American Bankers Association
Building Success. Together.

Nessa Feddis
Senior Vice President and Counsel
Consumer Regulations & Compliance Solutions
Regulatory Compliance and Policy
Phone: 202-663-5433
E-mail: nfeddis@aba.com

October 27, 2022

The Honorable Rohit Chopra
Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington DC 20552

Dear Director Chopra,

The American Bankers Association (ABA)[1] and two community bankers, John Moniak of Bank of Deerfield and David Long of Bryant Bank, were pleased to attend the "listening session" on September 29 with staff of the Consumer Financial Protection Bureau (CFPB) to discuss financial scams involving peer to peer (P2P) payments. We are following up with this letter as the time and format constraints of the listening session did not allow participants to fully discuss some of the scams banks and their customers are experiencing, steps banks take to prevent scams and other fraud, and the significant banking industry efforts to educate customers about how to avoid being a victim of fraud. In addition, we want to reiterate and supplement our members' concern about the implications and unintended consequences if liability for payments that consumers authorize—but later claim were part of a scam—is shifted to banks.

P2P services are highly popular and beneficial to consumers. Fraud is de minimis relative to the transaction volume, with 99.9 percent of the 5 billion Zelle transactions processed in the past 5 years without issue.[2]

P2P payment volume and popularity have soared in recent years and for good reasons.[3] They are a convenient, fast, and (currently) usually free way to send money to people a consumer knows and trusts, especially when compared to cash and checks—the only other practical alternatives for consumer to consumer payments. P2P payments make it easy to pay the babysitter, lawn mower, or handyman, to send money to a college student, or to repay a friend for dinner or concert tickets without having to worry about having cash or locating a checkbook.

Consumers value the fact that P2P payments are made quickly—and importantly—cannot be reversed. Sellers who accept a P2P payment do not have to worry that a buyer will cancel the payment after the seller has handed over the item being sold. The finality of payment means recipients can

---

[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 more than 2 million people, safeguard $19.6 trillion in deposits and extend $11.8 trillion in loans.

[2] Early Warning Services, LLC, "Zelle® Reaches Five-Year Milestone with More than Five Billion Safe, Secure Transactions" (Sept. 8, 2022), https://www.prnewswire.com/news-releases/zelle-reaches-five-year-milestone-with-more-than-five-billion-safe-secure-transactions-301619582.html#:~:text=SCOTTSDALE%2C%20Ariz.%2C%20Sept.,network%20operator%20of%20Zelle%C2%AE.

[3] Total transactions during the second quarter 2022 rose 27% to 554 million from a year ago. *Id.*

confidently use the money as soon as it is received without fear it may be returned. P2P recipients do not have to monitor when the payment is available to spend as it is available immediately and cannot be returned and the account debited, which may cause an overdraft.

Consumers also benefit from the safety of P2P payments. While rarely reported by the media, check theft from the U.S. Postal Service has increased significantly in recent years,[4] and cash can be stolen. P2P payments allows consumers to avoid this harm and inconvenience.

Disputes and complaints about P2P payments are uncommon, especially for Zelle payments when compared to nonbank P2P products. As noted, 99.9 percent of the 5 billion Zelle transactions processed in the past 5 years were sent without any report of fraud or scams. The share of disputed transactions made using PayPal is three times higher than Zelle. For Cash App, it is six times higher.[5] Similarly, a search of 2,954,837 consumer complaints reported on the Bureau's Consumer Complaint Database show there were:

- 18,797 matches for PayPal;
- 783 matches for Venmo;
- 656 matches for CashApp;
- 565 matches for Zelle.

Banks have made and continue to make significant investments to thwart scams through fraud controls and consumer education. Making public information about fraud controls would undermine their effectiveness.

As the popularity and ubiquity of P2P payments have increased, they have attracted the attention of scammers. Many of the scams are not new, but like consumers, fraudsters benefit from the speed, convenience, and near instant access to the funds from a P2P payment. In addition, because P2P services are relatively new, scammers are able to target people who are unfamiliar with them.

For those reasons, banks have made significant investments in fraud controls and consumer education. And, as with any new product, both users and providers have gained experience with P2P fraud schemes, permitting banks to tailor their fraud controls and customer alerts and education.

Some of these fraud controls are known and visible, such as: pop-up warnings that require affirmative user confirmation before the transaction may proceed; warnings that the consumer should send money only to people the consumer knows and trusts; requirements for passcode confirmation when new recipients are added or each time money is sent; and text and e-mail verifications of transactions. Other fraud controls are not publicized because announcing them would undermine their effectiveness. Scammers constantly work to identify fraud controls in order to manipulate and circumvent them. In addition, banks and other P2P providers continually adjust fraud controls as scammers learn about them and system vulnerabilities and alter their own strategies and techniques. For this reason, ABA has not described the full range of fraud controls in this letter or in any other public document.

---

[4] Criminals wash the stolen checks, alter the amounts and payee, and deposit them using a mobile phone.

[5] Bank Policy Institute, "Online Fraud is Real, But Zelle is a Safe Harbor, Not the Problem" (Oct. 3, 2022), https://bpi.com/online-fraud-is-real-but-zelle-is-a-safe-harbor-not-the-problem/.

In addition to fraud controls, banks devote significant resources to consumer education in order to protect their customers from scams. Consumer education includes cautions to customers at the time of a transaction and also other communications sent on a periodic basis through various media. Messages include, for example, warnings describing red flags that identify common and emerging scams and how to avoid them. Importantly, banks warn consumers that they will never ask customers to send money to the bank or themselves and that they should not share multi-factor authentication codes used to confirm their identity or a transaction or to add a user to an account.

ABA also educates consumers about fraud prevention. For example, ABA makes the following resources available to all banks free of charge:

- Banks Never Ask That Campaign. More than 2,000 banks have participated since the campaign began in 2020. The free materials were refreshed in early October 2022 and include educational information empowering consumers to spot common P2P payment scams.

- ABA Foundation infographics developed in conjunction with the Federal Trade Commission, including How to Safely Use Mobile Payment Apps and Services and Phishing: Don't Take the Bait, which are available to banks and the public.

- Publicly available information on ABA's Consumer Resources pages to help people understand how to "Protect Yourself and Your Money."

- The ABA Foundation's "Safe Banking for Seniors" campaign, through which bankers lead presentations to help older Americans and their loved ones prevent financial exploitation. The program includes seven newly released scam awareness videos that any bank may access, including:

    - How Scammers Scam Seniors
    - Family Impostor Scams
    - Government Impostor Scams
    - Lottery Scams
    - Money Mule Scams
    - Sweetheart Scams
    - Tech Support Scams

- Infographics to educate students about scams offering scholarship and student loan forgiveness

Banks have limited insight or opportunity to intervene in consumers' payment decisions.

While the banking industry has made substantial investments in fraud prevention and has had success in educating consumers, banks cannot stop all scams. Indeed, consumers are in the best position to know the reasons they are sending money, the circumstances of the payment, and who the recipient is. Banks, in contrast, typically have no knowledge about the relationship between the sender and the recipient, the reasons the consumer is sending money, or the context of the payment.

Moreover, experience demonstrates that banks have little ability to intervene. For example, banks report cases in which bank employees have warned a customer not to send money because the

transaction appears to be a scam, but the customer proceeds to send the money—and later files a claim with the bank and a complaint with the CFPB. For example, in the listening session David Long described how a bank employee and the chief of police, who happened to be in the bank, strongly advised a customer not to send money, suspecting it was a scam. Nonetheless, the customer sent the money and later filed a dispute with bank. In other cases, it is difficult to persuade customers not to send the money because criminals have coached them not to contact or trust banks. Banks have even less ability to understand or investigate a transaction when it involves a non-bank P2P transaction, because, unlike the case with Zelle, they have no direct relationship with non-bank P2P providers.

For these reasons, under payment systems rules and regulations, including the Electronic Fund Transfer Act (EFTA) and its implementing regulation, Regulation E, consumers are generally responsible for transactions they initiate[6] on the basis that liability and responsibility for fraudulent transactions lies with the party in the best position to identify and prevent the fraud.[7]

Shifting liability for payments the customer has authorized and later claims were made to a scammer will harm consumers in the form of higher costs, fewer options, and less competition.

Notwithstanding the limited ability of banks to stop or intervene in consumer authorized transactions, there have been reports that the CFPB is considering requiring banks to reimburse consumers for P2P payments consumers make but later *claim* were made to a scammer.[8] Shifting this liability to banks is not authorized by EFTA and will ultimately harm consumers and competition. Many banks will reconsider whether to offer P2P payments, whether to be more restrictive in access and options, and whether to begin charging for the service, which is now free at the vast majority of banks. In addition, consumers will have to wait to use their money. In effect, the value proposition of P2P disappears.

If banks must reimburse customers for P2P payments that a customer later claims were made to a scammer, banks will have to adjust their business models to reflect those risks and potential losses—over which they have little control—as well as the costs of claims investigation and compliance. While responses will vary, banks will have to consider whether: to charge for P2P transactions, which currently are usually free;[9] to limit access to P2P services; to reduce the frequency and amounts of P2P payments; and/or to close accounts.

---

[6] Consumers may not be responsible for certain transactions they initiate, for example, an "electronic fund transfer at an ATM. . . if the consumer has been induced by force to initiate the transfer." 12 C.F.R. §1005.2(m) cmt. 4. (2018).

[7] Though EFTA and Regulation E protect consumers from "unauthorized" electronic payments, (12 CFR §1005.6), consumers are generally responsible for payments they initiate. As the CFPB's Compliance Aid to Electronic Fund Transfer repeats. Consumer Fin. Prot. Bureau, Electronic Funds Transfers FAQs, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/ (last visited Oct. 25, 2022) ("under EFTA and Regulation E, an "unauthorized electronic fund transfer" means an electronic fund transfer from a consumer's account" — *initiated* by a person *other than the consumer* without actual authority to initiate the transfer and from which the consumer receives no benefit." (15 U.S.C. §1693a((12) and 12 C.F.R. §1005.2(m)) (emphasis added)).

[8] *See, e.g.,* Andrew Ackerman, *CFPB to Push Banks to Cover More Payment-Services Scams*, Wall St. J., July 19, 2022, https://www.wsj.com/articles/consumer-bureau-to-push-banks-to-refund-more-victims-of-scams-on-zelle-other-services-11658235601.

[9] ABA has heard from one member that now imposes P2P transaction fees to cover the cost of disputes.

Banks may also have to consider placing "holds" on money sent by P2P, which would fundamentally alter the value and appeal of the "faster payment" product that consumers have overwhelmingly indicated they want. If P2P payments may be challenged and reversed, banks will have to delay the recipient's access to the money. In effect, shifting the liability will defeat the purpose of faster payments, which is to provide certainty and finality of payment. P2P services will be less useful than paying by cash and check, the only practical alternatives for consumer to consumer transactions.

In addition, while banks work to identify possible scammers and deny them access to bank accounts (which they need to receive the victim's money), to better screen out scammers, banks may have to make account opening eligibility more strict, which will make it more difficult for some people to obtain accounts. There is an unavoidable tension between steps taken to identify potential fraudsters and being flexible in account eligibility criteria to encourage financial inclusion. As banks adopt stricter account eligibility criteria (such as more robust verification of a person's physical address and identification), it will invariably prevent some consumers who can manage and benefit from a bank account from having access.

Moreover, P2P systems cannot vet payment recipients as credit card networks do. Card networks strictly vet entities accepting card transactions and require that they comply with PCI security standards, error resolution processes, liability rules, and reserve requirements to cover charge backs, etc. P2P systems were developed to enable consumers to send electronic payments to other *consumers* whom the sender knows and trusts and imposing card network obligations and requirements on consumers is not practical or possible.

Further, competition will be reduced if banks are liable for P2P transactions that a consumer later claims was made to a scammer. Some banks will not be able to offer P2P services. In response to the media reports of even *potential* expansion of bank liability, some small banks have reported that they would probably have to exit the P2P payment business. Others who were considering adding P2P services have paused advancement. Just the *perception or threat* that banks will shoulder liability for authorized transactions will discourage small banks in particular from offering P2P, leaving them at a competitive disadvantage given the growing popularity of these services.[10]

Scammers will profit from a shift in liability for P2P payments the customer has authorized and later claims was made to a scammer.

Shifting liability to banks for authorized but fraudulently induced transactions also will increase scams and embolden scammers. Armed with a written federal government policy stating that consumers are entitled to a return of money sent to scammers, scammers will be better able to induce consumers to send money. They will assure them that there is no downside or risk in sending the money because the bank will reimburse them. Moreover, the internet will be replete with "advice" for consumers on the language to use in a dispute to ensure it comports with the new policy.

Fraud will also increase because consumers will have little incentive not to send money despite suspicious circumstances. However, as discussed above, banks' ability to detect scams or stop a

[10] Some banks, in limited circumstances, reimburse consumers for money they sent to a scammer even though the bank is not required to do so. However, voluntary bank actions should not be converted into a government mandate. Mandates cannot be adjusted as fraud evolves, and as previously discussed, may encourage some consumers to send money despite suspicious circumstances and others to misuse the protection by filing false claims.

consumer from making a payment is limited. As a practical matter, banks cannot know the circumstances or relationship between a sender and a recipient. In addition, they have little ability to stop a customer who insists on sending the money despite the bank's warning without assuming the risk of liability (and other negative consequences) for failure to follow a customer's payment instruction. There may be legal consequences and liabilities if a bank stops a payment that looks suspicious but, in fact, is legitimate. For example, a bank might face liability based on the consumer's claim that the failure to send money caused the consumer to miss out on a profitable investment or purchase opportunity.

Conclusion

The banking industry shares the CFPB's goal to protect consumers from P2P payments scams, and we understand the agency's interest in wanting to respond to instances when consumers have suffered losses. However, any CFPB effort to shift liability for authorized P2P transactions should acknowledge the substantial benefits of P2P payments to consumers, the relatively small incidences of fraud, and how consumers are warned about and can avoid scams.

In addition, we caution that any policy issuance interpreting the EFTA or Regulation E must be consistent with the statute's and regulation's provisions that consumers are liable for electronic fund transfers they authorize. Although EFTA and Regulation E protect consumers from "unauthorized" electronic payments,[11] consumers are generally responsible for payments they initiate. As the CFPB's Compliance Aid pertaining to EFTA,[12] repeats, under EFTA and Regulation E, an "unauthorized electronic fund transfer" means an electronic fund transfer from a consumer's account—"initiated by a person *other than the consumer* without actual authority to initiate the transfer and from which the consumer receives no benefit."[13] (emphasis added) Any interpretation that shifts liability to financial institutions for transactions the consumer has authorized, even if made to a scammer, would be inconsistent with the statute and regulation.

Moreover, any regulatory action must comply with the Administrative Procedure Act to ensure that any policy changes benefit from public input and a robust cost-benefit analysis that considers all consequences, including the negative impact on consumers and competition. In addition, we strongly recommend that the CFPB solicit public input if it chooses to publish interpretive guidance.

Finally, we want to reiterate a point made by several bankers during the listening session. That is, rather than concentrating on the question of who should bear liability for losses associated with scams involving P2P payments, the CFPB should work with financial institutions, bank and non-bank P2P service providers, other Federal agencies and law enforcement to prevent scams. For example, we encourage the CFPB to work with the Federal Trade Commission on consumer education, to support the Federal Communication Commission's work to stop the illegal "spoofing" of outbound calls and texts placed by banks, and to work with law enforcement to help identify and prosecute criminals and prevent the fraud before it happens. By working together, government and the financial services industry stand the best chance of preventing the bad actors from harming consumers in the first place.

ABA appreciates the opportunity to explain the banking industry's efforts to prevent fraud and scams and educate consumers on how to avoid them. We caution that any measures to shift liability to financial institutions for P2P payments that a consumer authorizes and later claims were paid to a

[11] 12 C.F.R. §1005.6.

[12] Electronic Funds Transfers FAQs, *supra note* 7.

[13] 15 U.S.C. §1693a(12); 12 C.F.R. §1005.2 (m).

scammer will harm consumers by diminishing the availability and value of P2P payments and increasing consumers' costs. It will also reduce competition and enrich and encourage criminals. We welcome discussion with the CFPB on these matters to understand better its concerns.

Regards,

Nessa Feddis

Attachment 1

Contact

Meghan Fintland

Early Warning

+1.925.785.9192

Meghan.Fintland@earlywarning.com

Zelle® Reaches Five-Year Milestone with More than Five Billion Safe, Secure Transactions

- **Five in Five**: Five billion+ transactions and nearly $1.5 trillion have moved across the network since 2017.
- **Safe Payments**: More than 99.9% of payments are sent without any report of fraud or scams.
- **Widespread Adoption by U.S. Financial Institutions**: Nearly 1700 banks and credit unions, including minority deposit institutions (MDI), now offer Zelle® in their apps.
- **More than P2P:** Disbursements increased 87% quarter-over-quarter; while growth in Zelle® for Small Business resulted in nearly eight million employees, contractors, and customers receiving payments from small businesses.

Scottsdale, AZ, September 8, 2022 – In the past five years, consumers and businesses, small and large, have sent more than five billion Zelle® payments, totaling nearly $1.5 trillion, according to Early Warning Services, LLC, the network operator of Zelle®.

Zelle® users have leveraged the convenience and security of Zelle® to gift money, pay rent, reimburse friends and family for shared costs, receive reimbursements, or access money in critical moments, usually within minutes using Zelle®.

"Zelle® has transformed the way more than a hundred million people move money and conduct digital transactions," said Al Ko, Chief Executive Officer at Early Warning. "We are part of consumers' everyday lives and committed to being their trusted source for digital payments that are easy to use and don’t require the sharing of any bank account information. Thanks to our financial institution participants, reseller partners, and employees, we continue to innovate and expand adoption while enhancing protection measures."

Commitment to Safe Payments

The network has achieved more than 99.9% of payments sent without any report of fraud or scams. Zelle® and its participating financial institutions are continuously evolving and adapting consumer protection measures to address the dynamic nature of deceptive activities. For instance, real-time safety notifications (within the user experience and payment flow) alert users to only use Zelle® when sending money to people they know and trust.

In addition to the extensive education that financial institution participants deliver to their customers, Zelle® partners with non-profits, consumer safety organizations, influencers, and enterprises. By collaborating with The Cybercrime Support Network, Detroit Pistons, EVERFI, Nev Shulman, The Knoble, and Vox Media, the company continuously educates consumers on how to stay safe when using digital payments such as Zelle®. The recently launched Zelle® Learning Hub is another resource that helps consumers make smart financial decisions that begin with education.

Empowering all Communities with Real-Time Access to Payments: Nearly 1700 Financial Institutions Now Offer Zelle®

The Zelle Network® is open to any size financial institution that wants to give its customers access to real-time payments. Today, nearly 1700 banks and credit unions, including 100+ MDIs, offer Zelle® in their app. Throughout the past year, the company worked with its resellers on rebate programs for qualifying MDIs that sign up to offer Zelle®, giving their customers equitable access to financial services with additional tools to help meet their financial goals.

Disbursements, Business Payments Lead the Way in Q2 2022

Fortune 500 companies, including major online retailers, educational institutions, and national non-profits, are disbursing funds—tuition, rebates, settlements, insurance payments— as a fast and safe alternative to sending checks. In Q2 2022, the Zelle Network® achieved an 87% quarter-over-quarter increase in disbursement transactions. Nearly eight million employees, contractors, and customers received payments from small businesses.

"Increased Zelle® usage by small businesses year over year is impressive," said Erika Bauman, director of commercial banking and payments at Aite-Novarica. "Our research shows that business adoption has more than doubled across the market. The rapid growth of Zelle® is due to greater efficiency, access to funds, and increased recipient satisfaction."

Overall payments in Q2 2022 equated to $155 billion sent through the Zelle Network® on 554 million transactions. Year-over-year payment values increased by 29%, while payment volume increased by 27%.

About Zelle®

Brought to you by Early Warning Services, LLC, an innovator in payment and risk management solutions, Zelle® makes it fast, safe, and easy for money to move. The Zelle Network® connects financial institutions of all sizes, enabling consumers and businesses to send fast digital payments to people and

businesses they know and trust with a bank account in the U.S. Funds are available directly in bank accounts generally within minutes when the recipient is already enrolled with Zelle®. To learn more about Zelle® and its participating financial institutions, visit www.zellepay.com.

About Early Warning Services, LLC

Early Warning Services, LLC is a fintech company owned by seven of the country's largest banks. For almost three decades, our identity, authentication, and payment solutions have been empowering financial institutions to make confident decisions, enable payments and mitigate fraud. Today, Early Warning is best known as the owner and operator of the Zelle Network®, a financial services network focused on transforming payment experiences. The combination of Early Warning's risk and payment solutions enables the financial services industry to move money fast, safe, and easy, so that people can live their best financial lives. To learn more about Early Warning, visit www.earlywarning.com

# # #