Testimony of
Paul Benda

On Behalf of the
American Bankers Association

Before the
United States Senate Committee on Banking, Housing, and Urban Affairs

February 1, 2024

Chairman Brown, Ranking Member Scott, and members of the committee, thank you for the opportunity to testify today for a hearing "Examining Scams and Fraud in the Banking System and Their Impact on Consumers." My name is Paul Benda, and I serve as Executive Vice President, Risk, Fraud and Cybersecurity for the American Bankers Association (ABA). The American Bankers Association is the voice of the nation's $23.4 trillion banking industry, which is composed of small, regional, and large banks that together employ approximately 2.1 million people, safeguard $18.6 trillion in deposits, and extend $12.3 trillion in loans. 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, 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.

A recent 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 tools 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[3] to receive and move the funds. They are also becoming more sophisticated, using new advanced deepfake

[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.

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.

These criminals can't 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 won't get intercepted, stolen, altered and cashed by the criminal. Most importantly, 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 punishments must match the crime, so these offenders won't 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. One recent industry analysis found that Financial Services, which is a category that includes more than just banks, account for only 5.4% of ransomware attacks in Q3 2023.[4] Unfortunately, bank customer losses from scams and fraud have been increasing significantly. 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.[5] This data is limited to certain types of fraud, and therefore 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 2022 Internet Crime Report ("the Report"), released in March 2023, data showed a nearly 50% increase in losses reported by consumers and businesses from 2021 to 2022.

[4] https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals
[5] www.ic3.gov

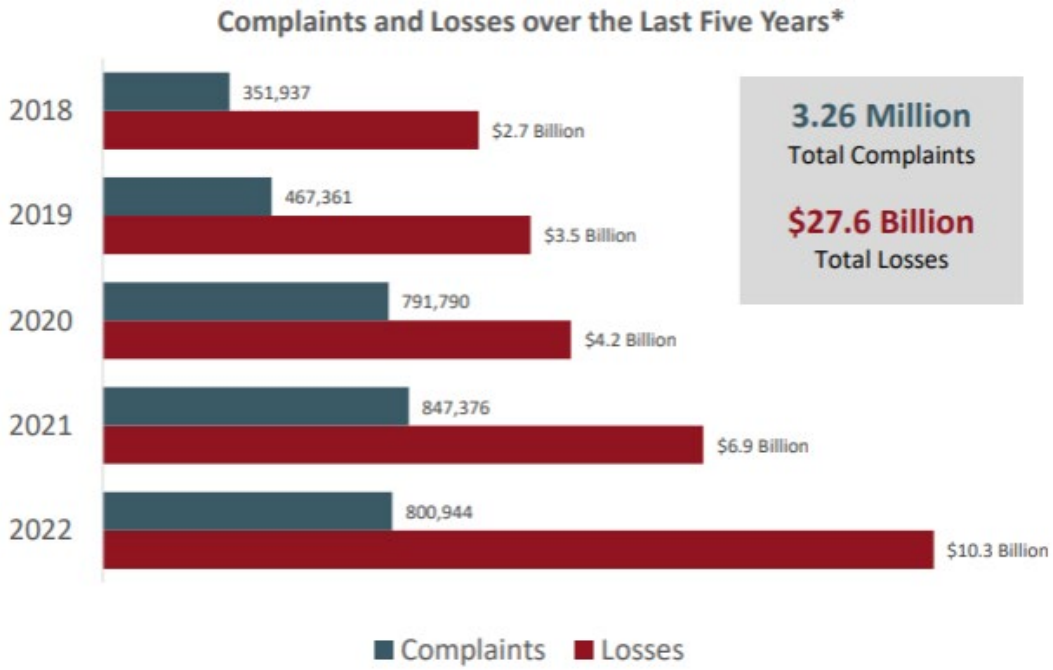

Figure 1. Complaints to IC3 over the last five years[6]

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 127% from 2021 of $1.45B to $3.31B lost.

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 June 2023 the Federal Trade Commission (FTC) published a Data Spotlight[7] that identified the top text messaging scams of 2022. The top scam was an impersonation scam—which is often in the form of a fake fraud alert from a bank:

> Reports about texts impersonating banks are up nearly twentyfold since 2019. You might get a fake number to call about supposed suspicious activity. Or they might say to reply "yes or no" to verify a large transaction (that you didn't make). If you reply, you'll get a call from the (fake) fraud department. People say they thought the bank was helping them get their money back. Instead, money was transferred out of their account. This scam's median reported loss was a whopping $3,000 last year.

[6] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[7] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

It's not just the private sector that is being impersonated. Just this year the Consumer Financial Protection Bureau (CFPB) became the victim of an imposter scam, confirming that "scammers are using CFPB employees' names to try to defraud members of the public. We've heard from people, specifically older adults, who received phone or video calls."[8] 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.

Though losses from the internet and impersonation-based scams are most prominent, check fraud has become one of the fastest-growing categories of fraud impacting consumers across the country. However, as noted above, it is extremely difficult to gather the actual volume of check fraud being perpetrated as there is no central repository of data. The IC3 does provide some data, but it combines check and credit card fraud for a value of $264M for 2022. Judging by what we are hearing from our members, this very likely under-represents the actual volumes of check fraud; one bank alone has reported losses of over $100M in a single quarter due to check fraud.

In order to determine if the anecdotal growth being reported is accurate, we must cross reference it with trend data. Treasury's Financial Crimes Enforcement Network (FinCEN)— charged with collecting and analyzing information about financial transactions to combat money laundering and financial crimes, including confidential Suspicious Activity Reports (SARs) banks are legally required to file—provides one such source. FinCEN categorizes and tracks the types of SARs being filed and the growth of check fraud-related reports by banks and other financial institutions has become so substantial that early last year FinCEN published an alert on the "Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail." The alert states:

> 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.[9]

Even though the exact dollar value of fraud being committed can't 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. Attacking these trends requires work in the following areas:

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

[8] https://www.consumerfinance.gov/about-us/blog/beware-of-new-cfpb-imposter-scams/
[9] https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf

- *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 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 significant churn in personnel that occurred as a result of the pandemic created very significant operational challenges for banks, resulting in processing delays for check fraud claims.

Banks are working diligently to reduce current timelines and improve the overall experience for customers. In the majority of instances, and assuming a customer reports the fraud promptly, they are not liable for a fraudulent check and the bank will make them whole. The process requires the bank that accepted the check for deposit (bank of deposit) and the bank that issued the check (the paying bank) to work out liability under applicable state law and contractual agreements. This is achieved in a number of ways, depending on the reason the check is unpayable. For certain claims, the paying bank whose customer has notified them of a fraudulent check will file a check warranty breach claim with the bank of deposit. Given the wide range of banks involved, one of the biggest challenges is determining a point of contact with which to exchange a claim.

Recognizing this challenge, in 2023 ABA worked collaboratively with other industry groups to establish a check fraud working group focused on expediting the processing of check fraud claims. Among other things, the working group exchanged points of contact and documentation requirements to process a claim. And while the working group focused on the banks handling the vast majority of claims, its success has resulted in ABA developing an online check fraud directory that any bank—whether an ABA member or not—can access for free as long as they reciprocate and provide their contact information. In just over six months the directory has grown to nearly 1,700 banks, and we have heard from banks how invaluable this resource is in speeding up the claim processing timeline. Our job is not done yet, and we continue efforts to expand the number of participating banks in the directory.

In addition to the directory, the check fraud working group has undertaken efforts to improve the overall claims process for banks and customers alike, including:

- Drafting a Universal Warranty Breach Claim form to help standardize the required information for a claim, reducing duplicative submissions.
- Reducing burdensome documentation hurdles by encouraging banks to drop notarization requirements.
- Making it easier to file a claim if a customer's stolen check was going to pay a recurring bill to a large company (e.g., an electric utility) by not requiring the normally standard affidavit from the utility, which can be very difficult for the consumer to obtain.
- Developing industry baselines for notifying the paying bank when a claim was received, assigning it a claim number, and providing an estimated time for processing.
- Attempting to standardize the time after a claim has been adjudicated and paid out, which can vary significantly.

The processing of check warranty breach claims is surprisingly complex and difficult, but banks and the ABA are committed to improving the system.

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 education of customers. For example, many provide tips for spotting scams in branches, customer communications, and websites and provide timely warnings that customers not share passcodes or send money to people they do not know, in addition to participating in ABA's cross-industry 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 actors or nonprofits, to partner with us to amplify the important work banks are doing to educate consumers on fraud.

Stopping Phishing

One of ABA's most important consumer protection initiatives is our #BanksNeverAskThat[10] 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 hope to drive home the message that your bank will also never ask for your password, pin or social security number. ABA provides all of the 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 2,300 banks have participated in #BanksNeverAskThat and spread its educational content to millions of Americans through social media, bank websites, ATM screens and bank branches across the country. ABA has promoted the campaign nationally and anyone who has been to a Capitals, Wizards or Nationals game has probably seen its education message.

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, an educational video game 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.

[10] www.banksneveraskthat.com

Combating Elder Fraud

In addition to its public outreach campaign, ABA through the ABA Foundation has active programs to protect seniors from 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 Community Engagement Foundation, known as the ABA Foundation, is a 501(c)3 corporation that helps banks and bankers make their communities better. Through its leadership, partnerships and national programs, the Foundation supports bankers as they provide financial education to individuals at every age, elevate issues around affordable housing and community development and achieve corporate social responsibility objectives to improve the well-being of their customers and communities.

The ABA Foundation offers banks a free toolkit on "Protecting the Financial Security of Older Americans." This three-part resource is designed to help banks develop a framework on educating and engaging their communities on preventing elder financial exploitation.

Since 2016, more than 1,850 banks have participated in the ABA Foundation's Safe Banking for Seniors program.[11] Through the free initiative, participating 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 a combination of in-person and virtual workshops, post videos and other content on social media, and share vital information during one-on-one conversations at teller stations. All the resources are available at no cost to ABA member and non-member banks.

Through a prior partnership with the FTC, 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: Fake Check Scams, Government Imposter Scams, Imposter Scams, Money Mule Scams, Online Dating Scams, Phishing Scams, and Peer to Payments.[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:

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

[12] https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money

- *Spoofing of Caller ID* – Criminals 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 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. 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 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. We appreciate that the FCC continues to make progress in fully implementing STIR/SHAKEN across all networks. Nonetheless, ABA strongly believes that more needs to be done. Only callers whose calls are fully authenticated—signed at origination and attested throughout the call's pathway—should be able to display data in the recipient's caller ID display. If at any point the authentication cannot be validated, the caller ID should simply display "unknown caller." We recognize that due to technical limitations some legitimate callers may have their caller ID data dropped, but we believe erring on the side of caution is the best course due to the vast scale of impersonation fraud being committed.

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[14] for the FTC's proposal to prohibit entities from providing the "means and instrumentalities" for another to impersonate a government or business.[15] We agree with the statement made by the National Association of Attorneys General in that

---

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

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

[15] 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).

proceeding that "when an entity provides substantial assistance or support to impersonators and knows or should have known that their products [or] services are being used in a fraudulent impersonation scheme, that company could also be held liable under the proposed impersonation rule."[16]

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.[17] 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.[18] 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.[19]

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.[20] 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

---

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

[17] *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*].

[18] 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].

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

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

bad actors from sending to consumers text messages that impersonate legitimate companies, while at the same time ensuring that text messages from legitimate companies are not blocked.[21]

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.

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 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

---

[21] 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.

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 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 predicate 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.

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.

For example, ABA and the U.S. Postal Inspection Service (USPIS) are entering into a formal partnership to combat check fraud. It is often publicized that the increase in check fraud is partly due to criminals targeting the U.S. mail infrastructure by stealing mailed checks and altering ("washing") them, leading to fraudulent transactions at banks.

This agreement builds on our current partnership—dating back to early 2022—when we began joint training initiatives to proactively address fraud: USPIS briefings for ABA-hosted fraud information sharing groups, participation in ABA webinars, and platforms at ABA conferences. Drawing on USPIS and ABA's respective resources and reach allows us to educate the public and bank and Postal employees with joint training and red flag alerts at a greater scale.

ABA and USPIS will kick off this new partnership by hosting a free webinar for banks with the USPIS on ways they can collect evidence and support criminal investigations. Following this webinar, ABA and USPIS will distribute co-branded materials to educate bank customers and consumers on how to spot and report on common check fraud activity.

ABA also applauds efforts by other agencies to educate the public regarding fraud and scams. We lead a committee on the FTC's Stop Senior Scams Advisory Group focused on the freezing and recovery of fraudulent transfers, are active in the Federal Reserve Bank of Boston's Scams Definition and Information

Sharing Working Group and have worked with CFPB on elder fraud prevention tools such as trusted contacts adoption among depository institutions and powers of attorney.[22]

There are more opportunities for agencies to improve consumer education about scams. For example, Congress established a Financial Education Office in the Consumer Financial Protection Bureau with a statutory mandate to "be responsible for developing and implementing initiatives intended to educate and empower consumers to make better informed financial decisions."[23] We encourage the CFPB to prioritize using this office's resources to help consumers detect and avoid scams and would welcome an opportunity to work collaboratively, as we have done with the FCC, FTC, FBI, USPIS.

While agencies can also effect fraud prevention through their regulatory actions, we urge them to take care not to impede or inhibit banks' fraud prevention efforts. For example, recently the CFPB outlined changes it is considering to regulations implementing the Fair Credit Reporting Act (FCRA), which could have a significant impact on banks' work to detect and prevent fraud, identity theft, and other financial crimes.[24] Among these, the CFPB is contemplating narrowing the permissible purposes for which information can be used under the FCRA, treating consumer-identifying information (including name, address, and social security number) as a consumer report subject to the FCRA, while expanding who could be considered a consumer reporting agency to potentially include vendors banks rely on to assist with fraud prevention. Doing so could create new legal, practical, and procedural difficulties for banks that use this information to detect and prevent fraud and crime. Indeed, a Small Business Regulatory Enforcement Fairness Act (SBREFA) that reviewed the CFPB's potential policies for their impact on small entities specifically recommended that the CFPB carefully consider the impacts on fraud prevention and detection, identity verification, and law enforcement and "consider … ways to mitigate any negative effects."[25] It is important that the CFPB and other regulators consistently evaluate how each policy they consider may impact banks' efforts to detect and prevent fraud.

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 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.[26]

---

[22] https://files.consumerfinance.gov/f/documents/cfpb_trusted-contacts-fis_2021-11.pdf

[23] Dodd-Frank Act Wall Street Reform and Consumer Protection Act, 12 USC 5493 § 1013(d).

[24] CFPB, Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration (Sept. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf

[25] Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Consumer Reporting Rulemaking (Dec. 15, 2023) at 47-48, https://files.consumerfinance.gov/f/documents/cfpb_sbrefa-final-report_consumer-reporting-rulemaking_2024-01.pdf

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

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.

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 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 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. I look forward to answering your questions.