inquiries, the Federal Reserve has taken operational steps to bolster the nation's defenses by releasing comprehensive online toolkits for scams and check fraud mitigation.[21] These resources are designed to support broad based education and increase awareness among both financial institutions and the general public, directly addressing the reporting and education gaps previously identified by the GAO. By providing detailed information on the fundamental mechanics of fraud and the specific tactics employed by illicit actors, the toolkits enable the payments industry to better identify and counteract sophisticated schemes in real time. These initiatives foster the type of industry collaboration that is essential for mitigating the financial impact of authorized push payment fraud and modern check washing techniques.

While these educational tools represent a component of a national defense strategy, they also highlight the ongoing necessity for a unified federal approach that combines consumer awareness with robust technological safeguards. The toolkits provide essential information on various scam scenarios to heighten consumer awareness, yet the long-term effectiveness of these measures will depend on their integration into a wider national strategy that includes standardized reporting and clear legal accountability for all participants in the digital payments ecosystem. By establishing a shared baseline of knowledge and fostering cooperation across the financial sector, the Federal Reserve's initiatives serve as a foundational element in the broader effort to protect the integrity of the American financial system from increasingly innovative criminal threats.

**Recommendations for Policymakers to Better Support the Private Sector and Federal Government in Stopping Fraud**

This relentless threat of fraud and scams can only be effectively addressed through a comprehensive, whole-of-government approach that promotes cross-sector, public-private collaboration. A coordinated federal strategy – integrating financial regulators, law enforcement, and other relevant agencies – should prioritize fraud and scam prevention as a core component of protecting consumers' economic well-being. Importantly, the tools that this strategy prioritizes for fighting fraud and scams need to be properly calibrated for targeting and addressing the unique aspects of both. To meaningfully reduce scam losses, Congress and the Administration must improve coordination across agencies, remove barriers to information sharing, update

[21] https://www.frbservices.org/news/fed360/issues/081425/industry-perspective-toolkits-scams-check-fraud-mitigation

regulatory tools for the digital era, and shift prevention efforts upstream—stopping scams before funds ever move through the banking system.

*Information Sharing*

Central to these efforts is robust information sharing that enables those on the front lines to identify, target, and disrupt illicit activity. The first step in stopping a threat is recognizing it, and initiatives that facilitate the sharing of actionable information are essential. To that end, a centralized, industry-wide framework, including a common fraud and scam taxonomy and consistent terminology, is vital. A shared language and standardized reporting structure would improve transparency, strengthen accountability, and enhance the quality and comparability of data across sectors. Uniform fraud reporting standards – developed collaboratively across the banking, social media, and telecommunications industries – would further streamline investigations and improve coordinated response efforts. To enable meaningful information sharing, policymakers should also clarify and expand safe harbor frameworks to explicitly cover fraud and scams, ensuring institutions can share relevant threat intelligence with confidence and without undue legal risk. Financial institutions are eager to share this information to strengthen collective defenses, but they must be assured that doing so will not expose them to unnecessary liability.

Fraud and scams are currently reported to the government through the FinCEN Suspicious Activity Reporting process. This process was designed for AML/BSA reporting that is typically retrospective and built around analyzing transactional data to evaluate potential money laundering which is submitted in a narrative format. In reality, fraud is very different than money laundering. Fraud prevention is reactive and urgent rather than retrospective. Fraud and scam signals are more time sensitive, with immediate action and decisioning to effectively prevent fraud and scams. Additionally, the signals are better consumed as specific data elements related to application, digital fingerprints, login data, and transaction initiation. To prevent and investigate fraud and scams, a more modern fraud-specific reporting system that captures data in a consistent manner would allow the data gathered to be more immediately actioned and potentially shared to prevent fraud and lead to more meaningful fraud investigations. Transitioning fraud from the Suspicious Activity Reporting process to a modern Fraud Signal Report would lead to more valuable and actionable data gathering by the government.

This sort of information-sharing effort could be further strengthened through the creation of a centralized fraud database to identify fraud signals, patterns of conduct, and repeat bad actors to leverage for fraud prevention. These initiatives should be supported by a proactive risk management approach that anticipates emerging threats through advanced analytics, consortium data, vendor partnerships, and real-time alerts paired with customer verification protocols.

According to an October 2025 study by researchers from Notre Dame and Carnegie Mellon universities, the number one thing a bank can do to retain a customer after a fraud incident is to identify the perpetrator.[22]

This underscores that victims want accountability and to deliver it, industry and government must share information more effectively, investigate more efficiently, and remove the operational and legal barriers that keep us from tracking down and stopping bad actors.

*Education Including a Nationally Coordinated Fraud and Scam Awareness Campaign*

Education is equally vital and must continually evolve to meet the challenges posed by increasingly sophisticated fraud schemes. Bank-led education efforts are most effective when delivered at key touchpoints, such as onboarding, product discussions, and annual reviews, using direct prompts that require user acknowledgment. These measures introduce thoughtful friction, creating meaningful pauses that encourage consumers to reassess potential risks. Real-time, personalized guidance from trusted banking professionals remains effective – though less scalable – method, particularly in countering rapidly shifting tactics and misleading social narratives that minimize the harm of scams.

Industry-wide collaboration is also critical. Partners benefit from specialized, ongoing education that emphasizes a holistic, end-to-end view of the fraud and scam lifecycle. A broad, nationally coordinated fraud and scam awareness campaign, similar in scale and visibility to Smokey Bear's wildfire prevention initiative, could help reach diverse audiences and shift public perception. The United Kingdom has shown this could be successful with their "Take Five to Stop Fraud" campaign. The shared challenge is connecting consumers with the necessary tools and knowledge *before* they become victims, which requires sustained innovation, cross-sector coordination, and a comprehensive understanding of fraud's lifecycle. New solutions and partnerships are especially important as a growing share of financial crimes originates overseas through organized global networks.

*Expanding Fraud Mitigation Services at the Federal Reserve System*

Operationally, expanding fraud mitigation services within the Federal Reserve System and developing centralized tools to support law enforcement in tracking and sharing fraud data would help prevent harm before it occurs and ensure that fraudsters are identified, apprehended, and prosecuted before they can victimize additional consumers.

[22] https://mendoza.nd.edu/news/banks-that-identify-fraudsters-increase-loyalty/

At the same time, anti-fraud tools and regulatory frameworks must be modernized to keep pace with increasingly sophisticated threats. For example, modernizing Regulation CC could significantly reduce consumers' exposure to fraud. Consumer protections would be strengthened by clarifying that, although certain Regulation CC exceptions may not apply to electronic payments, other fraud-related and anti-money laundering obligations may supersede next-day availability requirements. Providing greater flexibility under Regulation CC to implement enhanced check fraud safeguards – such as expanding exception holds based on fraud risk and broadening the definition and scope of "new account" exception holds – would support continued investment in modern payment systems while maintaining appropriate consumer protections. Additionally, timelines for submitting, handling, and responding to claims should reflect the modern reality that investigations often rely on instantaneously shared images rather than physically transported documents.

**Conclusion**

The fraud and scam epidemic confronting American consumers is not a series of isolated incidents. It is a rapidly evolving, technology-accelerated, globally coordinated threat that inflicts billions of dollars in losses each year and undermines trust in reputable institutions. Banks like EverBank are investing heavily in people, technology, education, and partnerships to protect our customers, but we cannot win this fight alone. The fact of the matter is that fraud today does not begin at the bank, and it cannot be solved by banks alone.

A whole-of-government strategy that brings together financial regulators, law enforcement, technology companies, telecommunications providers, and social media companies to address the root causes of fraud and scams before they reach our customers is critically necessary.

The good news is that this Committee, and Congress as a whole, have the opportunity to take important steps to further empower the public and private sector to combat the growing fraud and scam epidemic.

EverBank, and the Consumer Bankers Association's membership more broadly remain committed to working with you to increase public and private sector coordination, better protect consumers, and address the root causes of fraud and scams.

Thank you for your attention and for your leadership on this critical issue. I look forward to your questions.