Testimony of

Paul Benda

On Behalf of the

American Bankers Association

Before the

Subcommittee on Oversight and Investigations

Of the

House Financial Services Committee

September 18, 2025

American Bankers Association®

Testimony of

Paul Benda

On Behalf of the

American Bankers Association

Before the

Subcommittee on Oversight and Investigations

Of the

House Financial Services Committee

September 18, 2025

Chairman Meuser, Ranking Member Green, and members of the Subcommittee, thank you for the opportunity to offer testimony for today's Hearing entitled: "Fraud in Focus: Exposing Financial Threats to American Families." My name is Paul Benda, and I am the Executive Vice President of Risk, Fraud and Cybersecurity for the American Bankers Association (ABA)[1] and also serve as the Chair of the International Banking Federation Scams and Fraud Working Group as well as sit on the Advisory Board of the Global Anti Scam Alliance. At ABA, our members know that fraud takes a financial and emotional toll on their customers and banks of all sizes are making extraordinary efforts to protect and safeguard customer accounts as fraud has become more sophisticated.

Introduction

From using breakthrough technologies such as generative artificial intelligence (AI) to old fashioned theft of checks out of mailboxes, bad actors are relentlessly pursuing numerous ways to scam consumers and small businesses out of their money. Banks have a long history of improving and innovating to protect their customers—from the adoption of chip-enabled credit cards to multi-factor authentication to protect user accounts to the use of advanced AI tools to warn customers about potentially fraudulent transactions—banks have been on the front lines of innovation and deploying advanced capabilities to protect their customers. However, the fight against these criminals is one that banks cannot win on their own.

Unfortunately, bad actors are innovating, too. An example of widespread fraud efforts occurred when criminals took advantage of the economic devastation of Covid-19 and the unprecedented government response to support small businesses and out-of-work Americans. By the government's own estimate over $300 billion[2] was lost, fueling the growth of more organized and sophisticated networks of financial criminals who continue to look for new ways to keep the

[1] The American Bankers Association is the voice of the nation's $25.0 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $19.7 trillion in deposits and extend $13.1trillion in loans.
[2] See: https://www.sba.gov/sites/sbagov/files/2023-06/SBA%20OIG%20Report%2023-09.pdf

illicit funds flowing.[3] The criminals are now using the tools, the personal information they stole and bought, and networks they built during the pandemic, along with secure messaging technology, to share tactics, techniques and procedures to expand their reach, finding new people to cash stolen checks and provide "mule" bank accounts[4] to receive and move the funds. They are also becoming more sophisticated, using new advanced deepfakes.

Combating these criminals requires not just banks to act but all entities involved in the scam and fraud ecosystem. It's imperative for the telecommunications companies and their regulators to take action to prevent criminals from spoofing legitimate names and phone numbers to convince customers they are speaking with a bank. Also, social media companies should take steps to proactively root out accounts pretending to be bank employees or financial advisors to convince people to put their money into their investment scams. In addition, the postal service must improve the security of the mail system so that when someone mails a check, it will not get intercepted, stolen, altered or cashed by the criminal.

Most importantly, banks need strong partnerships with law enforcement. These criminals cannot be stopped by banks alone, and we support law enforcement as they combat this scourge. While banks need to have the technology and infrastructure in place to defend themselves and their customers, they can only provide the leads necessary for law enforcement to track down the perpetrators. Law enforcement must have resources adequate to address the size of the problem, and we must have ways of addressing foreign bad actors who operate outside U.S. jurisdiction. Offenders cannot be allowed to continue to steal from American consumers and businesses. Banks also welcome the chance to partner with community-based organizations that are doing critical work in this area, as they are trusted voices in many underrepresented communities.

Banks clearly play a key role in fighting fraud, but unless every player in the ecosystem joins the fight, criminals will continue to steal at a scale we have never witnessed before.

State of Fraud Today

Banks have made significant progress in protecting themselves and their customers from being hacked. One recent industry analysis found that Financial Services, which is a category that includes more than just banks, accounted for only 7.7% of ransomware attacks in Q2 2024.[5] Unfortunately, consumer losses from scams and fraud have been significantly increasing. Reliable data on consumer fraud is scarce, but the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) is the nation's hub for businesses and consumers to report cybercrime and elder fraud.[6] This data is limited to certain types of fraud, and therefore

[3] https://www.sba.gov/sites/sbagov/files/2023-06/SBA%20OIG%20Report%2023-09.pdf
[4] Money mules are people who, at someone else's direction, receive and move money obtained from victims of fraud. technologies to change their voice and appearance in real-time video calls to execute romance and impersonation scams. A significant portion of the $300B that was stolen during the pandemic has been reinvested by these criminals to create a highly advanced and sophisticated adversary who is a far departure from the basic phishing scams of yesteryear.
[5] https://www.coveware.com/blog/2025/7/21/targeted-social-engineering-is-en-vogue-as-ransom-payment-sizes-increase
[6] See, www.ic3.gov

under-reports the true dollar amount of fraud perpetrated, but it is still a useful proxy to identify trends and compare the number of different internet-based scams.

In the IC3's 2024 Internet Crime Report ("the Report"), released in April 2024, data showed a nearly 33% increase in losses reported by consumers and businesses from 2023 to 2024.

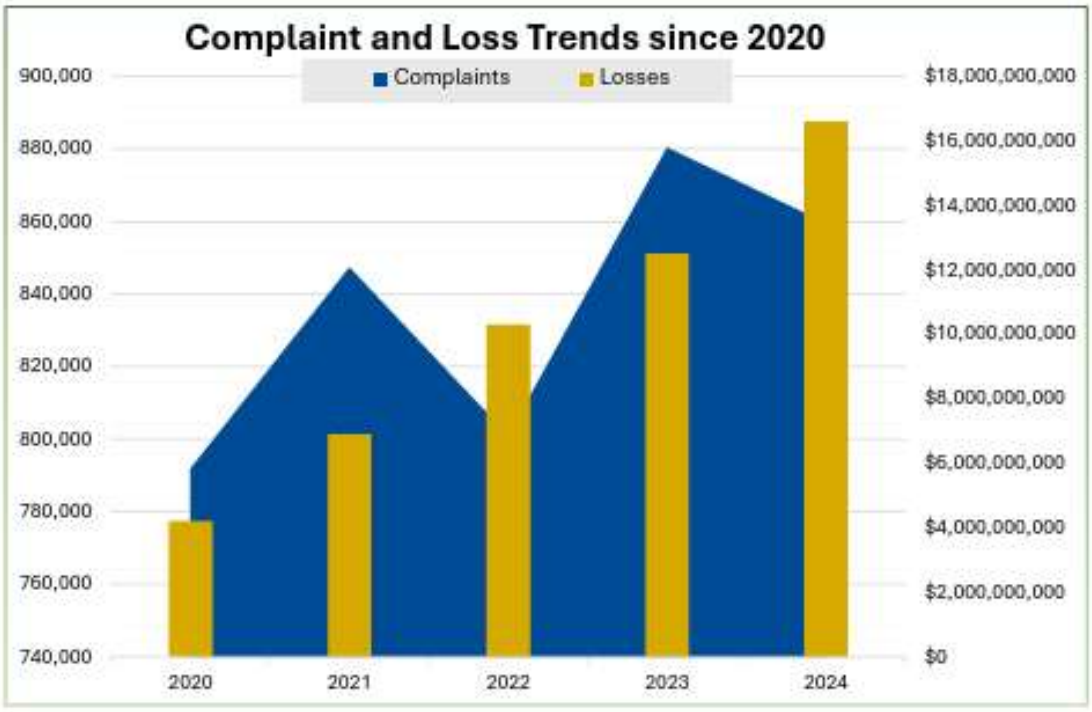

Figure 1. Complaints to IC3 over the last five years.[7]

According to the Report, the top three categories of scams in order of victim losses were investment scams, business email compromise, and technical support scams.

The Federal Trade Commission (FTC) also publishes the Consumer Sentinel Network Data Book[8] on an annual basis that attempts to quantify the amount of fraud being experienced by consumers. Their trendlines are similar to those reported by the FBI and show an increase of 25% from 2023 to 2024 with losses in 2024 of $12.5 billion. Unfortunately, neither the FBI nor the FTC have an accurate accounting of the total amount of fraud experienced by consumers. The FTC attempted to estimate the total amount of fraud due to potential under-reporting in 2023 and estimated total losses could be as high as $158.3 billion[9].

The lack of accurate data makes it difficult to accurately quantify the impact of fraud on Americans—it can be anywhere from $12 billion to nearly $160 billion. It is likely closer to

[7] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[8] https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf
[9] Page 12 - https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf

$100 billion than it is to $10 billion, with Nasdaq estimating fraud losses in the Americas (North and South America) at $151.1 billion[10] in 2024.

The FBI showed a 33% increase in reported fraud by consumers, and the FTC showed a 25% increase year over year. It is clear that fraud is a huge problem that is growing bigger every year and yet there is no central reporting mechanism, no data source that can accurately track the total amount of fraud being experienced, and no single government entity responsible for protecting Americans from the massive thefts of wealth that are taking place on a daily basis. If we cannot accurately measure the fraud that's occurring, the types of attacks taking place, how can we hope to effectively combat it?

One thing is clear from the data; the criminals have shifted their tactics from brute force attacks and account takeover schemes to focus on imposter scams that build trust with the consumer and convince them to authorize the transfer of funds. The 2024 FTC Data Book listed imposter scams as the number one reported fraud category, more than twice as high as the second highest category.

The FBI's top reported fraud loss categories, investment scams, business email compromise, and technical support scams, are all types of imposter scams. Imposter scams can take many different forms, including a criminal pretending to be a financial advisor or romantic partner attempting to convince someone to invest in the next "can't miss" opportunity, or a criminal who has hacked a realtor's email account and then convinces the buyer to change the wiring instructions for the home closing costs. All of these scams depend on the criminal building trust with their victim. In fact, one publication attempted to quantify the different ways that criminals convince their victims to go along with the scam.

They looked at ten different scam types and asked victims of scams how did the criminal gain your compliance—through threats or intimidation, promise of financial gain, or gain your trust? Far and away, the criminals built trust with their victims to gain their compliance, as can be seen in Figure 2.

[10] https://www.nasdaq.com/global-financial-crime-report

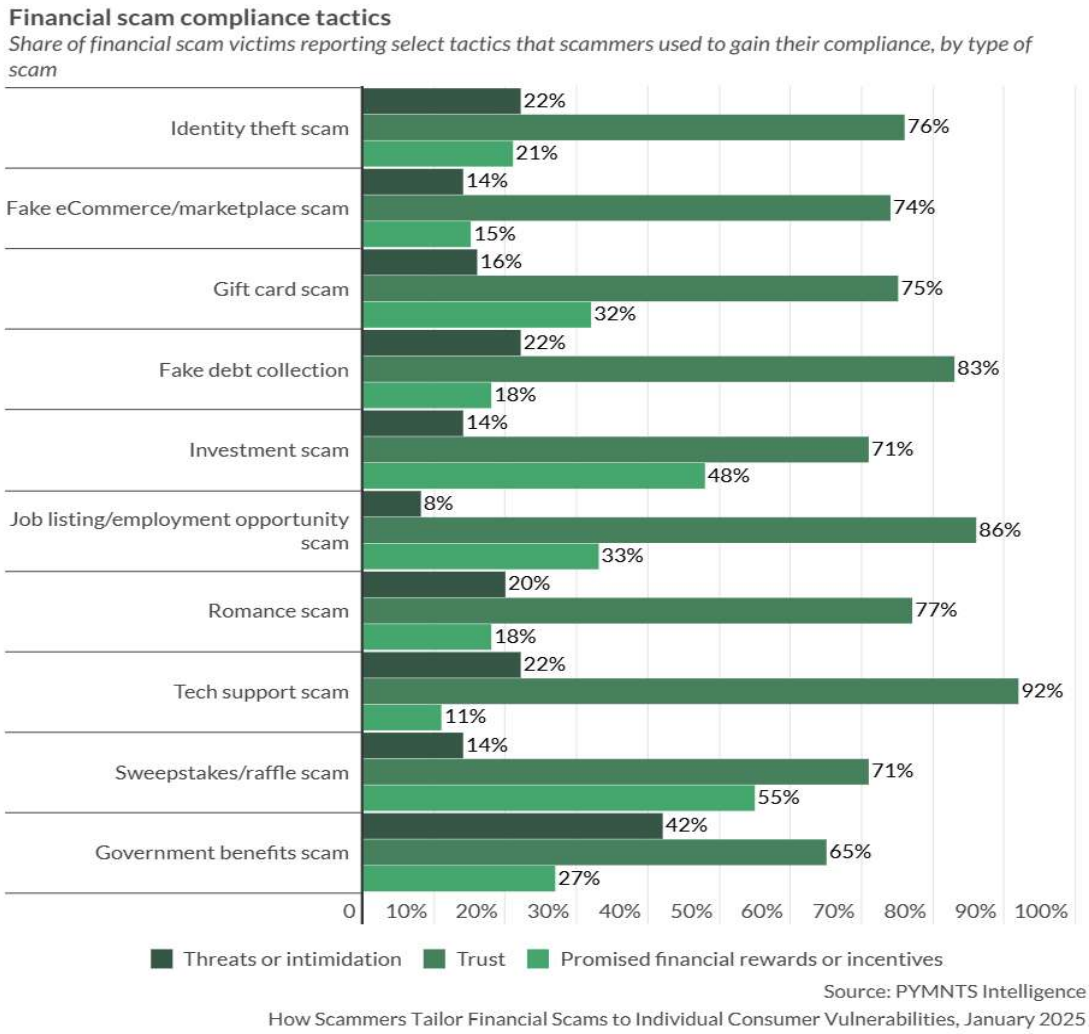

Figure 2. PYMNTS How scammers tailor financial scams to individual consumer vulnerabilities[11]

This presents huge challenges for financial institutions. A cornerstone of our fraud education campaigns revolves around telling our customers not to send money to someone they don't know and trust, but for many scams, by the time that customer is ready to send that payment, they believe they know and trust who they're talking to. In fact, in many instances it can be challenging even for a family member to intervene and stop a loved one from sending funds to a scammer who has built trust over time, and it can be almost impossible for a bank teller to try to convince that person not to make the payment.

How does the criminal gain the victim's trust? Unfortunately, there are many contributing factors, from spoofed caller IDs that fraudulently show the name of a trusted entity such as a bank when it's actually the criminal calling; to social media posts and profiles that either impersonate trusted people or use stolen profiles to peddle different scams; to using stolen personally identifiable information to demonstrate to the victim that they must be from the bank

[11] https://www.pymnts.com/study_posts/how-scammers-tailor-financial-scams-to-individual-consumer-vulnerabilities/

(how else would someone know their name, address, last four of their social security number, etc.?); to the skill of the scammer themselves who have practiced their lines on countless victims before and know all the right things to say to build rapport and trust with their victim. Looking at the myriad capabilities arrayed against the consumer and the industrial criminal complex in place to scam them, the question shouldn't be how someone fell for this scam. The better question is: how does anyone avoid becoming a victim when the deck is so stacked against them?

Combating imposter scams requires a whole of ecosystem approach, meaning each entity that is part of the scam lifecycle has a responsibility to protect the consumer and attempt to prevent the scam from happening in the first place. Telecoms have a responsibility to monitor their networks for scam activities and shut them down as well as ensure the fidelity of caller ID data. Social media companies should ensure that ads posted on their site are from legitimate businesses and shut down stolen and impersonated accounts. Financial institutions have a responsibility to monitor their payment networks for illicit transactions, stop them, and report the transactions to law enforcement. The government has a responsibility to create a national strategy to prevent scams and help coordinate activities across the ecosystem. The customer themselves have a responsibility to educate themselves about potential scams and learn about the tools and capabilities that could help them from being scammed. This type of shared responsibility model has been adopted in Australia and has shown significant promise. It is part of the reason that scam losses have decreased in Australia over the past year.

Though losses from the internet and imposter-based scams are most prominent, check fraud has become one of the fastest-growing categories of fraud impacting consumers across the country. Since the pandemic, check fraud has grown significantly and become one of the biggest drivers of fraud in the country. Unfortunately, just as there is limited data available for scam losses, the same is true for check fraud. Nonetheless, the scale of the problem can be seen with the number of Suspicious Activity Reports (SARs) filed with FinCEN that identify possible check fraud. In 2021, financial institutions filed more than 350,000 SARs to FinCEN to report potential check fraud, a 23 percent increase over the number of check fraud-related SARs filed in 2020. This upward trend continued into 2022, when the number of SARs related to check fraud reached over 680,000, nearly double the previous year's amount of filings.[12] The absolute value of check fraud occurring is unknown, but Nasdaq estimated check fraud losses in the Americas (North and South America) at $21 billion[10].

Even though the exact dollar value of fraud being committed cannot be determined, the trends are clear and troubling. Fraud is increasing across all channels. Banks are investing heavily in new technologies and capabilities to try to stop it, but when customers are convinced into giving their money to criminals or mail gets stolen from a post office, there are limits to what banks can do.

Attacking these trends requires work in the following areas:

[12] Subsequently, that rate has held fairly steady through 2024 with 662,000 check fraud SARs filed, potentially as a result of the law enforcement and regulatory resources focused on check fraud. *See* https://www.fincen.gov/reports/sar-stats

- *Develop a National Strategy to Prevent Fraud and Scams* – The scale of fraud being experienced is a national security threat and should be treated as such with a whole-of-government effort to prevent scams and fraud.

- *Close Loopholes to Stop Impersonation Scams* – Too many loopholes, such as phone number spoofing, exist allowing criminals to impersonate legitimate businesses and agencies.

- *Enhance Collaboration with Law Enforcement and Regulators* – Law enforcement plays a critical role in stopping fraud and ensuring perpetrators are prosecuted and prevented from further activity. Regulators can see patterns and trends that individual banks cannot.

- *Improve Information Sharing* – Criminals have an active information sharing ecosystem that banks and the public sector must match to try to slow the flow of illicit funds.

- *Continue to Enhance Banks' Anti-Fraud Operations* – The scale of fraud being experienced may make existing procedures and policies obsolete, and banks must continue to look for ways to improve bank to bank recoveries and customer experiences.

- *Increase Consumer Education* – Securing someone's account doesn't help if they can be convinced to willingly hand over their money or their login credentials.

Development of National Strategy to Prevent Fraud and Scams

While many of the funds stolen through scams and fraud go to U.S.-based criminals, large amounts are being transferred overseas. Fighting fraud is not only a priority to protect Americans from losing money to criminals, but also essential to protect national security. The lack of a centralized fraud response and tracking capability within the U.S. Government hinders the ability to spot trends, track tactics, techniques and procedures, and the ability to prevent fraud from occurring and to recover funds for Americans when fraud has been identified.

We believe that an Office of Scam and Fraud Prevention should be established within the Executive Office of the President to coordinate interagency efforts, streamline consumer reporting processes, and develop a national scam and fraud prevention strategy that involves both the public and private sectors.

Changes are Needed to Stop Impersonation Scams

Criminals' ability to impersonate legitimate businesses or government agencies is a major challenge that needs to be addressed to prevent the criminals from building trust with their potential victims and to break the scam cycle before it gets started. The challenge can be made more difficult when criminals are able to misrepresent themselves either through a spoofed caller ID that shows a legitimate business name and business' phone number, or through stolen or copycat social media accounts that are indistinguishable from real accounts. Currently technology can help criminals impersonate legitimate actors through three primary channels:

Spoofing of Caller ID – Currently there is very little oversight of the ownership of companies that can register as a telecom to authenticate calls and the numbers that are displayed on a caller ID. Unscrupulous actors have created a business model out of enabling criminals who have figured out loopholes that allow them to "spoof" the numbers and names of legitimate businesses with intent to defraud the call recipient. For example, banks have reported that customers have received calls that show they originate from the 1-800 number listed on the back of their debit card. When a customer is presented with what they believe is technologically validated information, it significantly aids the criminal in convincing the customer that the criminal is actually an employee of the customer's bank.

Impersonation Text Messages – Criminals can use email-to-text tools to create text messages that look like they come from a bank or simply use similar numbers and formats to pretend they are from a bank. These can include links to fake bank websites, call back numbers, or prompts that cause the criminal to call the customer to socially engineer them to give up security credentials or send money from their accounts. In addition to email-to-text messages, criminals are making more use of "SIM boxes," which are devices that allows the use and management of hundreds of SIM cards at once and enables the criminal to send thousands of scam texts in a short period of time. Other jurisdictions have banned SIM boxes. The United States should follow suit or at a minimum telecoms should monitor their networks for this type of activity and be given the authority to shut them down when they are used for fraudulent purposes.

Stolen or Spoofed Social Media Accounts – The FBI reported that investment scams had the highest losses in dollars of all scam types reported. There are many ways these scams can be perpetrated but one recent example is the unknowing takeover of actual bank employees' social media accounts, which were then used to reach out to their connections to convince them to invest in fraudulent investment scams.

Spoofing of Caller ID Information

The Truth in Caller ID Act should be updated to clarify that it is illegal to spoof numbers you do not own or control. The law's current prohibition—that it is illegal to spoof numbers with the "intent to defraud" —requires the government to prove that the bad actor intended to defraud the call recipient, which can be difficult to show. The FCC should be directed to increase enforcement and penalties against actors, including telecoms, that enable criminals to spoof the numbers and names of legitimate businesses on recipients' Caller ID displays when telecoms fail to implement adequate "Know Your Customer" authentication procedures.

In addition to updating the Truth in Caller ID Act, policymakers should take the following steps to prevent criminals from using our calling network to place illegal calls:

- Set a date certain by which voice service providers of TDM networks must convert their equipment to IP. The existing "STIR/SHAKEN" call authentication framework requires calls to be signed at origination and attested through the call pathway until the call reaches the recipient. But STIR/SHAKEN only works over IP networks. If a call passes through a non-IP framework, the STIR/SHAKEN attestation is dropped. There is evidence that criminals exploit this gap to perpetrate fraud on consumers. Setting a date

certain by which voice service providers of TDM networks must convert their equipment to IP would expedite telecoms' work to transition all networks to IP.

- Require voice service providers that use a non-IP network—i.e., a legacy Time Division Multiplexing (TDM) network—to implement a caller ID authentication framework for that non-IP network. The public should not wait for voice service providers to transition all non-IP networks to IP. Providers should implement a caller ID authentication framework for that non-IP network without delay.

- Prohibit voice service providers from displaying data on the consumer's caller ID device when the authenticity of calls cannot be adequately verified through a direct and verified relationship with the call originator. If a voice service provider delivers to the consumer a call with unauthenticated or falsified Caller ID information, it should state "Unknown Caller" or similar cautionary information in the caller ID display. This will make clear to the recipient that the call is highly likely to originate from a person that is illegally posing as a government or business.

It is well documented that a significant number of scams originate overseas. These criminal enterprises leverage lax controls at telecom companies allowing them to change their Caller ID display number to look like the criminal's unauthenticated call originated within the U.S. Several other countries (United Kingdom, Australia, Germany, etc.) automatically block incoming international calls that attempt to spoof their Caller ID displays. The U.S. should implement a similar capability to block unauthenticated calls. A focus on blocking unauthenticated calls would ensure that legitimate U.S. businesses that place authenticated calls from call centers overseas can display the appropriate Caller ID information and complete their calls to U.S. consumers.

Impersonation Text Messages

There is a persistent and growing concern that SIM Boxes or "SIM Farms" are being used to facilitate text phishing campaigns. SIM boxes are technical devices capable of holding multiple SIM cards enabling criminals to send scam texts to thousands of people at once. Some banks are experiencing over 300% growth in phishing messages. There are very few legitimate uses of SIM boxes, and the U.S. should follow the lead of the U.K. who in April 2025 banned the possession or supplying of SIM boxes. In addition to banning these devices, the FCC should require all telecoms to implement enhanced filtering and detection controls to identify and mitigate when SIM boxes are used and implement enhanced fraud controls to identify criminal actors at account origination.

The FCC should establish a centralized database of customer-reported "SPAM" messages—i.e., suspected fraudulent or spam messages that customers report to their telecom or messaging provider through the "Report Junk" feature on iPhones and "Block and report spam" option on Android devices. The database should allow registered companies, including banks, to review the submissions for brand impersonation so that they can identify ongoing scams. This would allow the company to take action to mitigate the impact on their customers. Additionally, a centralized portal with contributions from telecoms and all significant messaging providers would provide real time intelligence in ongoing scam activities, allowing affected industries to

better respond with tailored mitigation measures. Importantly, all messaging providers—e.g., telecoms, Apple, WhatsApp, etc. —should be required to submit customer-reported "spam/scam texts/messages" to the database.

In addition to establishing a database of reported "SPAM" messages, these other text-based mitigation measures should be considered:

- Require subscribers to opt into "email-to-text" before receiving these messages. Criminals distribute large volumes of "smishing" messages (a "phishing" attack through text message) from e-mail addresses, which convert the e-mail message to an SMS text message. Bad actors often send these "e-mail to SMS" messages from telephone numbers that cannot accept incoming calls. These numbers are not uniquely assigned to an email address, and therefore, they cannot easily be reported and shut down. Requiring mobile wireless providers to offer email-to-text as an opt-in service would significantly reduce the use of this technology to send illegal text messages.

- Require text messages to be authenticated and set a deadline for the development and mandatory implementation of a text message authentication solution.

- Require originating mobile wireless providers to investigate and potentially block text messages from a sender after the provider is on notice from the FCC that the sender is transmitting suspected illegal texts. Criminals frequently use multiple numbers from which to originate texts. Originating providers are well positioned to stop illegal texts from a source because they have visibility into all text messages that a particular source is sending—not solely text messages from a particular number. (Terminating providers already are subject to a requirement to block all texts from a particular number when notified by the FCC of illegal texts from that number.)

Protect Banks' Ability to Send Fraud Alerts

Banks send fraud alerts (also known as "suspicious activity alerts") to a customer when the bank suspects that a bad actor has gained access to the customer's account, such as through a stolen credit card, and is attempting a transaction on the customer's account. Fraud alerts play a critical role in thwarting attempted fraud against customers. However, a rule issued by the FCC in 2024 – and set to take effect this coming April – could effectively require banks to cease sending fraud alerts to certain customers.

Under the Telephone Consumer Protection Act, with limited exceptions, a bank or other business can place an autodialed or prerecorded voice call or text message only with the prior express consent of the called party.[13] A called party has the right to revoke his or her consent to receive these calls. In 2024, the FCC issued an order that requires a business that receives a text from a consumer (i.e., "stop") in response to one type of message to stop receiving *all* future communications from that business by phone or text on unrelated matters – even if that was not the consumer's intent (the "revoke all" rule).[14] Thus, a consumer's "stop" text message sent in

[13] 47 U.S.C. § 227 *et. seq*.
[14] *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rcd 1988 (2024).

response to an autodialed past-due message could lead the bank to opt the customer out of all consented-to messages from the institution, including fraud alerts. This could result in increased fraud perpetrated against the customer. ABA urges the FCC to initiate a rulemaking to revise or rescind the "revoke all" rule.

Stolen or Spoofed Social Media Accounts

Criminals also target consumers by stealing personal social media accounts of employees of legitimate businesses or building fake accounts that portray them as working for that business. In both instances, the brand of the company, often a bank, is used to grant legitimacy to the criminal's posts or messages. While this is a complex problem to combat and prevent, once these "impersonation accounts" are identified there should be a simple, quick and free method to request that they be taken down. Unfortunately, no major social media company offers such a method.

ABA strongly urges policymakers to ensure that social media companies provide a method to report impersonation accounts that is free to access and to use, and that results in an expedited removal of the offending account. Additionally, we recommend that if the hosting company refuses to take down the impersonation account, they then may be held liable for any fraud committed by that account as they are clearly providing the "means and instrumentalities" and have knowledge that the account is engaged in fraud.

Banks are committed to protecting their customers' data and money. Our goal is to provide a safe and sound financial system that allows our customers to achieve their financial goals. Banks spend billions of dollars a year on cyber security and anti-fraud measures to provide one of the most secure banking systems in the world, but banks cannot do it alone. The technology companies that enable criminals to pose as trusted agents must help as well. The criminals have realized the challenges in directly hacking someone's bank account, so instead they focus on convincing customers to give them that access. This is made easier when a phone, text message or social media site tells a consumer they are speaking with a banker and not the criminal behind the screen.

Partnership with Law Enforcement and Regulators

As I have discussed, the rising tide of fraud cannot be fixed by banks or technology alone. At some point, the criminals executing this fraud need to be caught, prosecuted, and sentenced so that they no longer commit these crimes. ABA has a history of partnering with law enforcement and the public sector on education and outreach activities along with identifying potential improvements in addressing fraud. We continue to work with our law enforcement partners and regularly connect law enforcement with banks to try and aid in the recovery of fraudulently transferred funds. Additionally, we are working to leverage existing reporting mechanisms of the IC3 to expedite the ability for banks to request another bank hold funds that were sent as part of a scam, but more needs to be done.

Law enforcement is a critical force in preventing and detecting fraud, and ABA applauds work by the FBI, United States Secret Service, and FinCEN to track and freeze funds that have been transferred fraudulently. The FBI IC3 Recovery Asset Teams have been great partners, but we

are concerned given the volume of fraud, that they may lack capacity to engage in lower dollar frauds that are reported to the IC3 portal. We would welcome a partnership with them to identify those cases that may not be pursued in a timely manner to determine whether a public-private partnership could be created to pursue those cases and result in more funds being returned to consumers.

Americans are losing billions of dollars to fraud annually. Yet, amid resource constraints and compelling demands, local law enforcement struggle to devote appropriate time and attention to these cases. Given the levels of fraud taking place against Americans, police departments and sheriff's offices should not have to choose between dedicating personnel to violent crimes and financial fraud cases. Additionally, law enforcement personnel need more effective training in addressing and responding to fraud allegations. Fraud is a continually evolving landscape and new fraud typologies develop each day. Enforcing the law and responding to these cases requires understanding the multifaceted strategies criminals employ to defraud Americans, particularly with respect to cybercrime. One state that has had success in engaging state and local law enforcement is Texas through their Financial Crimes Intelligence Center[15]. The Texas Financial Crimes Intelligence Center (FCIC) is the statewide fusion center that coordinates Law Enforcement Investigations for various types of Organized Financial Crimes.

While Federal law enforcement has a role to play in shutting down these scams, the volume of crimes being committed means that many cases reported to Federal authorities go uninvestigated and unprosecuted. Congress should establish a grant program for State and Local law enforcement to focus on financial crimes and scam response, enabling them to establish Financial Crime Intelligence Centers similar to the one in Texas. State and local law enforcement have close ties to their communities and can be nimbler in allocating staff to trending crimes.

Check Fraud and Partnership with U.S. Postal Service

Check fraud has increased significantly since the onset of the COVID-19 pandemic.
In response, the ABA and member banks have made combating this rapidly growing threat a top priority, as criminal organizations increasingly rely on check fraud to perpetrate financial crimes. Check fraud schemes commonly begin with a theft of a check from the U.S. mail system, leading to check alterations and counterfeit checks created from the image of the stolen check. Criminals then move quickly from the point of theft to depositing the compromised check(s) into a bank account to steal money.

These schemes range from the simple (a street-level complicit actor taking an altered/washed check to a bank branch to deposit), to the complex (a counterfeit check image being deposited into a criminal controlled account using remote deposit channels). Even using the oldest, most transparent monetary instrument in America (a check), the criminals can leverage the two most difficult factors to defend against bank-related frauds today: speed and anonymity.

ABA and the U.S. Postal Inspection Service (USPIS) quickly recognized the need for cross industry collaboration to combat the growing wave of organized check fraud. In March 2024, the

[15] https://fcic.texas.gov/

ABA and USPIS publicly announced a formal agreement to launch a joint Fraud Awareness Campaign. The joint initiative focuses on four main areas:

- Educating U.S. Postal Service and bank customers about check fraud and what they can do to protect themselves
- Addressing money mules and collusive accountholders
- Collaborating with law enforcement
- Training bank employees and postal workers on red flags and prevention.

Through the partnership, we have placed a strong emphasis on training banks. ABA featured USPIS as a keynote speaker at its Check Fraud Symposium, which included banks of all sizes, industry vendors, and key government agencies. USPIS has also served as a valuable resource on approximately five ABA webinars and podcasts, enabling us to reach banks across the nation.

These speaking engagements have provided banks with critical insights into the importance of robust information sharing with USPIS, particularly in navigating a challenging prosecutorial landscape. As a result, banks have a clear understanding that check fraud investigations are a priority—and that the speed and thoroughness of their reporting significantly enhances the effectiveness of these investigations.

Building on the need for public-private information sharing, USPIS also regularly engages with banks and ABA on check fraud in monthly ABA working group meetings. Through these meetings, bankers learn about evolving criminal trends, regional crime patterns, red flags associated with new fraud techniques, and guidance on where to report suspicious activity—including key elements that should be included in those reports. USPIS has also briefed bankers on the joint USPIS and FinCEN initiative to better track check fraud activity in a timely manner. Banks have been advised to use a key term when filing suspected check fraud activity with FinCEN. This allows USPIS to more easily search and obtain SARs about suspected check fraud activity.

ABA and USPIS have also presented together at law enforcement and private industry conferences and meetings, such as the International Association of Financial Crimes Investigators (IAFCI) and Financial Industry Mail Security Initiative (FIMSI) sponsored events. These events are well attended by local police departments looking for training and information relating to check fraud in their communities.

Joint training sessions provide substantial benefits to both banks and law enforcement agencies, fostering stronger collaboration in the fight against criminal activity. These sessions help clarify emerging criminal tactics that target both consumers and financial institutions alike. For instance, a growing threat involving the rapid movement of stolen checks and check images across state lines—from California to New York—via encrypted platforms like Telegram, poses significant challenges for prosecution given cross-jurisdictional activity. Through joint training, participants share best practices on how to identify, preserve, and report critical evidence.

Improve Information Sharing to Combat Fraud

Given the massive scale and global reach of fraud, it is simply not possible for one bank to fight back alone; collaboration is required to ensure success. One of the most important tools banks have in combating financial crimes is shared information. However, due to inconsistencies across financial institutions, among other reasons, there are challenges in accessing actionable information in a timely manner.

That is why ABA has been working to establish a program to help banks share information that identifies activity that may involve terrorist financing or money laundering and deter crimes like fraud. ABA formed an association of banks to design and develop this new information-sharing exchange, which ABA will manage. The goal is to encourage the sharing of information in real-time so it can reduce the flow of funds to criminals' accounts and improve the quality of banks' reporting. We believe this effort can make a real difference in fighting fraud and other financial crime.

In addition to sharing information across financial institutions, the barriers to sharing information across industries including telecoms, social media, internet service providers and financial institutions should be lowered. The goal should be to prevent fraud from occurring in the first place, so real time information sharing is needed, but the regulatory hurdles, both real and perceived, create disincentives. A safe harbor with appropriate privacy protections should be established for entities engaged in good faith efforts to combat fraud to allow proactive protection of consumers from criminals seeking to scam them.

While sharing of data between private sector entities in real time can help prevent fraud, the government must get better at using, and where appropriate, sharing the intelligence that financial institutions share with them via SARs. Using the FinCEN SAR Stats page and searching for the number of SARs filed in 2024 that relate to fraud turns up 2.2 million records. This means financial institutions file on average more than 6,000 SARs a day focused on fraud. This information and intelligence on fraudulent activity is kept exclusively in the domain of law enforcement and government regulators. To combat the criminals executing these fraudulent activities, government must get better at using, sharing and disseminating the information that the private sector provides. It is certain that some of the information in the SARs submitted, if shared in a timely manner with the right financial institution, could stop a fraud from occurring and stop a person from being victimized. Private sector institutions must get better at sharing between themselves, but the government has a responsibility to better utilize the vast amounts of information that the private sector shares with them with a goal of preventing the fraud.

Banks are Continually Improving Anti-Fraud Operations

The rise in fraud has not only impacted consumers but banks as well. The rise in the volume of cases, the complexity of processing check fraud claims, and the increasing capabilities of criminals with new tactics and technologies has created very significant operational challenges for banks both in combatting fraud and processing claims.

ABA and the banking industry are committed to improving their effectiveness fighting fraud and the experience of customers who experience fraud and scams. To that end, we have launched several initiatives to improve the overall process including:

- ABA established the Fraud Contact Directory. Surprisingly, there is no single resource that a financial institution can go to find a contact at another institution. ABA built this web resource starting with banks and focused on improving and accelerating the check fraud claims process. The effort has now expanded to offer contacts for all different kinds of fraud and has even been expanded to allow access to credit unions all at no cost to participants. This resource includes more than half of all banks in the country and is routinely cited by bankers as providing operational efficiencies as well as helping them recover fraudulently transferred funds.

- Treasury checks are sought after instruments by criminals due to the requirement that a significant amount of funds be made available the day after deposit. The Treasury Department hosts a public facing website called the Treasury Check Verification System (TCVS) that allows a bank to validate the check amount and check number, but unfortunately criminals figured out how to counterfeit Treasury checks and sell versions that are fake but also pass TCVS verification.

- To help address this issue, Treasury built a version of TCVS that also verifies the payee name but due to the sharing of personally identifiable information they did not allow its use through the public website but through a direct connection to Treasury systems. While this connection is free, it does require building of an interface to the Treasury system and onboarding with encryption keys. This process was challenging for some banks as well as for Treasury to try and interact with and distribute encryption keys to the 4500 banks operating in the U.S. To help alleviate these challenges, ABA built an interface to the Treasury Payee Verification TCVS system and hosts it on its website at aba.com/TCVS. This service is free for all ABA member banks and allows them to verify Treasury check details, including payee in real-time. Additionally, we are adding a capability for banks to report when a fraudulent check is found so we will be able to track in real time the level of fraud attempting to be perpetrated against banks. ABA fully supports the Administration's move away from paper checks, but we recognize that moving fully to electronic payments will likely take some time, and this effort will help prevent fraud during the transition. Since its launch in late June nearly 600 banks have logged onto the system and validated over 11,000 Treasury checks.

- Recognizing that check fraud is likely to be a continuous and ongoing problem, simply focusing on the claims process will not prevent the fraud from occurring. So ABA hosted a Check Fraud Summit with banks of all sizes, vendors and regulators and kicked off the National Check Verification Feasibility study. Currently no system exists for commercial/consumer checks like the TCVS system that can validate a check in real time at the bank of first deposit. This effort will explore the potential for development of a standard data file format that would allow existing positive pay vendors and potentially others to share the positive pay and payee positive pay data

recorded by banks which could then be queried in real time by the bank of first deposit to verify a check when it is initially presented for deposit. The initial idea is to build an information exchange that could be leveraged by multiple vendors to provide a capability and preserve competition and encourage vendor innovation. ABA plans to publish the results of the study in October 2025 and is actively exploring a pilot proof of concept with both bank and vendor participants.

- When a scam does occur, time is of the essence, both for the victim to report it and for the bank and/or law enforcement to take action. ABA has launched an initiative that augments existing payment rail recall procedures by attempting to develop a standardized process how banks can notify each other when a fraudulent transaction has been sent, how a customer can report and attest fraud has occurred, and how banks can quickly provide the required legal assurances that the funds can be returned. Currently this process can vary bank by bank but by creating a standardized framework, having outside counsel review the policies and procedures to ensure compliance with laws and regulations, and leveraging the contacts in the ABA Fraud Contact Directory, we hope to accelerate the timelines these hold requests can be sent and acted upon to "catch" the funds before they can be cashed out or sent to overseas banks that may not be cooperative in returning the funds.

In addition to the rise of scams and fraud affecting Americans of all ages, elder financial exploitation, defined as the illegal or improper use of an older adult's funds, property, or assets, is occurring at unprecedented levels. According to AARP, the average loss per victim is approximately $120,000, while the FTC estimates total annual losses of older Americans to be as high as $61.5 billion when accounting for underreporting. These crimes not only devastate individuals and families but also erode trust in financial institutions and place a growing strain on social support systems.

In response, the banking industry has stepped up efforts to detect and prevent exploitation. Banks train staff to recognize warning signs, report suspicious activity, and work closely with law enforcement and adult protective services to investigate cases. They are also educating customers and communities about how to protect themselves and are leveraging technology to flag unusual account behavior. Despite these efforts, banks face hurdles that limit their ability to act swiftly and decisively when exploitation is suspected.

To strengthen these protective measures, the federal government should enact legislation authorizing banks to delay, hold, or freeze transactions when elder financial exploitation is suspected. This law should be modeled after FINRA Rule 2165, which allows securities firms to pause disbursements and transactions to protect vulnerable clients. A national standard would give depository institutions the legal protection they need to take preventive action without fear of liability. It would also close gaps between varying state laws, enable earlier interventions, and ultimately provide stronger, more consistent safeguards for older Americans.

Banks Provide Extensive Consumer Education

Consumers are on the front lines of this fight, and we need to do all we can to ensure they have the tools and knowledge they need to protect themselves. We are proud to report that banks of all sizes have significantly increased their education of customers in recent years in addition to investing billions in fraud fighting technology and tools. For example, many banks routinely provide tips for spotting scams in branches, customer communications, and websites and provide timely warnings that customers do not share passcodes or send money to people they do not know. Many banks also bolster their individual fraud-fighting efforts by participating in ABA's industry-wide consumer education efforts.

However, while banks can help to keep customers' accounts secure, these controls can be defeated if a criminal convinces the customer to let them into the customer's account or to send them money. Ultimately, banks have little power to stop customers from withdrawing their own money, and indeed victims often are coached to ignore the bank employees who warn them not to withdraw or send the money. People need to hear from other sources as well, and ABA encourages other trusted sources, such as government agencies or nonprofits, to partner with us to amplify the important work banks are doing to educate consumers about fraud.

Stopping Phishing

One of ABA's most important consumer protection initiatives is our award-winning #BanksNeverAskThat[16] anti-phishing campaign. Since its launch in October 2020, we have helped educate millions of consumers on how to spot common scams from bad actors posing as their bank.

This public awareness campaign educates consumers by posing ridiculous questions banks would never ask a customer. Using humor, bold graphics, videos, an interactive quiz, and an educational video game, we drive home the message that your bank will also never contact you asking for sensitive personal information such as your password, pin or social security number. ABA provides all campaign materials free of charge to all banks, so they can deliver the #BanksNeverAskThat messaging in their local markets.

To date, more than 2,500 banks have participated in the #BanksNeverAskThat campaign and spread its educational content to millions of Americans through social media, bank websites, ATM screens and bank branches across the country. ABA has also promoted the campaign nationally through television and radio ads. In the Washington area, anyone who has been to a Washington Capitals, Wizards or Nationals game has probably seen its educational message. A Spanish language version of the campaign is also available at: www.BancosNuncaPidenEso.com

[16] www.banksneveraskthat.com

ABA National Consumer Campaign to Combat Check Fraud

Building on the success of the "#BanksNeverAskThat" anti-phishing campaign, the ABA also launched "#PracticeSafeChecks," campaign in 2024. Partnering with more than 1,600 banks across the country in its first year, the campaign educates consumers on how they can protect themselves against check fraud and encourages the use of more secure digital banking tools to send money.

The campaign features educational videos that use humor to engage consumers while delivering clear, actionable fraud prevention tips. ABA and our member banks are sharing these resources—including videos, striking graphics, and safety tips—across social media platforms, websites, ATM screens, and bank branches nationwide.

ABA provides all campaign materials free of charge to member and non-member banks, allowing participating institutions to customize and deploy the content in ways that best serve their local communities, while consumers can also find the helpful tips by visiting www.PracticeSafeChecks.com and our Spanish language website www.CuidaTusCheques.com Both the #PracticeSafeChecks and #BanksNeverAskThat campaigns will relaunch on October 1 with new educational content for consumers. We would welcome and deeply appreciate any amplification of these important campaigns by members of Congress and their offices.

Combating Elder Fraud

In addition to its public awareness campaigns reaching all consumers, ABA has active programs to specifically protect seniors from scams. Given the unique risks facing older customers, ABA works through its non-profit foundation to ensure that all banks, irrespective of membership status, can access tools and resources to prevent, detect, and combat elder financial exploitation.

The ABA Foundation is a 501(c)3 corporation that provides free programs and resources to help banks support the financial well-being of their customers and communities. The ABA Foundation offers banks free resources through the Safe Banking for Seniors program to educate their communities on materials to inform their communities about avoiding scam, preventing identity theft, and financial caregiving. [17]

Since 2016, more than 2,000 banks have participated in the ABA Foundation's program. Banks use the materials to help empower their communities and lead workshops, post videos and other content on social media, and share vital information during one-on-one conversations with customers. All the resources are available at no cost to ABA member and non-member banks.

Through partnerships with the FBI, FTC, USPIS, and other federal agencies, the ABA Foundation has also developed infographics and tip sheets to raise awareness about: check theft scams, cryptocurrency investment scams, deep fake scams, fake check scams, government

[17] https://www.aba.com/seniors

imposter scams, imposter scams, money mule scams, online dating scams, peer-to-peer payments, phishing scams, and tech support scams.[18]

While ABA's campaigns have made a difference in educating the public, we are just one voice. We really need a nationwide message coordinated among multiple agencies (including the CFPB and FTC), nonprofits, and the private sector to promote a simple and memorable action plan for people of all ages facing scams. The campaign should also focus on dispelling the behavioral techniques scammers use in impersonating authorities, indicating urgency, requiring secrecy, and manipulating people into action.

Conclusion

Banks are working every day to protect their customers from fraud by investing in new technologies, deploying public relations campaigns to educate consumers and small businesses about old and new scams, and partnering with law enforcement and other federal agencies on new initiatives to combat fraud. Yet our industry recognizes that there is more work to do, and banks cannot stop criminals by themselves. Every player in the fraud ecosystem must play a role; from the telecommunications firms to the social media companies to the Postal Service. And we would welcome collaboration with community groups who have the trust of consumers across the country. The goal of all banks is to help their customers have a safe and secure financial future, and ABA and the banking industry stand ready to work with all stakeholders to protect our customers from fraud.

Thank you once again for the opportunity to testify. I look forward to answering your questions.

[18] https://www.aba.com/protectyourmoney