**Testimony of**

**John Breyault**
**Vice President of Public Policy, Telecommunications, and Fraud**
**National Consumers League**

**on**

# "Examining Scams and Fraud in the Banking System and Their Impact on Consumers"

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

**February 1, 2024**

## Introduction

The National Consumers League appreciates the opportunity to provide the committee with our views on protecting consumers from fraud involving misuse of the banking system.

Founded in 1899, the National Consumers League ("NCL") is the nation's pioneering consumer and worker advocacy organization. Our non-profit mission is to advocate on behalf of consumers and workers in the United States and abroad.[1] For more than twenty-five years, NCL has worked, via our Fraud.org campaign, to educate consumers about the warning signs of fraud and promote public policies that protect the American public from scams of all kinds.

## Fraud Involving Peer-to-Peer Platforms, Gift Cards, and Cryptocurrency Is Getting Dramatically Worse

There is an epidemic of fraud and identity theft in the United State. While the number of complaints received by the Federal Trade Commission ("FTC") has leveled off since hitting a record of 5.96 million in 2021 during the height of the COVID-19 pandemic, complaint levels remain unacceptably high. Nearly 5.2 million consumers submitted complaints in 2022, according to the FTC.[2] And while fewer complaints may suggest that the situation is improving somewhat, scammers are getting better at extracting more money from their victims. From 2020-2022, fraud losses increased from $3.3 billion to a staggering $8.8 billion. Median fraud losses more than doubled from $311 to $650.

When NCL last testified before this committee in 2021, we warned that peer-to-peer ("P2P") payment platforms such as Zelle, Venmo, Cash App, and PayPal had become

[1] For more information, visit www.nclnet.org.
[2] Federal Trade Commission. Consumer Sentinel Data Book 2022 (February 2023) Pg. 6. Online: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf

"payment methods of choice for scammers." Unfortunately, the problem has only worsened since then. In 2020, the FTC received 62,000 complaints where payment apps were the method of payment, with total reported losses of $87 million.[3] By 2022, reported losses from fraud involving payment apps had grown to $163 million.[4] We anticipate that when the FTC report its 2023 fraud data, this regrettable trend will only continue.

The situation is similarly dismal when it comes to fraud involving one of scammers' other favorite payment methods: gift cards. In 2020, the FTC received 43,242 complaints where a gift card was the method of payment, with reported losses of $124 million.[5] In 2022, complaints rose to 48,800 with losses nearly doubling to $228 million.[6] Even NCL itself was recently targeted by scammers who tried to get our staff to purchase gift cards by impersonating our CEO. Despite the relative savvy of our staff, several considered going out and buying gift cards, scratching off the back and sending the codes as the scammers asked.

An explosion in the fraudulent use of cryptocurrency as a payment method should be of particular concern to the committee. Since the FTC first began tracking it as a payment method in 2020, losses involving cryptocurrency payments have ballooned from $129 million to $1.59 billion in 2022—a tenfold increase in just two years. Complaints received at NCL's Fraud.org website last year were littered with references to fraudulent cryptocurrency investment schemes, and such scams were by far the costliest type of fraud for their victims.[7] Law enforcement agencies like

[3] Federal Trade Commission. Consumer Sentinel Network Data Book 2020. (February 2021) Pg. 11. Online: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf
[4] Federal Trade Commission. Consumer Sentinel Data Book 2022 (February 2023) Pg. 11. Online: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf
[5] Federal Trade Commission. Consumer Sentinel Network Data Book 2020. (February 2021) Pg. 11. Online: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf
[6] Federal Trade Commission. Consumer Sentinel Data Book 2022 (February 2023) Pg. 11. Online: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf
[7] National Consumers League. *2024 Top Ten Scams Report.* (Forthcoming, February 2024)

the Federal Bureau of Investigation have reported similar spikes in cryptocurrency scam losses.[8]

All consumers, of every age, income, and education level are vulnerable to falling victim to professional criminal fraudsters. Unfortunately, fraud is a chronically underreported crime due in part to the stigma too often directed at fraud victims.[9] While these numbers are sobering, they are almost certainly a significant undercount of the true scope of the fraud.

**Consumers Should Not Shoulder the Costs of Financial Fraud Alone**

This data makes clear that we are not winning the fight against fraud. A common thread running through P2P, gift cards, and cryptocurrency is that once funds are sent, they are available to scammers on the other end of the transaction nearly instantaneously. And when a victim discovers the fraud, it is extremely difficult to recover lost funds. From a scammer's point of view, this is exactly why payment methods like these are so attractive in the first place. Through NCL's Fraud.org campaign, we know that consumers are not only bewildered at becoming a victim of fraud, but also outraged that the companies to whom they entrusted their money do so little to protect their customers' interests or help make them whole.

While P2P platforms, banks, and cryptocurrency trading platforms profit from ever-increasing transaction volumes, they bear little of the costs of fraud that occur on their systems. Instead, the liability for fraud falls on those who can least afford to absorb the losses — individual consumers. The costs of fraud to individual victims can be life-altering. Nearly every day, NCL's fraud counselors hear stories from

[8] Lyngaas, Sean and Rabinowitz, Hannah. "FBI says $10 billion lost to online fraud in 2022 as crypto investment scams surged," CNN.com. (March 13, 2023) Online: https://www.cnn.com/2023/03/13/politics/fbi-online-fraud-report/index.html
[9] Ianzito, Christina. "Let's Stop Blaming Scam Victims, New AARP Report Says." AARP. (July 21, 2022) Online: https://www.aarp.org/money/scams-fraud/info-2022/victim-blaming.html

consumes of how scams erased victims' life savings and caused deep trauma. We clearly need better solutions.

No amount of consumer education, better disclosure, or "friction" put into payment flows will solve this problem alone. We believe the payment platforms where fraud occurs must have a bigger financial incentive to stop scams before they happen. By spreading risk across all the participants in this system, the costs can be better absorbed, resulting in a safer and more secure payments marketplace.

A model for consumer protection for P2P apps and gift cards should be credit and debit cards. Thanks to the Electronic Funds Transfer Act ("EFTA") and Fair Credit Billing Act ("FCBA"), consumers typically shoulder none of the risk when there is unauthorized use on their credit or debit cards. Instead, fraud risks are shared across issuing and receiving banks, card networks, and merchants. As a result, card networks are protected by 24/7 fraud monitoring, with more secure payment technologies such as chip-and-PIN and tap-to-pay regularly replacing older, out of date technology.

From a consumer's perspective this works well. Consumers typically first become aware that fraud has occurred on their credit or debit cards when they receive communication from their bank letting them know that their card has been compromised and will need to be replaced. Unfortunately, because many of the scams involving P2P apps and gift cards involve consumers being induced into authorizing a transaction, banks and payment platforms usually refuse to bear liability for this fraud, resulting in a far less secure payment system.[10]

**Fixing the "Unauthorized Transactions" Loophole in EFTA Should Be a Priority**

[10] Mierzwinski, Ed et al. Virtual Wallets, Real Complaints. MASSPIRG Education Fund. June 2021. Pg. 9. Online: https://masspirg.org/sites/pirg/files/reports/MA_wallets.pdf

To meaningfully reduce fraud on P2P apps and gift cards, a multi-faceted approach will be required, including better information sharing among stakeholders in the payments ecosystem and more fraud-fighting resources and authorities for law enforcement agencies. Congress can and should play a leading role in this effort by strengthening EFTA so that it protects consumers who are victims of induced fraud. Already, pressure from Congress has led Zelle to take some initial steps to protect victims of impersonation scams.[11] However, voluntary actions by one actor in the payments ecosystem is no substitute for robust safeguards that protect consumers no matter what payment technology they use. Congressional action is urgently needed to address the rising costs of fraud to consumers.

NCL supports the legislative policy proposals that the National Consumer Law Center included in their written testimony for this hearing. We urge Congress to give special priority to passing legislation, such as the Protecting Consumers From Payment Scams Act,[12] to expand the definition of "unauthorized electronic fund transfer" in the Electronic Funds Transfer Act to cover fraudulently induced payments. This simple fix would address fraudulently induced payments on all payment platforms covered by EFTA, including P2P apps and gift cards. Recently enacted rules in the United Kingdom require banks to reimburse victims of fraud in the inducement, with issuing and receiving banks sharing liability for making victims whole.[13] The UK's rules should serve as a model for U.S. law in this area.

**The Explosion in Cryptocurrency-Related Scams Must Be Addressed**

[11] Lang, Hannah. "Payments app Zelle begins refunds for imposter scams after Washington pressure," Reuters. (November 13, 2023) Online: https://www.reuters.com/technology/cybersecurity/payments-app-zelle-begins-refunds-imposter-scams-after-washington-pressure-2023-11-13/

[12] Online: https://democrats-financialservices.house.gov/UploadedFiles/BILLS-117pih-ProtectingConsumersFromPaym-U1.pdf

[13] Payment Systems Regulator (UK). "PSR confirms new requirements for APP fraud reimbursement. Press release. (July 6, 2023) Online: https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/

Cryptocurrency will soon become, and by some estimates already *is*, the payment method of choice for criminal scammers. Driven by the mania for Bitcoin and other cryptocurrencies, as many as 34,000 cryptocurrency kiosks (also known at "BTMs") have been placed in convenience stores, malls, smoke shops, laundromats, and grocery stores around the country.[14]

The proliferation of the kiosks in relatively insecure retail locations has made them a favorite tool of scammers.[15] At Fraud.org we often see complaints where scammers direct victims to their closest convenience store to deposit cash into the criminals' cryptocurrency wallets. Kiosk operators, one of whom was reportedly making a 20% commission on every transaction,[16] lack sufficient incentives to crack down on these scams.

More must be done to protect consumers from scammers using BTMs. Simply relying on better disclosures or under-trained retail employees will not meaningfully reduce fraud rates. Congress must act. To this end, NCL supports policies that:

- Require cryptocurrency kiosk operators to provide regulators the physical addresses of any crypto BTM's they operate;

- Require cryptocurrency kiosk operators to abide by longstanding anti-money laundering and know-your-customer requirements, including ID verification for parties involved in a transaction;

[14] Oguz, Kaan. "Why bitcoin ATMs are taking over malls and gas stations across the U.S." CNBC.com. (November 7, 2023) Online: https://www.cnbc.com/video/2023/11/07/why-bitcoin-atms-are-taking-over-malls-and-gas-stations-across-the-us.html
[15] Duncan, Jericka, et al. "Unregulated crypto ATMs give criminals a loophole to prey on unsuspecting victims," CBS News. (March 22, 2023) Online: https://www.cbsnews.com/news/crypto-atm-scams-unregulated-machines/
[16] Anderson, Zach. "Bitcoin of America indicted for operating unlicensed kiosks," Blockchain News. (March 7, 2023) Online: https://blockchain.news/news/bitcoin-of-america-indicted-for-operating-unlicensed-kiosks

- Require businesses that host cryptocurrency kiosks to provide training to their employees on how to spot and intervene in likely fraud involving crypto ATMs; and

- Require businesses that host cryptocurrency kiosks to prominently display warnings about the risks associated with depositing cash into crypto ATMs, especially when the funds will go to digital wallets the consumer does not own.

Senator Warren's Digital Asset Anti-Money Laundering Act of 2023 includes many of these protections and would do much to begin cracking down on the use of cryptocurrency as a payment method for fraudsters.[17] Her bill has NCL's full support and we urge the Committee to approve it.

**Conclusion**

Chairman Brown, Ranking Member Scott, and the members of the committee, we thank you for your continuing work to protect consumers and for holding this hearing. On behalf of the National Consumers League, thank you for including the consumer perspective as you consider these important issues.

[17] Senator Elizabeth Warren. "Warren Expands Coalition of Banking Committee Support for Bill Cracking Down on Crypto's Use in Money Laundering, Drug Trafficking, Sanctions Evasion." Press release. (December 11, 2023) Online: https://www.warren.senate.gov/newsroom/press-releases/warren-expands-coalition-of-banking-committee-support-for-bill-cracking-down-on-cryptos-use-in-money-laundering-drug-trafficking-sanctions-evasion