Statement for the Record

On Behalf of the

American Bankers Association, Bank Policy Institute,

Consumer Bankers Association, and National Bankers Association

Before the

Permanent Subcommittee on Investigations

Of the

U.S. Senate Committee on Homeland Security and Governmental Affairs

July 23, 2024

Statement for the Record

On Behalf of the

American Bankers Association, Bank Policy Institute,

Consumer Bankers Association, and National Bankers Association

Before the

Permanent Subcommittee on Investigations

Of the

U.S. Senate Committee on Homeland Security and Governmental Affairs

July 23, 2024

Chairman Blumenthal, Ranking Member Johnson, and distinguished Members of the Committee, the American Bankers Association[1] (ABA), the Bank Policy Institute[2] (BPI); Consumer Bankers Association[3] (CBA), and the National Bankers Association[4] (NBA) (hereinafter, Associations) appreciate the opportunity to submit a statement for the record for the July 23, 2024, hearing: "Instant Payments, Instant Losses: Zelle and the Big Banks Fail to Protect Consumers from Fraud."

Introduction

From using breakthrough technologies such as generative artificial intelligence (AI) to old fashioned theft of checks out of mailboxes, criminals are relentless in their efforts to steal money from the bank accounts of consumers and small businesses. As outlined in our May 21, 2024, statement for the record[5], banks have a long history of improving and innovating to protect their customers, including the adoption of chip-enabled credit cards, the use of multi-factor authentication to protect user accounts, and the use of advanced AI tools to prevent and warn customers about potentially fraudulent transactions. Banks work tirelessly to identify and report suspicious accounts to law enforcement; to help educate and warn their

[1] The American Bankers Association is the voice of the nation's $24 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $19 trillion in deposits and extend $12.4 trillion in loans.

[2] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. The Institute produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues.

[3] The Consumer Bankers Association is the only national trade association focused exclusively on retail banking. Established in 1919, the association is a leading voice in the banking industry and Washington, representing members who employ nearly two million Americans, extend roughly $3 trillion in consumer loans, and provide $270 billion in small business loans.

[4] Founded in 1927, the National Bankers Association is the voice for the nation's minority depository institutions (MDIs), and the only organization focused solely on the survival and strengthening of MDIs. Its members include Black, Hispanic, Asian, Pacific Islander, Native American, and women-owned and -operated banks across the country, all working to help communities who are underserved by traditional banks and financial service providers. MDIs are located in 32 states and territories. Learn more at nationalbankers.org.

[5] Statement for the Record on Behalf of the American Bankers Association, Bank Policy Institute, Consumer Bankers Association, and National Bankers Association before the Permanent Subcommittee on Investigations of the U.S. Senate Committee on Homeland Security and Governmental Affairs, May 21, 2024 https://www.aba.com/advocacy/policy-analysis/sfr-fraud-alert-zelle

customers about common scams, and to root out accounts that have been used by criminals. Banks, however, cannot win this fight on their own—it is going to take a cross-industry effort to stay ahead of fraudsters and scammers.

The activities of these criminals touch more than just the banking industry, and the efforts to counter frauds and scams must similarly be cross-industry. Each step in the scam ecosystem—from how a scammer identifies consumer targets, to how a scammer communicates instruction to a victim, to how the money is processed—offers an opportunity to stop the flow of funds to the criminal. Focusing on only one aspect or one step in the process will not stop this surge of scams. Rather, a holistic approach to address all the entities and elements of a scam has the best chance of being successful.

Banks are but one contributor to the overall safety and security of the payments ecosystem, and cannot single-handedly prevent criminals from defrauding consumers or financial institutions. Government must also play a role to protect the payments ecosystem. Banks are investing heavily in new technologies and capabilities to try to thwart criminals, and some hold great promise, but when customers are deceived into transferring their money to criminals or mailing packages containing checks or sensitive consumer information is stolen from a post office, there are limits to what banks can do to protect consumers. Reversing this trend requires work in the following areas:

1. Enhancing collaboration with law enforcement and regulators[6]
2. Increasing consumer education
3. Developing a national strategy for scam and fraud prevention and response
4. Involving other sectors to protect consumers from scams
5. Preventing risky data scraping practices
6. Facilitating improved information sharing

Enhancing Collaboration with Law Enforcement and Regulators

The rising tide of fraud cannot be fixed by banks alone. The criminals executing this fraud need to be caught, prosecuted, and sentenced so that they no longer commit these crimes. Banks have a history of partnering with law enforcement and the public sector on education and outreach activities along with identifying potential improvements in addressing fraud.

Some of the losses Americans experience goes to US-based criminals, but 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, as well as the ability to recover funds for Americans when fraud has been identified.

We applaud efforts by government agencies to educate the public regarding fraud and scams. The banking industry participates in both proactive and reactive initiatives through various agency projects such as the FTC's Stop Senior Scams Advisory Group, the Federal Reserve Bank of Boston's Scams Definitions and

[6] Read more in February 1, 2024, testimony before the Senate Banking Committee for a hearing titled "Examining Scams and Fraud in the Banking System and Their Impact on Consumers," where ABA provided a comprehensive summary of the challenges fraud poses for consumers and the industry across the board and includes detailed suggestions and action items to accomplish this goal. See: https://www.aba.com/advocacy/policy-analysis/aba-testimony-on-scams-and-frauds-in-banking-system

Information Sharing Working Group and the CFPB's activity on elder fraud prevention tools.[7] We continue to support work on innovative programs to defeat fraud and recover funds.

While agencies can also affect fraud prevention through their regulatory actions, we urge them to take care not to impede or inhibit banks' fraud prevention efforts.[8] 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 we applaud 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 by Committee unanimously last year, which urged the facilitation of a public-private partnership on fraud prevention.[9]

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. **Consideration should be given to establishing a grant program for state, local and tribal law enforcement focused on financial crimes, including fraud, and appropriate ways to support victims of financial crimes. Additionally, this strategy should include consideration of ways to increase the number of prosecutions of those who commit financial crimes.**

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 and check fraud. As such, we recommend strengthening the relationship between local law enforcement and federal agencies to facilitate this training and education.

---

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

[8] 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.[8] 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." See: https://files.consumerfinance.gov/f/documents/cfpb_sbrefa-final-report_consumer-reporting-rulemaking_2024-01.pdf

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

Increasing 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 customer education efforts. For example, many provide tips for spotting scams in branches, via customer communications, and through bank websites and provide timely warnings that customers should not share passcodes or send money to people they do not know, in addition to participating in cross-industry consumer education efforts.

People need to hear from other sources as well, though, and we encourage other trusted sources, such as government agencies or nonprofits, to partner with us to amplify the important work banks are doing to educate consumers on fraud. For example, many banks partner with advocacy groups like AARP to provide education around bank fraud for the elderly, offering targeted resources and support to help seniors recognize and avoid scams.

However, 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."[10] **We encourage the CFPB to prioritize using this office's resources to help consumers detect and avoid scams~~,~~ welcome an opportunity to work collaboratively, as we have done with the FCC, FTC, FBI, USPIS and the Treasury Department.**

Stopping Phishing

Every day, thousands of people fall for fraudulent emails, texts, and calls from scammers impersonating a bank. These are commonly referred to as phishing scams and victims can lose hundreds, even thousands of dollars. ABA launched #BanksNeverAskThat,[11] an anti-phishing campaign in October 2020, to turn the table on fraudsters by empowering consumers to spot bogus bank phishing scams.

The campaign has increased in size and scope each year with more than 2,300 banks participating to date and spreading its educational content to millions of Americans through social media, bank websites, ATM screens and bank branches across the country. 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. An updated version of the successful campaign will launch in the fall of 2024 and be available to all banks.

Combating Elder Fraud

Older adults are a growing population in the United States as well as a growing target for scams. Elder fraud is the fastest-growing form of elder abuse, and is defined as the illegal, unauthorized, or improper use of an older person's funds, property, or assets.[12] It's a crime that deprives older adults of their resources and ultimately their independence. In 2023, IC3 received reports of over $3.4 billion in losses from people aged 60 and older, representing an almost 11% increase from 2022.[13] As such, safeguarding the financial assets of older Americans is a top priority for banks of all sizes across the country.

---

[10] Dodd-Frank Act Wall Street Reform and Consumer Protection Act, 12 USC 5493 § 1013(d).
[11] See: www.banksneveraskthat.com
[12] See: https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf
[13] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf

For example, ABA through the ABA Foundation[14] 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.

Since 2016, more than 1,930 banks have participated in the ABA Foundation's Safe Banking for Seniors program.[15] Through the free initiative, participating banks have access to turnkey materials to inform their communities about avoiding scams, 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, 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 alike.

In addition to encouraging public education and outreach, the banking industry partners with federal agencies to combat frauds and scams. For example, in collaboration with the FBI, the ABA developed a reference guide for banks about recognizing, responding to, and reporting elder fraud, and is partnering with the United States Postal Inspection Service to combat check fraud and money mule scams, which disproportionately affect older people.

Developing A National Strategy for Scam and Fraud Prevention And Response

While industry campaigns and partnerships[16] with federal agencies have been instrumental in educating the public, we are just one voice. Fraud and scams are costing consumers billions of dollars each year and current Federal activities are disjointed and uncoordinated, lacking an overarching strategy. **A National Scam and Fraud Prevention strategy is vital to develop and implement a coordinated Federal approach focused on stopping consumers from being scammed in the first place and developing solutions to assist consumers once the scam has been perpetrated.**

A comprehensive strategy that addresses all parts of the fraud ecosystem is necessary to reduce the number of Americans being scammed. The strategy should include developing or strengthening capabilities that reduce the ability of criminals to be "technologically authenticated" through the use of impersonated social media accounts or spoofed/fake Caller ID messages. Messages that impersonate a legitimate company allow the criminals to show the name of a trusted company, such as a bank, and hide the fact that the consumer is talking to a criminal--not the bank that their phone display shows. These efforts need to be coordinated amongst multiple regulators and be reported to law enforcement so that when these schemes are discovered, law enforcement is made aware and appropriate action is taken.

---

[14] 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.

[15] See: https://www.aba.com/seniors

[16] One example of such a partnership is between bank associations and P2P providers like Zelle, launching anti-fraud educational social media campaigns. Zelle will provide the content, and the associations will distribute to their audience and member banks to raise awareness and equip users with the knowledge to protect themselves from online scams.

Additionally, coordination among all the agencies that are fighting financial crime and gathering information is essential. Consumers are asked to report fraud to the FBI, to the FTC, to the CFPB, to their local police, etc., which can create confusion among consumers and can result in siloed data.

We recommend a single streamlined and centralized government reporting process for consumers. First, it would help law enforcement efforts if there was comprehensive, centralized reporting of fraud losses. Additionally, bank customers should be incentivized to report fraud losses to their banks as soon as possible. If the fraud is reported immediately, there is a better chance of potentially recovering the funds. A centralized collection point would facilitate improved sharing of information among the government and private sector partners, enabling them to better identify trends and the source of scams so that the numbers and websites being used to perpetuate these scams can be blocked.

Not only is more information sharing needed regarding consumer reported scams, but also a strategy is needed to improve sharing of sensitive information that could help both the government and banks to identify the accounts used to facilitate the flow of fraudulent funds and shut them down. As part of their Bank Secrecy Act (BSA) compliance obligations, banks report millions of suspicious activity reports (SARs) to Treasury's Financial Crimes Enforcement Network (FinCEN) every year. In addition, banks may choose to share information with other banks and other financial institutions under FinCEN's Section 314(b) information sharing rules. A coordinated strategy is needed to remove barriers, both perceived and real, that can hamper the sharing of critical information. The faster information is shared, the better the chance these accounts can be identified and blocked, and law enforcement will have better tools to detect, investigate and prosecute criminal actors, and increase the likelihood that customers' funds may be recovered.

Better knowledge of the fraud being perpetrated and better information sharing between banks and the government will allow the development of new mitigation strategies to protect consumers and catch criminals. The goal of a National Scam and Fraud Prevention strategy should be to stop the fraud from happening in the first place so that no consumer has to go through the trauma of losing their savings, and no funds go to these criminal enterprises.

Part of the strategy should include an education component. Similar to other countries, the US should develop a nationwide anti-scam message coordinated among multiple agencies (including the CFPB and FTC), nonprofits, and private companies that promotes a simple and memorable action plan for people of all ages facing scams. The campaign should also focus on identifying and exposing the behavioral techniques scammers use in impersonating authorities, indicating urgency, requiring secrecy, and manipulating people into action. An education campaign should also work to destigmatize falling victim to fraud and scams so as to encourage more reporting of fraud and scams by consumers.

Involving Other Sectors to Protect Consumers from Scams

Limiting criminals' ability to impersonate legitimate businesses or government agencies is critically important to reduce the amount of fraud Americans experience. It is far too easy for criminals to misrepresent themselves 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 legitimate accounts.

Currently, technology enables criminals to impersonate legitimate actors through three primary channels:

- *Spoofing of Caller ID* – Criminals "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 the caller is from their bank.

- *Impersonation Text Messages* – Criminals use email-to-text tools to create text messages that look like they come from a bank, or they use similar numbers and formats to pretend they're from a bank. These can include links to fake bank websites, call back numbers, or messages that state a bank representative will call the customer (after which the fraudster calls the customer and uses social engineering to persuade the customer to give up security credentials or send money from their account).
- *Stolen or Spoofed Social Media Accounts* – The FBI reports that investment scams have 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.[17] 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, our Associations strongly believe that more needs to be done. Specifically, we call on the FCC and wireless providers to take the following actions**:

First, regulators should take action to prevent 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. Two regulators—the FCC and FTC—are well situated to address this problem. The FCC should prohibit the practice by voice service providers of displaying data on the consumer's caller ID device even when the authenticity of calls cannot be adequately verified. 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 committed against Americans.[18]

For its part, the FTC should finalize its proposal to make it unlawful to provide goods or services "with knowledge or reason to know" that those goods or services will be used to spoof a government or business.[19] We agree with the statement made by the National Association of Attorneys General that "when an entity provides substantial assistance or support to impersonators and knows or should have

[17] See: https://www.fcc.gov/call-authentication
[18] See: https://www.aba.com/advocacy/policy-analysis/ltr-fcc-eighth-npr-call-blocking.
[19] See: https://www.federalregister.gov/documents/2024/03/01/2024-04335/trade-regulation-rule-on-impersonation-of-government-and-businesses

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."[20] Using this authority, the FTC should impose liability on voice service providers that provide consumers with unauthenticated or falsified Caller ID information in the consumer's Caller ID display.[21]

Second, the FCC should increase enforcement of voice service providers that improperly sign calls with "A-level" attestation. Under the STIR/SHAKEN call authentication framework, a call may receive "A-level" attestation—the highest level of attestation available—if the originating voice service provider can verify the caller's identity and verify that the caller has lawful access to the number that is displayed in the recipient's caller ID. A large bank ABA member reported that voice service providers are improperly signing outbound calls with A-level attestation without verifying the caller's identity or that the caller has lawful access to the number that is displayed in the recipient's caller ID.

Third, the FCC should require non-IP network providers to implement a commercially available call authentication solution within one year. To prevent illegal number spoofing, the FCC requires IP-based originating providers to attest to the authenticity of the telephone number that will be displayed in the recipient's caller ID.[22] Each intermediate provider in the call path that has an IP network must pass this STIR/SHAKEN attestation information to the next downstream IP-based provider until the call reaches the terminating provider. However, because STIR/SHAKEN only works on IP networks, any non-IP network in the call chain will prevent the STIR/SHAKEN attestation from being transmitted. Evidence suggests that the presence of non-IP networks is substantially undermining the STIR/SHAKEN framework by allowing calls to be delivered to the recipient without authentication.[23] Therefore, the investment by network providers and others to implement STIR/SHAKEN is being undermined by the continuing prevalence of unauthenticated non-IP networks, and the laudatory goal of STIR/SHAKEN to prevent illegal number spoofing is not being met.

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." Our Associations have worked to ensure 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.

The Associations support the FCC's efforts to combat illegal text messages, but we believe more needs to be done. The FCC now requires "terminating mobile wireless providers" (providers that deliver calls to recipients) to investigate and potentially block texts from a sender after the provider is on notice from the

[20] See: https://www.regulations.gov/comment/FTC-2021-0077-0164
[21] For additional discussion see:https://www.aba.com/advocacy/policy-analysis/joint-ltr-impersonation-of-banks.
[22] 47 C.F.R. § 64.6301.
[23] TransNexus (a provider of telecommunications solutions) found an increase between January and August 2022 in the number of providers "signing" calls under the STIR/SHAKEN call authentication framework. Yet, in each month during this time period, only 24% of calls that were delivered to recipients included STIR/SHAKEN call authentication information. For the remaining calls, either the call was not signed at origination or that signature was lost during the call's transit, indicating that non-IP networks may be preventing the transmission of the attestation information. Reply Comments of TransNexus, CG Docket No. 17-59, WC Docket No. 17-97, at 6 (rec. Sept. 16, 2022), https://www.fcc.gov/ecfs/document/10916337622768/1.

agency that the sender is transmitting suspected illegal texts.[24] **We urge 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.[25]** In spring 2023, 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.[26] The Associations 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.[27]

We also urge 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.[28] As described earlier, bad actors use numerous approaches to impersonate legitimate companies in text messages sent to consumers. In September 2022, the FCC tentatively concluded that mobile wireless providers should implement caller ID authentication for text messages.[29] However, the FCC has not moved forward with mandating caller ID authentication even though there is consensus that identity spoofing (not number spoofing) is a key problem.[30] Policymakers should focus on authenticating the text sender rather than simply extending the STIR/SHAKEN caller ID authentication framework to the SMS ecosystem. We urge the FCC to require mobile wireless providers to provide the Commission with updates, on a set schedule, of the nature and status of providers' work to develop and implement solutions to provide authentication of text senders. As necessary and feasible, the FCC should develop firm deadlines for providers to deploy authentication technologies.[31]

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 the public to 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

---

[24] *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*].

[25] See: https://www.aba.com/advocacy/policy-analysis/joint-comments-to-fcc-on-tcpa-2024, and https://www.aba.com/advocacy/policy-analysis/joint-ltr-txt-msgs-lead-generators.

[26] 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].

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

[28] See: https://www.aba.com/advocacy/policy-analysis/joint-ltr-txt-msgs-lead-generators

[29] *Targeting and Eliminating Unlawful Text Messages*, Notice of Proposed Rulemaking, FCC 22-72, CG Docket No. 21-402, ¶¶ 28-36 (released Sept. 27, 2022).

[30] See: https://www.fcc.gov/ecfs/document/10606087722721/1 (and https://www.fcc.gov/ecfs/document/1209746509660/1.

[31] 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. The FCC should ensure that the framework adopted does not interfere unduly with these texts.

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 to 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 the 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 by 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.

The Associations strongly urge 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 pose as trusted agents must help as well. The criminals have realized the challenges to 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.

Preventing Risky Data Scraping Practices

Efforts to prevent fraud reflect the bank's focus not only on the transaction, but the access to the platforms to even conduct the transactions. However, even with the use of one-time-passcodes, out-of-band authentication and/or biometrics, the current environment continues to require default authentication steps that are knowledge based. These authentication steps exist when the customer has difficulties with mobile or digital platforms and is often used in our more vulnerable populations. In this process, the banks attempt to use information that should be private to authenticate their client's identity through knowledge based questions. However, the proliferation of social media and public data sharing has significantly exposed previously private information.

Criminals have become adept at pulling together the information the client shares on unrelated sites to determine answers to challenges in a knowledge based multi-factor authentication. In addition, this information may lead to compromises with their phone service provider creating a risk of taking over their device. This could allow another path to circumvent bank controls. Many of these sites' terms of use agreements do not permit scraping software, but these provisions are not routinely enforced. While some legitimate companies also web scrape for certain reasons, this practice is not consistent with end-users' expectations nor the policies of the websites themselves. Accordingly, this practice should be prohibited.

In addition, the practice of screen scraping in the consumer-permissioned data sharing ecosystem (otherwise known as open banking, personal financial data rights, or Section 1033) is inherently dangerous from a privacy and security standpoint. The CFPB is currently engaged in rulemaking on this issue which could eventually ban screen scraping and mandate safer means such as application programming interfaces (APIs).[32] **The CFPB's rules must take steps to ensure that consumer data is protected whether it is held by a bank or nonbank in the consumer-permissioned data sharing ecosystem and apportion liability to help incentivize robust consumer data protection by nonbanks that are not subject to the same requirements or oversight regarding data security.**

Facilitating Improved Information Sharing

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 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 crimes.

Peer-to-Peer (P2P) Fraud and Scams

Banks clearly play a key role in fighting fraud and scams, but unless every participant in the scam ecosystem joins the fight, criminals will continue to steal from and defraud consumers. This is evident in all types of financial transactions, whether check fraud or through Peer-to-Peer (P2P) transactions conducted through online applications such as Venmo, PayPal, CashApp and Zelle.[33]

Unlike the other P2P platforms, however, the Zelle Network (Zelle) is owned by banks, and it has grown in popularity with bank customers because it is fast, free and easy to use. Financial institutions of all sizes participate in the Zelle Network and offer their customers the ability to send money with Zelle. Minority Depository Institutions (MDIs), credit unions, and community banks constitute over 95% of the 2,100 financial institutions that participate on Zelle.[34] Most importantly, Zelle helps local community banks,

[32] See: https://www.aba.com/advocacy/policy-analysis/letter-to-cfpb-on-data-sharing-rules and https://www.aba.com/advocacy/policy-analysis/letter-to-the-cfpb-on-proposed-rule-for-personal-financial-data-rights
[33] See: https://www.zellepay.com/how-it-works
[34] See: https://www.zellepay.com/get-started

MDIs, and credit unions by allowing them to provide the same innovative payment services directly to the communities they serve, no matter the size of the institution.

Zelle enables customers of U.S. financial institutions to quickly send money to friends, family, businesses, and others they know. Consumers send funds directly from their deposit account to another deposit account using the recipient's mobile phone number or email address without having to share sensitive financial information, such as their bank account or routing number.

Unlike other P2P payment services that operate outside of the regulatory perimeter, hold funds in uninsured intermediary accounts, and may assess consumers a fee to move funds to their bank accounts, Zelle enables consumers to receive money directly into their bank accounts within minutes generally at no charge. Also, unlike other P2P services, all funds transferred using Zelle move directly from one insured deposit account at a U.S. bank or credit union to another.

Furthermore, unlike nonbank P2P services, the Zelle Network and all of its bank and credit union participants are subject to compliance with all consumer financial protection laws and multiple layers of regulatory supervision—including by the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (FRB), National Credit Union Administration (NCUA) and the CFPB. Indeed, as the CFPB recently noted in connection with its proposed rulemaking on larger participants in the market for digital payment applications:

> The rule proposed today would ensure that these nonbank financial companies … adhere to the same rules as large banks, credit unions, and other financial institutions already supervised by the CFPB …. Despite their impact on consumer finance, Big Tech and other nonbank companies operating in the payments sphere do not receive the same level of regulatory scrutiny and oversight as banks and credit unions … Specifically, the proposed rule would help ensure these large nonbank companies … Play by the same rules as banks and credit unions.[35]

Of the five billion transactions processed on Zelle in the past 5 years, the vast majority were sent without any report of fraud or scam.[36] Furthermore, Zelle customers report far fewer instances of disputed transactions relative to other P2P services.[37] This is likely the case because Zelle provides consumer protection measures including the following:

- Senders are shown the recipient's name, as registered with the recipient's bank account, and asked to verify the recipient's contact information in the app before a payment can be sent.
- Username, password, or secure cryptographic keys unlocked by device biometrics is sent to the financial institution for customer identity verification using end-to-end encryption.
- Consumers must have a U.S. mobile phone number, email address, and U.S.-based bank account to enroll in Zelle.
- Zelle requires that consumers already have a deposit account at a U.S. based, regulated financial institution, which ensures that rigorous "know your customer" and anti-money laundering legal requirements apply.
- Financial institutions monitor for unusual activity, block suspected fraudulent transfers, and report incidents of suspected fraud or scams to the Zelle Network so that other banks can use that information to protect consumers.

---

[35] See: https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-new-federal-oversight-of-big-tech-companies-and-other-providers-of-digital-wallets-and-payment-apps/

[36] See: https://www.zellepay.com/press-releases/zelle-soars-806-billion-transaction-volume-28-prior-year

[37] See: https://bpi.com/fraud-on-p2p-payment-apps-like-zelle-and-venmo-a-primer. For example, the share of disputed transactions made using PayPal is three times higher than Zelle, and for Cash App, it is six times higher.

- Zelle and financial institutions remove bad actors from the Zelle Network.
- Financial institutions advise consumers to only send money to trusted contacts, such as friends and family, and use popup alerts within the app and payment flow to help consumers identify and avoid common scams.

But criminals use many avenues to exploit consumers, and that is why we have urged policymakers and law enforcement to join with banks in focusing on steps to prevent bad actors from scamming customers out of their money and educating consumers on how to use their services safely.

The solution to these scams is to pursue criminals and to empower consumers with the tools and education to identify and avoid potential scams before they become victims—not to make banks liable for what they cannot control.

Electronic Fund Transfer Act (EFTA) and Regulation E

Federal consumer payments law generally is designed on the principle that the party best situated to prevent fraud loss will bear the cost. This aligns with principles of fairness and efficiency and seeks to minimize moral hazard. The Electronic Funds Transfer Act (EFTA) and its implementing regulation, Regulation E, govern consumer electronic payments and transfers of money, including via P2P apps such as Zelle. Banks are best able to secure the accounts and to track and identify suspicious usage of a debit card. EFTA limits a consumer's liability for unauthorized transactions, such as those arising from electronic payments made using a stolen debit card or a hacked banking portal.[38]

By contrast, EFTA does not limit a consumer's liability for authorized transactions that the consumer voluntarily initiates, including when those transactions turn out to have been made to a criminal.[39] This reflects the fact that banks have limited ability to prevent or manage the risk of authorized-transaction fraud. The proliferation of digital platforms used to anonymize a scammer's identity has increased the tools for this crime. While banks strive to protect access to online or mobile banking platforms and to educate consumers about fraud typologies, scams that trick a consumer into initiating an electronic payment take advantage of areas difficult for a bank to control. Banks cannot know the full circumstances or reasons a customer decides to make a transfer. For example, if a consumer wants to purchase a pedigree puppy, they have more context and information than the bank to assess if they are dealing with a reputable breeder or an online scammer. Banks cannot second-guess every decision a customer makes to transfer their own money, and should not be liable for decisions that are the customers' to make.

Moreover, banks have limited power to stop customers from withdrawing their own money. Even when bankers are convinced their customer is being scammed, they cannot always convince the customer. Bankers often report that they tried everything to make a customer realize they were being scammed but still could not dissuade them from sending the money. Indeed, scammers often coach victims to ignore bank employees' warnings.

Shifting liability would not reduce fraud but increase it, creating a moral hazard and potentially allowing more false claims. Criminals would have new tools to convince consumers to send money under clearly suspicious circumstances if consumers knew their bank had to bear the risk of loss, even if the customer authorized the payment. The criminal could easily convince the consumer they have nothing to lose by pointing out that if the online puppy purchase is a scam, it's only the bank's money at risk. Additionally, it

[38] See 15 U.S.C. § 1693g.
[39] See generally id. (limiting consumers' liability only for unauthorized electronic funds transfers).

would encourage false and questionable claims if consumers could get reimbursed for a transaction by simply asserting a payment was fraudulently induced.

Shifting liability would reduce consumers' access to the P2P payments they value. P2P services are popular because they are a free, fast, and convenient way to send money to friends and family. Because they function like cash, they are inherently different from payment systems like credit card networks, where limitations on who can accept payments, error resolution processes, and liability rules slow transactions and make them more expensive. If banks were liable for consumer-authorized P2P transactions, they would have to charge for the service, make some consumers ineligible to use it, delay transactions, and place more restrictions on payments.

Community banks and MDIs would be most harmed by increased liability, as they are less able to absorb fraud losses. And if P2P becomes less viable to offer, it will be harder for small banks to compete by offering innovative services to win customers, as they often do now.

It would reduce financial inclusion to shift liability for authorized payments to banks. To protect themselves from increased fraud losses and offset fraud costs, financial institutions would have to be more selective about who qualifies for an account and charge more for basic banking services.

To successfully combat these scams, Congress must enact a National Scam and Fraud Prevention strategy, not make banks liable for authorized payments by consumers. Congress should act to provide law enforcement resources, require other industries to join banks in their efforts to prevent fraud, and ensure consumers receive education that empowers them to identify and avoid potential scams.

Conclusion

There is little doubt that financial fraud is a growing phenomenon that is taking a toll on consumers and financial institutions across all types of financial transactions. Banks are taking significant steps to mitigate fraud and other criminal activity by investing in new technologies, deploying public relations campaigns to educate consumers and small businesses about common 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 participant in the scam ecosystem must play a role, from telecommunications firms to social media companies to law enforcement. And we would welcome greater collaboration with engaged community groups who have the trust of consumers across the country.

We urge Congress, regulators, and law enforcement to partner with the banking industry to continue to identify ways to help prevent bad actors from scamming customers out of their money, to educate consumers on how to use P2P services safely, and to apprehend the criminals perpetrating these schemes against consumers.

Thank you for the opportunity to submit this Statement for the Record on this important topic.