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

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

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 May 21, 2024, hearing: "Fraud Alert: Shedding Light on Zelle."

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. 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 warn customers about potentially fraudulent transactions. Banks, however,

[1] The American Bankers Association is the voice of the nation's $23.7 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $18.8 trillion in deposits and extend $12.5 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 low- and moderate-income communities who are underserved by traditional banks and financial service providers. MDIs are located in 32 states and territories. Learn more at nationalbankers.org.

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 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 work tirelessly to identify and report suspicious accounts to law enforcement; to help educate and warn their customers about common scams, and to root out accounts that have been used by criminals.

Consumers are on the front lines of this fight, and banks work diligently 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 where they can best reach their customer, whether in a physical branch, in customer communications, and on their websites, and provide warnings to customers not to share passcodes or send money to people they do not know.

The ABA launched #BanksNeverAskThat,[5] an anti-phishing campaign. Since its launch in October 2020, ABA and member banks have helped educate millions of consumers on how to spot common scams from bad actors posing as their bank. An updated version of the successful campaign will launch in the fall of 2024 and be available to all banks.

However, while banks can educate consumers and help 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. We encourage other trusted sources, such as government actors and nonprofits, to partner with us to amplify the important work banks are doing to educate consumers on fraud.

But even these measures alone will not stop scammers. While banks have technology and infrastructure in place to help defend themselves and their customers, they can only provide the leads necessary for law enforcement to track down the perpetrators. It is critical that federal telecommunications regulators take steps to prevent criminals from "spoofing" legitimate names and phone numbers to impersonate banks. Moreover, telecommunications companies must pursue meaningful initiatives in conjunction with their regulators to counter the rising threat of fraud and scams.

Social media companies must also proactively root out accounts impersonating bank employees or financial advisors that convince people to send them money for supposedly legitimate reasons. Given the magnitude of potential consumer harm, it is critical that law enforcement both have strong partnerships with banks and appropriate resources to combat these crimes. And when these criminals are caught, the punishments must match the crime and disincentivize future

[5] See: www.banksneveraskthat.com

criminal activity, so these offenders will not continue to steal from American consumers and businesses. Banks also welcome opportunities to partner with community-based organizations that are doing critical work in this area, as they are trusted voices in many communities, particularly underserved communities.

A Comprehensive Response to Fraud and Scams is Needed

Banks are but one input into the overall safety and security of the payments ecosystem and are not responsible for and cannot single-handedly prevent criminals from defrauding both consumers and 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 mail 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:

- ***Enhancing Collaboration with Law Enforcement and Regulators*** – Law enforcement agencies play a critical role in stopping fraud and ensuring perpetrators are prosecuted and prevented from further activity, and they must be resourced at a level commensurate with the scale of criminal activity taking place.[6]
- ***Increasing Consumer Education*** – The U.S. government should play a leading role in helping educate consumers on how to protect themselves. Securing someone's account does not help if they can be convinced to willingly hand over their money or their login credentials. Financial education is listed as a core function of the Consumer Financial Protection Bureau (CFPB) on its website.[7] The CFPB should do more to inform consumers about fraud threats.
- ***Developing a National Anti-Scam Strategy*** – Fraud and scams are costing consumers billions of dollars each year and current Federal activities are disjointed and uncoordinated with no overarching strategy. A National Anti-Scam Strategy is critically needed 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.
- ***Closing Loopholes to Stop Impersonation Scams*** – Too many loopholes, such as phone number spoofing, exist allowing criminals to easily impersonate legitimate businesses and agencies. The Federal Trade Commission (FTC) and Federal Communications Commission (FCC) should act against voice service providers that do not signal to consumers that the call they received has not been signed and validated under the existing call authentication framework.
- ***Facilitating Improved Information Sharing by Government Agencies Across Industries*** – Criminals have an active information sharing ecosystem that banks and the public sector must match to try to slow the flow of illicit funds. Laws should be

[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

[7] See: https://www.consumerfinance.gov/about-us/the-bureau/

put in place that support improved data and intelligence sharing between institutions and the government. Additionally, voice service providers, among others, must proactively share information about fraudsters with banks and other responsible companies.

- ***Involving Sectors Beyond Just Banking to Protect Consumers from Scams*** – Banks alone cannot address the problem of fraud and scams without collaboration from other industries. Each step in the scam ecosystem— from how a consumer is introduced to a scam to how the money is processed—offers an opportunity to stop the flow of funds to the criminal. Those sectors that do not provide an appropriate duty of care should be held accountable.
- ***Preventing Risky Data Scraping Practices*** – Screen scraping as a way for third parties to access sensitive consumer information should be eliminated.[8]

These recommendations are consistent with the report language that accompanies Congress' recently passed FY24 appropriations bill. The report language directs the Treasury Department to jumpstart an all-of-society response to increased fraud and scam threats by establishing a private-public sector task force focused on prevention. This task force would encourage greater information sharing across sectors, promote collaboration in the development of counter-fraud technologies and provide a dedicated forum for stakeholders to strategize around innovative approaches to combating emerging fraud and scam threats. The report language also calls on the Treasury Department to report back to Congress on the resources needed to effectuate this directive. Congress should ensure the Treasury Department not only follows through on this request but does so publicly through a formal report.[9]

Person-to-Person (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 Person-to-Person (P2P) transactions conducted through online applications such as Venmo, PayPal, CashApp and Zelle.[10]

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.[11] Most importantly, Zelle helps local community banks, MDIs, and credit unions by allowing them to

[8] *See* Statement for the Record Bank Policy Institute Senate Committee on Banking, Housing and Urban Affairs Hearing: "Examining Scams and Fraud in the Banking System and Their Impact on Consumers" (Feb. 1, 2024), Statement-for-Record-Senate-Banking-on-Fraud-and-Scams.pdf (bpi.com).

[9] See: Financial Services and General Government Appropriations Bill, S. Report 118-61, at 10 (2023), https://www.congress.gov/congressional-report/118th-congress/senate-report/61/1?outputFormat=pdf

[10] See: https://www.zellepay.com/how-it-works

[11] See: https://www.zellepay.com/get-started

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.

Further, 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.[12]

Of the five billion transactions processed on Zelle in the past 5 years, more than 99.9% were sent without any report of fraud or scam.[13] Furthermore, Zelle customers report far fewer instances of disputed transactions relative to other P2P services.[14] This is likely the case because Zelle provides consumer protection measures including the following:

- Username, password, or biometric data 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.

---

[12] 88 F.R. 80197 (Nov 17, 2023). CFPB Proposes New Federal Oversight of Big Tech Companies and Other Providers of Digital Wallets and Payment Apps (Nov 7, 2023) available at 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/

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

[14] 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 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.
- 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.
- 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.

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.

Impersonation Driven Scams

Banks have made significant progress in protecting themselves and their customers from being hacked. Unfortunately, bank customer losses from scams have still been increasing, many times due to the criminals' ability to impersonate a trusted party. Is it the consumers fault that they believe their caller ID that shows their bank's 1-800 customer service number which matches the number on the back of their debit card, or that the amazing crypto investment they are researching is being pitched by a social media account of a well-known successful investor?

Many people inherently trust these technology "verified" identities, which creates an opening for the criminal they are interacting with. By the time the scam has moved to the payment phase, the customer has been fully convinced of the legitimacy of the transaction.

A key part of breaking the scam ecosystem is to eliminate this "trusted" entry point into the scam ecosystem.[15] 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[16] that identified the top text messaging scams of

[15] See 2022 report entitled "Fighting Fraud: Breaking the Chain," highlighting the cost of fraud, the impact of fraud and the actors involved in the fraud lifecycle, and highlights real-world experiences of institutions attempting to educate their customers, available at: https://committees.parliament.uk/publications/31584/documents/177260/default/

[16] See: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

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 did not 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.

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.