Testimony of Delicia Reynolds Hand, Senior Director, Digital Marketplace, Consumer Reports

Before the United States Senate
Permanent Subcommittee on Investigations

"Fraud Alert!: Shedding Light on Zelle"

Tuesday, May 21, 2024
Dirksen Office Building
Washington, DC

Chairman Blumenthal, Ranking Member, and members of the Subcommittee, thank you for the opportunity to testify on the critical issue of consumer protection in the rapidly growing market for peer-to-peer (P2P) payment services. I am Delicia Reynolds Hand, Senior Director for the Digital Marketplace at Consumer Reports (CR).

Consumer Reports is an independent, nonprofit member organization that works side by side with consumers for truth, transparency, and fairness in the marketplace. We use our rigorous research, consumer insights, journalism, and policy expertise to inform purchase decisions, improve the products and services that businesses deliver, and drive for fair and competitive practices. Over recent years we have built on this work to provide this same value and information by expanding our focus as an organization to evaluate digital devices and products such as digital financial services.

The proliferation of sophisticated scams on P2P payment apps is causing devastating financial and emotional harm to consumers, and swift action is needed to address this growing problem. Today, I aim to shed light on the unique risks posed by Zelle and other P2P services, the inadequacy of current consumer protections, and the urgent need for reform.

The Human Impact of P2P Scams:

To understand the true cost of P2P fraud, we must look beyond the numbers to the real life experiences of people who have been scammed. Take the case of Mary, an 80-year-old grandmother who received a call from someone claiming to be her grandson, urgently in need of $10,000 for bail after a car accident. Frightened and wanting to help, Mary followed the

scammer's instructions to send the money via Zelle. Only later did she learn her real grandson was safe at home - and her money was gone.[1][2]

Given the proliferation of new products and services that deliver the convenience of real-time and near instant payment tools to consumers, the focus of today's hearing on fraud and scams on the Zelle payment network is particularly timely and important. Payment apps that enable consumers to move money fast, put them at risk to easily lose money just as quickly. The median loss for P2P scam victims is $500, a significant amount for many households.[3]

But the impact goes beyond just financial losses. Romance scams, where fraudsters gain victims' trust online before requesting money for fake emergencies, are also surging on P2P apps. The psychological and financial toll of realizing you've been manipulated by someone you grew to care for can be devastating. Victims often report feelings of shame, guilt, and a loss of trust that can take years to recover from. For seniors on fixed incomes or living alone, the effects can be particularly severe.

As P2P payment apps like Zelle have surged in popularity, with 64% of Americans now using them,[4] so too have reports of consumers falling victim to scams and struggling to obtain reimbursement from their banks.[5] Consumer Reports has been closely studying the P2P payments market to identify risks to consumers and recommend improvements. Our recent white paper, "Peer-to-Peer Payment Apps: A Case Study for a Digital Finance Standard," provides a comprehensive look at the state of consumer protection across popular P2P services.[6]

The Consumer Reports Peer to Peer App Study:

In 2022, Consumer Reports conducted a comparative evaluation of four leading P2P payment apps - Apple Cash, Cash App, Venmo, and Zelle - assessing their safety, privacy, and

---

[1] Creswell, J. (2022, March 6). "Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem." The New York Times.
[2] Witt, E. (2021, February 3). "Torn Apart by Distance (and Scammers)." The New York Times.
[3] A February 2023 Federal Trade Commission (FTC) report discusses consumer fraud on social media platforms, including peer-to-peer payment scams and the financial losses associated with them. Federal Trade Commission. (2023, February). Consumer Fraud on Social Media Platforms. Federal Trade Commission. https://www.ftc.gov/system/files/ftc_gov/pdf/Consumer_Fraud_on_Social_Media_Platforms_Feb_2023_Report.pdf
[4] Consumer Reports nationally representative American Experiences Survey of 2,116 US adults (March 2022).
[5] A recent article by The New York Times titled "Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem" (March 2022). discusses the increasing number of scams on Zelle and the challenges consumers face when seeking reimbursement from their banks. Creswell, J. (2022, March 6). Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem. The New York Times. https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html
[6] Consumer Reports. (November 2022). The Fair Digital Finance Framework: Initial Application to the Peer-to-Peer Payments Sector.

transparency policies and practices.[7] As it pertains to safety, we found that all four services lacked clear, accessible disclosures about the availability of FDIC insurance for user balances and the full scope of their fraud and error resolution policies. Notably, Zelle stood out for providing the least comprehensive information to users about their rights and protections.

Our research also highlighted the alarmingly high incidence of fraud and scams on P2P platforms. In a March 2022 CR survey, 12% of weekly P2P users reported sending money to the wrong person, while 9% said they had been scammed.[8] This tracks with recent data from the "Big Four" banks (Bank of America, JPMorgan Chase, U.S. Bank and Wells Fargo), which reported a combined $255 million in Zelle-related disputed transactions in 2021 and the first half of 2022.[9] The banks' internal data shows scams and fraud are rampant on Zelle.

The Unique Risks of Zelle:

Several aspects of Zelle's business model and policies create outsized risks for users compared to other P2P services:

- Lack of a clear, published fraud liability policy: Unlike Venmo or Cash App, Zelle does not have a public-facing policy detailing consumer protections and reimbursement rights for unauthorized transactions. This leaves victims unclear on where to turn for help.
- Fragmented customer service: Zelle support is split between the network operator and participating banks, which can bounce victims back and forth. A centralized, consistent process is needed to help consumers when they fall victim to fraud and scams.
- Weaker authorization safeguards: Zelle enables instant transfers with less upfront friction, like two-factor authentication, which is less secure and can enable faster fraud compared to other P2P apps.[10]
- Lack of transparent data: Zelle does not regularly publish statistics on the volume and resolution of fraud and scam complaints. This hinders effective oversight of how well its policies are working.

The crux of the issue is that Zelle enables instant bank account-to-account transfers without the critical friction and multi-layered protections offered by other P2P services like PayPal or Cash App. This speed is convenient for users but also attractive to and exploited by scammers.

Consumer Harm and the Path to Redress:

When a consumer realizes they've been scammed on Zelle, they often face an uphill battle to recover their money. Banks frequently deny claims for reimbursement, arguing that since the

[7] Consumer Reports. (November 2022). The Fair Digital Finance Framework: Initial Application to the Peer-to-Peer Payments Sector.
[8] Consumer Reports nationally representative American Experiences Survey of 2,116 US adults (March 2022).
[9] Warren, E. (October 2022). Facilitating Fraud: How Customers Defrauded on Zelle are Left High and Dry by the Banks that Created It.
[10] Chakravarty, R. (May 2024). "Wells Fargo says US authorities probing Zelle disputes." Banking Dive.

consumer initiated the transaction, even if induced by fraud, they are not liable under Regulation E of the Electronic Fund Transfer Act.[11] This struggle is not limited to scam victims; even in cases of legitimate transactions gone awry, consumers are left to fend for themselves. Take the case of Bob from Florida, whose friend sends him $250 a month to repay a loan. One month, the payment was deducted from his friend's account but never arrived at Bob's. When he contacted Zelle, their response was essentially, "it's not our problem, we are just the middleman." Despite several conversations with both banks and Zelle, Bob eventually gave up, unable to recover the missing funds.

Consumer Reports has argued that in cases of fraudulently induced payments, banks should provide reimbursement to victims under Regulation E.[12] Recent data on peer-to-peer (P2P) payment fraud in the U.S. highlights the growing scale and complexity of the issue.[13] In 2023, consumers in the U.S. reported losing over $10 billion to fraud in 2023, a 14% increase from the previous year. Among these losses, investment scams accounted for more than $4.6 billion, and imposter scams nearly $2.7 billion. Also in 2023, consumers reported significant losses due to scams involving P2P payment apps like Venmo, Zelle, and Cash App. The FTC's Consumer Sentinel Network Data Book for 2023 indicated that bank transfers and payments, which include P2P transactions, accounted for $1.86 billion in losses, marking it as the payment method with the highest fraud losses, followed closely by cryptocurrency at $1.41 billion.[14] These figures underscore the prevalence and financial impact of fraudulently induced payments.[15]

With the rise of generative AI and advanced technologies, fraudsters can create highly convincing scams that are increasingly difficult for any consumer to detect, regardless of their financial literacy or awareness. A recent Wall Street Journal article highlighted how scammers are using generative AI to create realistic deep-fake videos, impersonating individuals known to the victims and deceiving them into transferring large sums of money.[16] Relying on consumer awareness alone is not sufficient to combat these evolving threats.

---

[11] 12 C.F.R. § 1005 (2022).
[12] Consumer Reports. (October 2018). Peer-to-Peer Payments Are Generally Safe, But Consumers Must Be Aware of Risks.
[13] UK Finance. (2023). Annual Fraud Report 2023. https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf
[14] FTC report on U.S. fraud losses in 2023: Federal Trade Commission (Federal Trade Commission) (Federal Trade Commission) (Federal Trade Commission) (Consumer Advice).
[15] When it comes to peer-to-peer (P2P) payment fraud in the U.S., the situation is increasingly concerning. Several types of scams are prevalent in this space, including imposter scams, romance scams, fake product or service purchase scams, and unauthorized money transfers. In 2023, significant losses were reported due to these types of fraud. For instance, imposter scams, where scammers pose as trustworthy individuals to convince victims to transfer money, continue to be a major issue. Romance scams similarly exploit users by promising high returns on fake investments or pretending to seek a romantic relationship to solicit funds(EY US). Unauthorized transfers are another common fraud method, often involving scammers sending money "by mistake" and then asking the recipient to return it, which can lead to the exposure of personal financial details or direct monetary loss (LibertyID).
[16] Einis, J. (2023, June 6). Generative AI Is Pushing Fraud to New Levels. PaymentsJournal. https://www.paymentsjournal.com/generative-ai-is-pushing-fraud-to-new-levels/

A consumer who sends money under duress, in fear for their own or a loved one's safety, cannot be said to have authorized that payment in any meaningful sense. The scammer has deprived them of true choice and control. Additionally, the notion that financial institutions should not share responsibility for reimbursing certain scams also ignores the reality of how sophisticated scams exploit human vulnerabilities.

As financial services grow more complex, it is banks, not consumers, who are best positioned to prevent and absorb losses from fraud. This is not a radical idea.As the courts have long recognized in product liability cases, as manufacturing processes grow more sophisticated, the scope of a company's responsibility to ensure consumer safety expands as well.[17] So too should banks' obligations to protect customers grow in proportion to the evolving risks of digital finance. Just as manufacturers are expected to implement robust safety measures and bear the cost of product defects, banks should be required to invest in advanced fraud prevention technologies and reimburse customers for losses resulting from increasingly sophisticated scams.

Balancing Liability in the Age of Instant Payments:

The current legal framework, which shields banks from liability for fraud when the consumer initiates the transaction, is a relic of a bygone era. In a world of instant, irreversible P2P payments, this approach puts an unfair burden on consumers to spot increasingly sophisticated scams. Banks and P2P service providers are far better equipped to both prevent fraud and absorb fraud losses. They have access to vast troves of transaction data and the latest technology for anomaly detection to prevent fraud. And by investing in more robust fraud controls and spreading losses across their customer base, they can act as a shock absorber for individual consumers.[18]

Other countries are already moving in this direction. The UK, for example, has proposed requiring banks to reimburse scam victims in certain cases, recognizing that the speed and ease of modern payments requires a new approach to liability.[19] The US should follow suit.

A Path Forward

Protecting consumers in the instant payment era will require a collaborative effort between policymakers, industry, and consumer advocates. Congress should also clarify through legislation that Regulation E applies to fraudulently induced payments, not just unauthorized transfers where the consumer had no knowledge of the transaction. Banks should put in place the necessary safeguards and frictions when initiating P2P payments, invest in real-time transaction monitoring, and establish a streamlined, consistent process for reporting and resolving scams across all P2P services.

---

[17] MacPherson v. Buick Motor Co., 217 N.Y. 382 (1916).
[18] Kaur, S., & Anand, M. (2021). "Real-Time Anomaly Detection Techniques Using Transaction Data for Fraud Detection in Financial Services." In Machine Learning and Deep Learning in Real-Time Applications (pp. 269-283). IGI Global.
[19] Financial Conduct Authority. (2021, May). "Consultation on a New Authorised Push Payment (APP) Scams Reimbursement Process."

Most importantly, we need a philosophical shift in how we think about financial fraud. Rather than treating it as a personal failure of the consumer, we must recognize it as a systemic risk to be managed collectively. Only then can we create a fair and sustainable P2P payment ecosystem for all.

To better protect consumers from P2P payment scams, Zelle and participating banks should:

1. Adopt and publish a clear, enforceable policy guaranteeing reimbursement for all unauthorized transactions, as well as authorized transactions induced by fraud.
2. Implement stronger transaction monitoring and identity verification safeguards.
3. Create a streamlined, centralized process for consumers to report fraud and seek reimbursement.
4. Provide greater transparency about fraud trends and reimbursement rates across the Zelle network.
5. Establish a robust framework for sharing fraud information across the industry.[20]

By adopting these changes, the financial sector and policymakers can create a P2P payment ecosystem that better balances consumer protection with the benefits of fast, convenient money movement. Consumer Reports looks forward to working with the Subcommittee, industry stakeholders, and consumer advocates to advance this important goal.

Thank you again for the opportunity to testify, and I look forward to answering your questions.

[20] By collaborating and sharing data on emerging scam tactics, suspicious actors, and successful prevention strategies, financial institutions can strengthen their collective defenses against fraudsters. This collaborative approach has proven effective in other areas of financial crime prevention, such as anti-money laundering efforts. Implementing similar information-sharing mechanisms for P2P payment fraud would enable banks to proactively identify and mitigate risks, reducing losses for both consumers and financial institutions. See Köster, F., & Pelster, M. (2020). Information Sharing and Cooperation in Anti-Money Laundering Regulation. Journal of Financial Regulation, 6(2), 238-271.