Statement for the Record

On Behalf of the

American Bankers Association

before the

Joint Economic Committee

March 25, 2026

Statement for the Record

On Behalf of the

American Bankers Association

before the

Joint Economic Committee

March 25, 2026

Chairman Schweikert, Ranking Member Hassan, Members of the Committee, the American Bankers Association (ABA) appreciates the opportunity to provide a Statement for the Record for this hearing, "The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters." The ABA is the voice of the nation's $25.3 trillion banking industry, which is composed of small, regional and large banks that together employ over 2 million people, safeguard $20.1 trillion in deposits and extend $13.5 trillion in loans.

Introduction

From using breakthrough technologies such as generative artificial intelligence (AI) to old fashioned theft of checks out of mailboxes, criminals are relentlessly pursuing new ways to scam consumers and small businesses and steal money from their bank accounts. 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. Unfortunately, however, the fight against these criminals is one that banks cannot win on their own.

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 $300B[1][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 illicit funds flowing. The criminals are now using the identities and personal information they stole, along with the tools and networks they built during the pandemic, to share tactics, techniques and procedures to expand their reach, finding new people to scam or to cash stolen checks for them or to provide "mule" bank accounts[3] to receive and move illicit funds. They are also becoming more sophisticated, using advanced deepfake 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.

[1] See: https://www.sba.gov/sites/sbagov/files/2023-06/SBA%20OIG%20Report%2023-09.pdf

[2] https://www.sba.gov/sites/sbagov/files/2023-06/SBA%20OIG%20Report%2023-09.pdf

[3] Money mules are people who, at someone else's direction, receive and move money obtained from victims of fraud.

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. Banks also need the telecom companies and their regulators to close regulatory loopholes that allow criminals to spoof legitimate names and phone numbers to convince customers they are speaking with a bank.

Banks need social media companies to proactively root out accounts pretending to be bank employees or financial advisors to convince people to put their money into their investment scams. Banks need the postal service to improve the security of the mail system so that when someone mails a check, it will not be intercepted, stolen, altered, and cashed by the criminal.

Additionally, banks need strong partnerships with law enforcement, so the resources to combat these crimes match the amount of money being stolen from consumers. And when these criminals are caught, the punishment must match the crime, so these offenders will not 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've never witnessed before.

State of Fraud Today

Banks have made significant progress in protecting themselves and their customers from being hacked, but unfortunately bank customer losses from scams have been increasing significantly. Reliable data on consumer fraud are 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 fraud, including elder fraud.[4] These data are limited to certain types of fraud, and therefore under-report the true dollar amount of fraud perpetrated, but are still useful proxies 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 2025, data showed a nearly 33% increase in losses reported by consumers and businesses from 2023 to 2024.

[4] www.ic3.gov

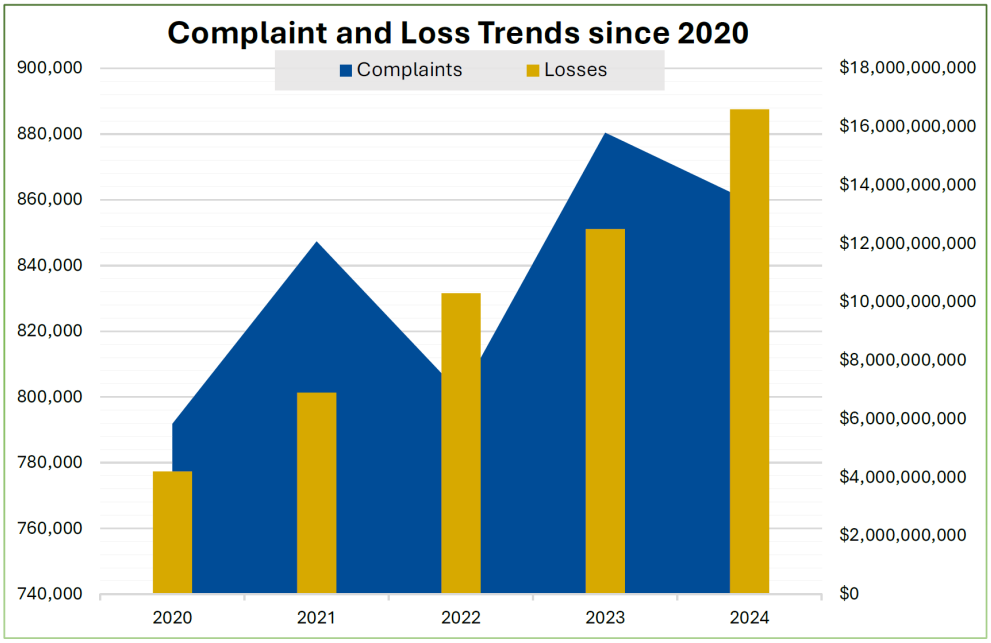

Figure 1. Complaints to IC3 over the last five years[5]

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 rise of investment scams was especially pronounced with an increase of 44% from 2023 of $4.57B to $6.57B.

While the top three scams rely on different mechanisms, impersonation is the common enabling factor. Impersonation scams can take many different forms, including a criminal pretending to be a financial advisor or romantic partner 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.

Impersonation scams directly affect banks and their customers. In April 2025, the Federal Trade Commission (FTC) published a Data Spotlight[6] that identified the top text messaging scams of 2024. Fake fraud alerts — often impersonating a bank — were the third most common type of scam.

Many people reported texts about so-called suspicious activity or a big purchase they did not make. These texts often look like they're from a bank or Amazon. They might give a number to call. Or they might say to reply YES or NO to verify a large transaction. People who reply are connected to the (fake) fraud department for "help" fixing the made-up problem.

Unfortunately, many times these types of scams impersonating public and private entities are aided by inadequate technology controls that allow the criminals to show a legitimate business or agency phone number and name on caller ID giving an air of authenticity to the criminal.

[5] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[6] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/04/top-text-scams-2024

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 duped into giving their money to criminals or mail gets stolen from a post office, there are limits to what banks can do.

To combat scams and fraud, a whole of ecosystem approach is necessary along with a focus on prevention. Banks constantly message their customers to only send money to people they know and trust, but criminals ability to impersonate individuals, digitally authenticate themselves with spoofed phone numbers and callerID data, and fake social media profiles enable them to build trust with their victims so that when they're ready to make a payment *they believe they know and trust* the criminal they are talking too. Prevention is worth a pound of cure and our approach to fighting scams must also include methods that prevent scammers from engaging with their potential victims.

We believe three key strategies are necessary to meaningfully combat the continued threat from scams and fraud:

1. **A whole of ecosystem approach where all participants in the scam lifecycle actively work to protect Americans.** Unlike financial institutions, which are legally required to verify customer identities and invest billions annually in fraud prevention, wireless providers and social media platforms have taken few steps to stop fraudsters from misusing their networks. By the time fraudulent activity reaches a financial institution, it is often too late to prevent consumer harm. This imbalance must end. Telecom and social media companies must share responsibility for preventing fraud before it reaches consumers. Legislation such as the bipartisan Safeguarding Consumers from Advertising Misconduct or SCAM Act (H.R. 7548/S.3774), and improved enforcement by the FCC on abusive communications service providers is essential.

2. **Establish a National Fraud and Scam Prevention Coordinator in the Executive Office of the President**. A centralized governmental lead needs to be established that can coordinate a "whole of government" response to protect Americans from scams and fraud with a focus on prevention and early intervention. One of the first tasks of this organization should be the development of a National Scam and Fraud Prevention Strategy that includes enactment of policies that allow timely information sharing within and across sectors and provides a safe harbor for those sharing information in a good faith effort to prevent harm to their customers.

3. **Grants for State and Local Financial Crime Intelligence Center**. 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.

In addition to these over-arching strategies the following specific measures are necessary:

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

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. Many banks have significantly increased their efforts to educate customers. For example, many provide tips for spotting scams in branches, customer communications, and websites. They also lead community workshops and provide timely warnings, telling customers to refrain from sharing passcodes or sending money to people they do not know, in addition to participating in ABA's cross-industry consumer education efforts

However, while banks can and do 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 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 actors 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 #BanksNeverAskThat[7] 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.

The public awareness campaign, developed with input from banks of all sizes across the country, educates consumers by posing ridiculous questions banks would never ask a customer. Using humor and bold graphics, we drive home the message that your bank will also never ask for your password, pin, social security number, or other sensitive information. ABA provides all campaign materials, free of charge, to any bank in the country interested in participating, so they can deliver the #BanksNeverAskThat messaging in their local markets.

The campaign has increased in size and scope each year. To date, more than 2,500 banks have participated in #BanksNeverAskThat and spread its educational content to millions of Americans

[7] www.banksneveraskthat.com

through social media, bank websites, ATM screens and bank branches across the country. ABA promotes the campaign nationally and anyone who has been to a Capitals, Wizards or Nationals game has probably seen our informational messages.

In 2023, ABA launched a Spanish language version of the campaign, available at www.BancosNuncaPidenEso.com. This year's campaign also features an interactive quiz, and short entertaining videos. The campaign has been recognized by federal, state, and local officials for its consumer protection message, and it has received numerous national awards for its creative approach. We've briefed other industry trade groups interested in launching something similar and are already planning for next year's campaign.

In 2024, to address the rising threat of check fraud, ABA launched the #PracticeSafeChecks companion campaign.[8] This public education effort uses humor and bold imagery to show consumers how to safely use checks if safer, digital payment options are not available. Like #BanksNeverAskThat, all campaign materials are provided at no cost to any bank in the country wishing to participate.

Combating Elder Fraud

In addition to its public outreach campaigns, ABA through the ABA Foundation[9] has active programs to specifically focus on protecting seniors from frauds and scams. Given the seriousness of the issues 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 developed a one stop resource page [10] to help banks protect older customers. It offers banks four sets of supports focused on banker training, leveraging technological solutions, fostering relationships with law enforcement and adult protective services, and consumer outreach and awareness. Among the tools available, banks can access an online elder financial exploitation prevention course and a free guide on "Protecting the Financial Security of Older Americans." This three-part guide is designed to help banks develop a framework on educating and engaging their communities on preventing elder financial exploitation.

Since 2016, over 2,550 banks have participated in the ABA Foundation's Safe Banking for Seniors program.[11] Through the free initiative, banks have access to turnkey materials to inform their communities about avoiding scams, choosing executors, financial caregiving, preventing identity theft, known perpetrator fraud, and understanding powers of attorney. Banks use the materials to help empower their communities and lead in-person and virtual workshops with millions of seniors, post videos and other content on social media, and share vital information during one-on-one conversations in branches. All the resources are available at no cost to ABA member and non-member banks.

---

[8] www.practicesafechecks.com

[9] The ABA Community Engagement Foundation, known as 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.

[10] https://www.aba.com/OlderAmericans

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

Through partnerships with the FBI, FTC, and United States Postal Inspection Services the ABA Foundation also developed infographics to raise awareness about scams that disproportionately affect older customers. Banks and non-banks alike can freely access and disseminate materials on: Check Theft and Check Washing, Cryptocurrency Confidence Scams, Fake Check Scams, Imposter Scams, Money Mule Scams, Online Dating Scams, Peer to Payments, and Phishing Scams.[12]

While ABA's campaigns have been instrumental in educating the public, we are just one voice. We need a nationwide message coordinated among multiple agencies (including the CFPB and FTC), nonprofits, and private companies 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.

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 reduce the amount of fraud Americans experience. 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* – Criminals have figured out loopholes that allow themselves 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 are coming 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 they are from their 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're 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.
- *Stolen or Spoofed Social Media Accounts* – The FBI reported that investment scams had the highest losses in dollars among all scams. 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 contact their connections to convince them to invest in fraudulent investment scams.

[12] https://www.aba.com/protect-your-money

Spoofing of Caller ID Information

The Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) caller ID authentication framework established by the Federal Communications Commission (FCC) is meant to help protect consumers from illegally spoofed robocalls by verifying that the caller ID information transmitted with a particular call matches the caller's telephone number.[13] Unfortunately, technical limitations of existing networks used, particularly non-IP networks, and calls originating from overseas communications providers have hampered the effectiveness of the framework, leaving loopholes that criminals can exploit to spoof the data (i.e., phone number) shown on a consumer's caller ID. Under STIR/SHAKEN, a call that receives an "A-level" attestation – the highest form of attestation – means the voice service provider originating the call (originating provider) knows the caller and knows the caller has the legal right to the number that will be displayed in the recipient's caller ID. If a call receives A-level attestation, it is eligible for vendors' call branding designed to signal that the call is from a legitimate source, such as green "checkmark."

But available data show that many A-level-attested calls are in fact illegally spoofed calls. In one analysis conducted for ABA of 12,900 calls that illegally spoofed telephone numbers belonging to 47 large banks, retailers, and healthcare providers, more than half of the calls received an A-level or B-level attestation. In another example, fraudsters placed six waves of illegal imposter calls (where the fraudster claimed to be a bank) to consumers over eight weeks between mid-September and mid-November; each wave consisted of over 500,000 illegal calls, for a total of 15 million estimated illegal calls. Significantly, over two-thirds of these calls received A- or B-level attestation.[14] To achieve a meaningful reduction in illegally spoofed calls, we have urged the FCC (1) to require voice service providers to follow robust and specific "know your customer" procedures before allowing a caller to place calls on the provider's network, and (2) to require the caller to demonstrate to the provider that the caller has the legal right to use the number that will be displayed in the recipient's caller ID display when the caller seeks to place an A-level attested call.[15]

Additionally, we believe that telecommunications providers who enable criminals to impersonate legitimate numbers and incorrectly authenticate their calls with impersonated numbers and company names should be held to account. We have expressed strong support[16] for the FTC's proposal to prohibit entities from providing the "means and instrumentalities" for another to impersonate a government or business.[17] We agree with the statement made by the National Association of Attorneys General in that proceeding that "when an entity provides substantial assistance or support to impersonators and knows or should have known that their products [or]

---

[13] https://www.fcc.gov/call-authentication

[14] *See In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Dismissal of Outdated or Otherwise Moot Robocalls Petitions*, CG Docket No. 17-59, 02-278, & 25-307, WC Docket No. 17-97, Comments of the American Bankers Association *et al.* 21 (filed Jan. 5, 2026), https://www.fcc.gov/ecfs/document/10106019480304/1

[15] *See id.* at 22.

[16] Letter from Am. Bankers Ass'n *et al.* to Lina Khan, Chair, Fed. Trade Comm'n (Dec. 16, 2022), "https://www.aba.com/advocacy/policy-analysis/impersonation-proposal-comment-letter/."

[17] Notice of Proposed Rulemaking and Request for Public Comment, Trade Regulation Rule on Impersonation of Government and Businesses, 87 Fed. Reg. 62,741, 62,751 (Oct. 17, 2022).

services are being used in a fraudulent impersonation scheme, that company could also be held liable under the proposed impersonation rule."[18]

The vast majority of telecommunications providers follow the law, but those who know or should know that they are enabling criminals to steal from Americans should be held accountable and be liable for the harms they enable.

Impersonation Text Messages

Texting has become a primary method of communication for Americans and criminals have shifted their tactics to "meet their customers where they are." ABA has focused on ensuring that banks have the tools to identify fraudulent texting trends quickly enough to prevent or mitigate customer harm. Unfortunately, banks are still encountering barriers as they seek to prevent fraudulent texts from reaching customers.

ABA has supported the FCC's efforts to combat illegal text messages, but we believe more needs to be done. With ABA's support, the FCC now requires "terminating mobile wireless providers" (providers that deliver calls to recipients) to investigate and potentially block texts from a sender after they are on notice from the agency that the sender is transmitting suspected illegal texts.[19] We have urged the FCC to apply this requirement to entities that originate text messages, as these entities are best positioned to stop illegal texts from being sent in the first place. Last spring, ABA identified "email-to-text" as a common method by which bad actors send large numbers of phishing or otherwise fraudulent messages because the bad actor can load consumers' cell phone numbers into an e-mail application to send these texts.[20] We support the FCC's December 2023 statement encouraging providers to make email-to-text an opt-in service—whereby consumers have the option whether they receive text messages that originated through an email platform.[21]

We also have urged the FCC to finalize a requirement that text messages be authenticated and set a deadline for the development and mandatory implementation of a text message authentication solution.[22] As described earlier, bad actors use numerous approaches to impersonate legitimate companies in text messages sent to consumers. The FCC should work with mobile wireless providers and other entities involved in the texting ecosystem to design an authentication framework that prevents bad actors from sending to consumers text messages that impersonate

[18] Comments of Nat'l Ass'n of Attorneys General 10 (Feb. 23, 2022), https://www.regulations.gov/ comment/ FTC-2021-0077-0164.

[19] *In the Matter of Targeting and Eliminating Unlawful Text Messages*, CG Docket No. 21-402, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Second Report and Order, Second Further Notice of Proposed Rulemaking in CG Docket Nos. 02-278 and 21-402, and Waiver Order in CG Docket No. 17-59, ¶¶ 16-25 (released Dec. 18, 2023) [hereinafter, *Second Report and Order*].

[20] Reply Comments of Am. Bankers Ass'n *et al.*, *In the Matter of Targeting and Eliminating Unlawful Text Messages*, CG Docket No. 21-402, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, at 8 (filed June 6, 2023), https://www.aba.com/advocacy/policy-analysis/joint-ltr-txt-msgs-lead-generators [hereinafter, ABA Reply Comments].

[21] *Second Report and Order*, *supra* note 17, at ¶ 86.

[22] ABA Reply Comments, *supra* note 18, at 10-11.

legitimate companies, while at the same time ensuring that text messages from legitimate companies are not blocked.[23]

Beyond creating an authentication regime for text messages, the FCC should provide banks with access to the information necessary to protect their customers from fraudulent texts. Currently, the telecommunications industry asks that the public forward scam texts to the short code 7726, which spells "SPAM" on your phone. It would be very helpful for banks to have access to the spam messages in order to identify those impersonating their bank and the fake phone numbers and links they are trying to get consumers to use. In fact, one bank worked with telecommunications companies to establish a pilot program whereby the bank gained access to and reviewed reported SPAM data. The bank then used that data to actively issue take-down requests to the relevant phone numbers and internet links that were in the messages so that they no longer functioned. Unfortunately, this program was discontinued because the telecommunication companies revoked the bank's access to the data.

We strongly urge policymakers ensure banks and other legitimate businesses are allowed to access, with appropriate privacy safeguards, data from scam/spam reporting services, whether it is the 7726 data, the "Report Junk" data in Apple's iMessage application, or other similar scam/spam reporting features in other closed messaging applications. Additionally, consideration should be given to requiring all significant messaging services to operate a "Report Spam" feature and be required to share that data so that businesses can protect their customers even if these messaging providers are unwilling to do so.

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.

According to a new survey conducted by Morning Consult[24] on behalf of the ABA, consumers support requiring social media and telecom companies to do more to fight fraud.

- Seventy-eight percent support federal legislation that requires social media companies to do more to identify and remove fake accounts and fraudulent ads from proliferating on their platforms. With the proliferation of scammers spoofing caller ID to impersonate trusted entities like banks, government agencies and law enforcement, 77% of consumers said they support regulatory action that requires telecommunications providers to do

[23] In designing an authentication framework, however, the Commission should recognize that legitimate companies frequently send text messages through "short code" text messages – a five- or six-digit number registered through CTIA's short-code registry that businesses use to send and receive text messages – or through a 10-digit number that is registered with a third-party aggregator. Short Code Registry, *Frequently Asked Questions*, https://www.usshortcodes.com/learn-more/faq (last visited May 2, 2023). The FCC should ensure that the framework adopted does not interfere unduly with these texts.

[24] https://www.aba.com/about-us/press-room/press-releases/morning-consult-survey-spring-2026-fraud

more to authenticate the identity of a caller and prevent spoofed caller IDs. The FCC is considering regulatory action in this area.

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.

ABA Urges Support for Bipartisan SCAM Act

ABA strongly supports a bipartisan bill in Congress, the Safeguarding Consumers from Advertising Misconduct or SCAM Act (H.R. 7548/S.3774), which would require social media companies to combat fraud more aggressively. The SCAM Act would combat fraudulent online advertisements by requiring online platforms to implement procedures to verify the identity of the advertiser before placing the advertisement. Platforms must also implement a program to detect impersonation on their site. If an individual, business, or government agency reports a fraudulent or deceptive advertisement, the platform must investigate the advertisement within 72 hours and, within 24 hours of completing the investigation, notify the reporter of the outcome of that investigation.

Paid advertisements are not neutral or passive user content. They are commercial products that platforms actively curate, target, and monetize. Platforms that profit from advertising should bear responsibility for preventing the dissemination of fraudulent paid ads.

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 cybersecurity and anti-fraud measures to provide one of the most secure banking systems in the world, but banks can't 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.

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 combatting financial crimes is shared information. However, due to different policy interpretations across financial institutions and lack of regulatory clarity, there are challenges in sharing actionable information in a timely manner.

The ABA is part of the International Banking Federation and is working to figure out processes to share information between banks both domestically and internationally. During the 2026 UN Global Fraud Summit the ABA in partnership with IBFed announced the expansion of the ABA Fraud Contact Directory to include international banks. While this is a simple capability, it can make a material difference if a bank can easily identify a contact at another bank when fraud has

occurred and increase the chance of funds recovery. The Directory currently includes contacts for over half of all US banks, and some credit unions, as well as a handful of international banks from the UK, Australia, the Netherlands and Canada, and the list is growing.

Additionally, many countries have systems that allow development of a risk score for an account based on different characteristics allowing a financial institution to identify potential risky transactions and require stepped up security measures prior to interacting with those accounts. Unfortunately, in the US there is no system that covers all accounts and there is currently no system that allows sharing in real-time across international boundaries. The ABA through the IBFed is attempting to identify different capabilities in this space and willing partners both domestically and abroad that are interested in piloting the sharing of this account information.

Partnership with Law Enforcement and Regulators

As 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. The ABA applauds the establishment of the Department of Justice's Scam Center Strike Force. This multi-agency task force launched in November 2025 focuses on combatting Southeast Asian-based organized crime syndicates and has already seen significant success. We believe this type of joint action between public and private entities and international governments are key to fighting scams and protecting Americans.

Additionally, ABA commends work by the FBI, United States Secret Service, and FinCEN to try and freeze funds that have been transferred fraudulently. The FBI IC3 Recovery Asset Teams have been great partners, but we are concerned that they may lack capacity to engage on 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. Congress has recommended similar efforts by the Treasury Department, as seen in a report accompanying a bipartisan Senate Appropriations bill approved Committee unanimously, last year, which urged the facilitation of a public-private partnership on fraud prevention.[25]

Americans are losing billions of dollars to fraud annually. Yet, amid resource constraints and competing 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 on 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. As such, we recommend strengthening the relationship between local law enforcement and federal agencies.

[25] See page 10; https://www.appropriations.senate.gov/imo/media/doc/fy24_fsgg_report.pdf

Moreover, while the losses Americans experience goes to US-based criminals, large amounts are being transferred overseas and potentially by and to those who threaten our national security. The lack of a centralized fraud response and tracking capability within the US government hinders the ability to spot trends, track tactics, techniques and procedures, and the ability to recover funds for Americans when fraud has been identified. Additionally, there is no central agency with which banks can work on innovative programs to defeat fraud and recover funds.

Conclusion

Banks are working every day to protect their customers from fraud by investing in new technologies, deploying public awareness 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 can't 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 America's banks are ready to help protect our customers from fraud.