

“Fraud in Focus: Exposing Financial Threats to American Families”
**Oversight and Investigations Subcommittee of the U.S. House Financial
Services Committee**

Thursday, September 18, 2025

Testimony of Carla Sanchez-Adams

**National Consumer Law Center
on behalf of its low-income clients**



“Fraud in Focus: Exposing Financial Threats to American Families”

Oversight and Investigations Subcommittee of the U.S. House Financial Services Committee

Testimony of Carla Sanchez-Adams
Thursday, September 18, 2025

Executive Summary	2
I. Fraud Is a National Threat That Affects Everyone.	5
II. Payment Systems and Telecommunication and Social Media Companies Play an Important Role in Enabling or Preventing Fraud and in Protecting Consumers.	6
III. Person-to-Person (P2P) Payment Fraud.	7
A. The prevalence of P2P use and the incidence of fraud on these platforms.	7
B. How technology perpetuates P2P fraud and theft.	9
C. Current ambiguity in the law leaves consumers insufficiently protected from P2P fraud.	10
D. Responsibility of receiving institutions.	11
E. Problems with P2P apps when consumers make mistakes.	12
F. Potential remedies to address P2P payment fraud.	13
1. Update the Electronic Funds Transfer Act.	13
2. Consider the United Kingdom as an example.	13
3. When liability is split between sending and receiving institutions and not pushed onto consumers, more will be done to protect consumers.	15
4. Address the lack of oversight for certain parties involved in the payments market.	17
IV. Fraud through Crypto-Assets.	17
A. Crypto-assets are a common payment method for criminal fraudsters.	17
B. Crypto companies must be subject to the same BSA requirements as banks.	18
C. Stablecoins and crypto-assets must be subject to consumer protection statutes such as the EFTA when used for consumer payments.	20
V. Bank-to-Bank Wire Transfer Fraud.	20
A. Consumers are devastated by bank-to-bank wire transfer fraud.	20
B. Technology enables more bank-to-bank wire transfer fraud.	24
C. Banks claim bank-to-bank wire transfers are exempt from the EFTA, leaving consumers exposed to losing thousands of dollars.	24
D. Potential remedies to address bank-to-bank wire fraud.	26

VI. Check Fraud.	27
A. Check alteration fraud is on the rise.	27
B. Though some protections exist for consumers harmed by check fraud, they are often left scrambling.	28
C. Potential remedies to address check fraud.	29
VII. Electronic Benefit Transfer (EBT) Card Fraud.	30
A. EBT card skimming and theft leave cardholders without any protections.	30
B. Potential remedy to address EBT card fraud.	31
VIII. Problems with the Collection of Accurate Payment Fraud Data Create an Additional Barrier to Addressing Payment Fraud.	32
A. The problem of fragmented data collection on payment fraud.	32
B. Potential remedies to address the problem of fragmented payment fraud data collection.	33
1. Interagency collaboration.	33
2. Simplify fraud reporting.	34
3. Require fraud reporting within payment systems.	35
4. Require FinCEN to update the Suspicious Activity Report (SAR) to capture information about accounts that receive fraudulent funds.	35
5. Ensure consumers are protected from false positives.	36
IX. Challenges with Account Freezes, Closures, and Holds Due to Fraud Lead to Debanking Consumers.	37
A. Overaggressive fraud algorithms can shut out innocent consumers from access to their bank accounts and funds, and overly broad BSA programs prevent these consumers from understanding why those actions were taken.	38
B. Potential remedies to address improper freezes or account closures due to the use of automated fraud detection.	40
X. Fraud Traverses Many Industries and Sectors, and the Federal Government Must Take a Holistic Approach to Combatting Fraud.	40
A. Criminal Fraudsters rely heavily on text messages to initiate fraud schemes.	40
B. Recommendations to address scams initiated by text.	41
XI. Fraud Prevention Education Is Necessary in the Fight Against Fraud, But It Will Not Solve the Problem.	43
XII. Conclusion	45

Chairman Meuser, Vice Chairman Moore, Ranking Member Green, and Members of the Subcommittee, thank you for inviting me to testify today regarding fraud and its impact on American families. I am Carla Sanchez-Adams, a senior attorney at the National Consumer Law Center. I offer my testimony on behalf of NCLC's low-income clients.

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law to work for consumer justice and economic security for low-income and vulnerable consumers in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services; and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness. NCLC has long advocated for stronger laws, regulations, and enforcement to ensure that consumers' funds and payments are safe and to prevent and remedy fraud.

I am one of the co-authors of NCLC's treatise, *Consumer Banking and Payments Law*. My colleagues and I interact with legal services, government, and private attorneys, as well as community groups and organizations from all over the country who represent low-income and vulnerable individuals on consumer issues. As a result of our daily contact with these advocates, we have seen many examples of the damage wrought by payment fraud from every part of the nation. It is from this vantage point that I supply this testimony.

NCLC has previously provided testimony before Congress on the need to address payment fraud.¹ Additionally, NCLC has provided feedback to various regulatory agencies on the same issue.² I reiterate and incorporate those comments here as well.

¹ See Testimony of Carla Sanchez-Adams, NCLC "Examining Scams and Fraud in the Banking System and Their Impact on Consumers," Hearing Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, (February 1, 2024), available at <https://www.nclc.org/wp-content/uploads/2024/02/Written-testimony-The-Problem-of-Payment-Fraud.pdf>; NCLC *et al.*, Statement for the Record, "What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments," Hearing Before the House Financial Services Taskforce on Financial Technology at 10-11, (April 28, 2022), available at https://www.nclc.org/wp-content/uploads/2022/10/Digital_Wallet_testimony.pdf; Testimony of Odette Williamson, NCLC "Fraud, Scams and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic," Hearing Before the U.S. Senate Special Committee on Aging, (September 23, 2021), available at https://www.nclc.org/wp-content/uploads/2022/08/Testimony_Covid_Aging-1.pdf.

² See NCLC, *Comments regarding the Request for Information on Potential Actions to Address Payments Fraud by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation*, (September 15, 2025), available at https://www.nclc.org/wp-content/uploads/2025/09/2025.09.15_Comments_Fraud-RFI-on-Payments-Fraud.pdf; NCLC, *Comments regarding the Expansion of Fedwire Funds Service and National Settlement Operating Hours*, (September 6, 2024), available at https://www.nclc.org/wp-content/uploads/2024/11/2024.09.06_Comments_NSS-Comments.pdf; NCLC, *Comments regarding FinCEN's Rulemaking on Anti-Money Laundering and Countering the Financing of Terrorism Programs*, (September 3, 2024), available at https://www.nclc.org/wp-content/uploads/2024/09/2024.09.03_Comments_FinCEN-Dept-Treasury-on-AML-Rulemaking.pdf; NCLC *et al.*, *Comments regarding the FTC Collaboration Act of 2021*, (August 14, 2023), available at https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final3-Lauren-Saunders.pdf; NCLC *et al.*, *Letter Urging Federal Reserve Board to Prevent FedNow Errors and Fraud*, (August 10, 2022), available at https://www.nclc.org/wp-content/uploads/2022/09/FedNow_fraud_ltr.pdf; *Comments of 43 consumer,*

Executive Summary

Fraud continues to pose a threat to U.S. households, businesses, financial institutions, and the economy as a whole. In 2024, consumers reported over \$12.5 billion fraud losses to the Federal Trade Commission,³ though total fraud losses are far higher. According to the Pew Research Center, 73% of U.S. adults have experienced some kind of online scam or attack, and one in five U.S. adults reported having lost money because of an online scam or attack.⁴ But the impacts of fraud are most keenly felt by certain vulnerable populations such as older Americans,⁵ communities of color, and low-income consumers,⁶ who have a more difficult time recovering from fraud losses.

Consumers are plagued by problems with unauthorized transactions as well as fraudulently induced payments involving peer-to-peer payment applications, crypto-assets, bank-to-bank wire transfers, check alterations and forgeries, and Electronic Benefits Transfer (EBT) card skimming. The increasing ease and use of mobile and online banking through technological advancement have also simultaneously provided opportunities for scammers to exploit newer payment technologies. However, obtaining a complete and holistic picture of the volume, loss, and threat of payment fraud is difficult because of the fragmented way we collect fraud data.

The financial institutions and companies that design and run these payment systems, including the financial institutions and companies that hold the accounts of criminal fraudsters and money mules that receive fraudulent payments, need to take more responsibility for making these systems safe and protecting consumers. Given the increasing sophistication of fraud schemes, warnings to consumers are insufficient. If payment system participants take responsibility for protecting consumers, they will have the incentive to leverage the latest innovative technologies to prevent and detect fraud and apportion liability among the various system participants, thereby making the entire system safe. At the same time, any attempts to combat fraud must also be tempered with policies and procedures that protect innocent consumers who do not engage in payment fraud but whose funds might be frozen for extended periods of time.

small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16, (September 9, 2021), available at <https://bit.ly/FedNowCoalitionComments> (“FedNow Comments”).

³ See FTC “*New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024*,” (Press Release) (March 10, 2025), available at <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>.

⁴ Anderson, Monica, Gottfried, Jeffrey, and Park, Eugenie, “*Online Scams and Attacks in America Today*,” Pew Research Center, (July 31, 2025), <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>. The Pew study found that, “nearly all Americans view online scams and attacks as a national problem. More than nine-in-ten say online scams and attacks are a problem in the country, including 79% who describe them as a major problem. Most U.S. adults have been a victim of an online scam or attack. We find that 73% of U.S. adults have ever experienced things like credit card fraud, ransomware or online shopping scams.”

⁵ According to the Federal Trade Commission, though younger people (ages 20-29) reported losing money to fraud more often than older people in 2024, those aged 70+ had a higher median loss than those aged 20-29 (\$1,650 compared to \$417). See

<https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic>.

⁶ *Id.* “Black, Hispanic and Asian adults are more likely than White adults to say they have lost money because of an online scam or attack, (and) those with lower incomes (26%) are more likely than those in upper-income households (15%) to say they have lost money in this way. Those in middle-income households fall in between the two other groups (20%).”

Telecommunication companies, including VOIP providers and aggregators, and social media platforms must also take responsibility for keeping criminals off their systems. Most frauds start with a text or a fraudulent social media post on a marketplace or other platform.

To combat payment fraud, we recommend addressing the current gaps and ambiguities in the Electronic Funds Transfer Act (EFTA) that leave consumers unprotected. These include:

- Ensuring consumers are protected from liability when they are defrauded into initiating a transfer;
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the criminal fraudster to receive the fraudulent payment;
- Ensuring that the EFTA applies to stablecoins and crypto-assets when used for consumer payments;
- Eliminating the exemptions for bank wire transfers⁷ and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Eliminating the exclusion of EBT cards from the EFTA, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Clarifying that the EFTA's error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient;
- Clarifying that the error resolution duties under the EFTA apply if a consumer's account is frozen or closed, or the consumer is otherwise unable to access their funds, with an exception if the consumer was denied access due to a court order or law enforcement, or the consumer obtained the funds through unlawful or fraudulent means; and
- Considering whether consumer protections for checks should be included in the EFTA.

Federal regulators should also take additional steps to address fraud and protect innocent consumers who are harmed by fraud. For example, federal regulators should:

- Enforce and strengthen laws that require financial institutions and other companies to protect consumers from unauthorized and fraudulently induced charges, especially when EFTA violations occur;
- Devote more attention to the responsibilities of institutions that receive fraudulent payments, including stepping up enforcement of Bank Secrecy Act /Anti-Money Laundering obligations;
- Establish interagency collaboration to assist consumers with reporting fraud, collecting data on fraud, and establishing systems for sharing fraud data and findings; and
- Provide guidance to financial institutions about the timelines and procedures for consumers to regain access to improperly frozen funds, including providing clarity about

⁷ As discussed below, Regulation E exempts some wire transfers, though a court has held that that exemption may not apply in every circumstance.

what information can and should be given to accountholders regarding account closures and freezes.

Congress should also pass legislation and work with the Federal Communications Commission (FCC) to address the role that telecommunications providers play in facilitating fraud. Some of these measures include:

- Requiring a bond for transmitters of phone calls and texts.
- Requiring rigorous know-your-customer and know-your-traffic procedures that force carriers to vet callers and calls that transit their network.
- Requiring record-keeping for call originators to ensure that information about callers is available for government or private enforcement efforts.
- Requiring carriers to investigate call traffic that displays suspicious characteristics, like a high percentage of short-duration calls and other indicia of fraud.
- Adopting federal regulations for phone number resellers to address phone number rotation schemes that allow callers to undermine the goals of the STIR/SHAKEN framework.
- Authorizing the FCC to file actions for civil penalties in federal district courts.
- Strengthening the Telephone Consumer Protection Act (TCPA) to encourage robust enforcement against scam callers and those who facilitate fraud.
- Strengthening the Telemarketing Sales Rule (TSR) to expand enforcement.

In the testimony below, I will focus on five payment vehicles that have seen increasing fraud: person-to-person payments, crypto-assets, bank-to-bank wire transfers, check alterations, and Electronic Benefit Transfer cards. I will discuss how these payment frauds impact consumers and how protections can be improved. I will also discuss additional measures needed to combat fraud, such as improving data collection and addressing the problem of false positives when innocent consumers are impacted by account closures or freezes due to fraud.

I. Fraud Is a National Threat That Affects Everyone.

Fraud continues to climb and devastates millions of consumers across the country each year. In 2022, the Federal Trade Commission (FTC) received more than 2.5 million reports of fraud with reported losses totaling almost \$9 billion (\$8,996,000) from its Consumer Sentinel Network.⁸ Those losses were up a shocking 46.7% from 2021. And in just two years (2024), that amount rose to a little over 2.6 million reports of fraud totaling approximately \$12.8 billion in losses, a 42.2% increase in dollars lost.⁹

Additionally, the FTC numbers reflect only fraud cases reported to the Consumer Sentinel Network. Fraud is substantially underreported; only a small percentage of U.S. fraud victims report the fraud to law enforcement.¹⁰

As AARP noted:

“While nearly nine in 10 respondents (87%) feel people should report incidents of fraud, only an estimated 15% contact law enforcement. The gap may be tied to attitudes and awareness about fraud. Sometimes those who have been victimized by a scam feel embarrassed, guilty, or believe there is nothing police can do.”¹¹

Fraud impacts all of us, across every community— the young and the old, those with higher and lower household incomes, as well as the highly educated and those with lower levels of formal education.¹²

While the common belief is that older consumers are more likely to be susceptible, in fact younger people are also significantly likely to experience fraud. But when older people suffer fraud, they lose far more money, as shown by the following FTC chart:¹³

⁸ FTC, Fraud Reports by Amount Lost, *available at* <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses>.

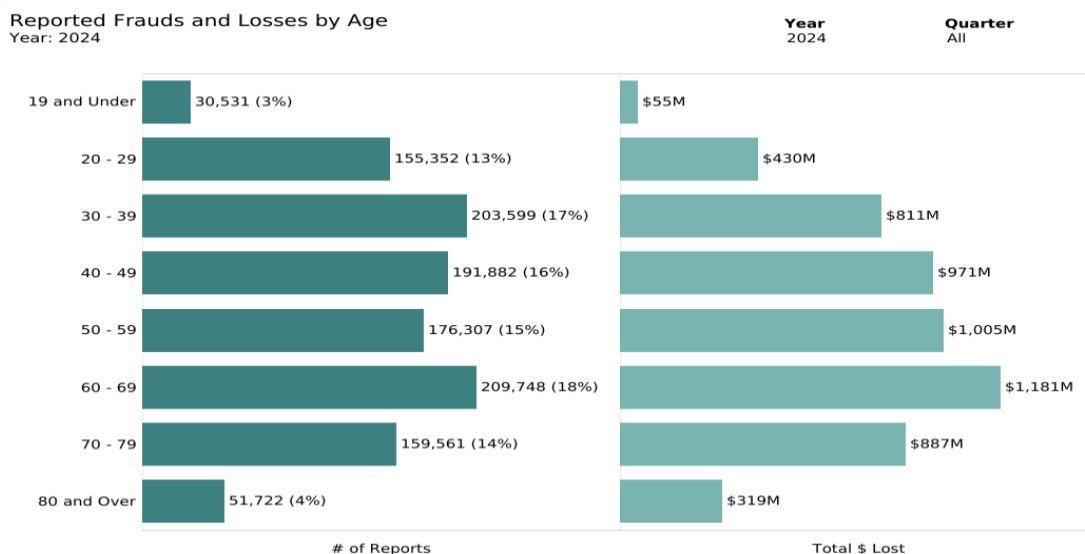
⁹ *Id.*

¹⁰ Anderson, Monica, Gottfried, Jeffrey, and Park, Eugenie, “Online Scams and Attacks in America Today,” Pew Research Center, (July 31, 2025), *available at* <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>. The Pew study found that roughly three-quarters of the survey group did not report to law enforcement that they lost money from an online scam or attack, while only 26% said they had informed law enforcement. *See also* Department of Justice, U.S. District Attorney’s Office, District of Alaska, Financial Crime Fraud Victims, (2020), *available at* <https://www.justice.gov/usao-ak/financial-fraud-crimes>.

¹¹ Williams, Alicia R., “Americans Are Aware of Fraud’s Pervasiveness but Remain Vulnerable,” AARP Research, (May 17, 2023), *available at* <https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/fraud-awareness-older-adults/>; *see* Department of Justice, U.S. District Attorney’s Office, District of Alaska, Financial Crime Fraud Victims, (2020), *available at* <https://www.justice.gov/usao-ak/financial-fraud-crimes>.

¹² Anderson, Monica, Gottfried, Jeffrey, and Park, Eugenie, “Online Scams and Attacks in America Today,” Pew Research Center, (July 31, 2025), *available at* <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>. *See also* Levinthal, Dave, “Cyberthieves stole \$186,000 from a Republican member of Congress as fraud epidemic plagues political committees,” Business Insider, (November 29, 2022), *available at* <https://www.businessinsider.com/online-fraud-congress-diana-harshbarger-cybertheft-2022-11>.

¹³ FTC, Reported Fraud and Losses by Age (2024), *available at* <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses>.

Reported Frauds and Losses by Age
Year: 2024

Percentages are based on the total number of fraud reports for the quarters selected in which consumers provided their age: 1,178,702.

FEDERAL TRADE COMMISSION - ftc.gov/exploredata

Fraud has a particularly harsh impact on low-income families and communities of color, who have fewer resources to help them recover. Fraudsters often take the last dollar from those least able to afford it, and often target older adults, immigrants, and other communities of color.

II. Payment Systems and Telecommunication and Social Media Companies Play an Important Role in Enabling or Preventing Fraud and in Protecting Consumers.

Criminal fraudsters who steal money through fraud schemes need a way to contact a victim to initiate the fraud scheme and a way to obtain a victim's money. They use a variety of avenues to contact their victims, including text messages, phone calls, and contact on social media platforms. The criminal fraudsters also use a variety of payment systems to receive that money, including person-to-person (P2P) transfer services, crypto-assets, bank to-bank wire transfers, bank transfers through Zelle, checks, and gift cards. Each of these systems has a role to play in keeping criminals out, preventing fraud, and protecting consumers. Fraud does not succeed if the fraudster cannot contact a victim or if the fraudster cannot receive the money.

Fraud may result in unauthorized transactions or fraudulently induced transactions, each with different protections. After obtaining information through phishing schemes, fraud schemes, or data breaches, criminals may make unauthorized transactions for which consumers generally have protection (though, in some cases, imperfect protection, as discussed below). Checks can also be stolen and altered, another form of unauthorized transaction. Or criminals can defraud a consumer into making a fraudulently induced transaction where protection is sorely lacking.

As discussed in more detail below, payment fraud usually involves at least two institutions – the institution that holds the fraud victim's account (the consumer's institution)¹⁴ and the institution

¹⁴ Though businesses can also be the victims of fraud, this testimony will focus on consumers and consumer protection.

that receives the stolen funds and holds the account of the fraudster or money mule (the receiving institution). When seeking to prevent and remedy fraud, it is important to focus on the responsibilities of both the consumer's institution and the receiving institution as well as the payment system itself, regardless of whether the fraud is unauthorized or fraudulently induced. When consumers are protected, these institutions and systems will have incentives to use their resources and technological innovations to prevent fraud and make everyone safer.

III. Person-to-Person (P2P) Payment Fraud.

A. The prevalence of P2P use and the incidence of fraud on these platforms.

Person-to-person (P2P) payment apps have become increasingly popular among consumers. According to the Atlanta Federal Reserve, as of 2023, almost three-quarters of U.S. consumers used payment accounts such as PayPal, Venmo, Zelle, and Cash App in 2023.¹⁵ In addition to P2P payment services, consumers are also increasingly adopting other forms of technology to make payments.¹⁶ P2P payment systems, if properly designed, can provide broad benefits to consumers. But those benefits will only be realized if the systems are safe to use.

According to the FTC, “payment app or service” is the second largest category of payment method specified by fraud victims in terms of number of reports (after credit cards) for all of 2024, and the largest category of payment method specified by fraud victims in terms of number of reports for the first two quarters of 2025.¹⁷ The Consumer Financial Protection Bureau (CFPB) has also seen high growth in complaints about fraud in P2P apps and digital wallets.¹⁸

As consumer, small business, civil rights, community, and legal service groups described at greater length in comments submitted to the Federal Reserve Board (FRB) and the CFPB, the existing P2P payment systems of large technology companies and financial institutions simply are not safe for consumers to use.¹⁹ The news media has reported many of the fraudulent

¹⁵ Federal Reserve Bank of Atlanta, *2023 Survey and Diary of Consumer Payment Choice: Summary Results*, (June 2024), available at https://www.atlantafed.org/-/media/documents/banking/consumer-payments/survey-diary-consumer-payment-choice/2023/sdcpc_2023_report.pdf.

See Federal Trade Commission, *New FTC Data Show Consumers Reported Losing Nearly \$8.8 Billion to Scams in 2022*, (Press Release) (February 23, 2023), available at <https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022>

¹⁶ Chen, Jane, Deepa Mahajan, Marie-Claude Nadeau, and Roshan Varadarajan, “*Consumer Digital Payments: Already Mainstream, Increasingly Embedded, Still Evolving*,” Digital Payments Consumer Survey, (October 20, 2023), available at <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving>.

¹⁷ FTC fraud reports by payment method, available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>. The FTC can identify the payment method that the criminal used in only a small fraction of fraud reports, and fraud is underreported in general, so the FTC's numbers vastly understate the amount of fraud facilitated by Payment app or service.

¹⁸ U.S. PIRG Educ. Fund, *Virtual Wallets, Real Complaints*, at 2, (June 2021), available at https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

¹⁹ See *Comments of 65 Consumer, Civil Rights, Faith, Legal Services and Community Groups to CFPB on Big Tech Payment Platforms* at 4-5, Docket No. CFPB-2021-0017, (December 21, 2021), available at <https://bit.ly/CFPB-BTPS-comment> (“CFPB Big Tech Payment Platform Comments”); *Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by*

schemes enabled by the P2P systems.²⁰ Generally, these scams and theft would not have been possible without the payment apps.

P2P fraud has a particularly harsh impact on low-income families and communities of color. These communities, already struggling and often pushed out of the traditional banking system, can least afford to lose money to scams and errors. Because many people of color and immigrant communities are also unbanked or underbanked,²¹ they are the target audience for use of many of the P2P apps. For example, a September 2022 Pew Research Center survey shows that 59% of Cash App users are Black and 37% are Hispanic.²²

Yet Cash App has also been subject to reports of widespread fraud,²³ failing to protect the very vulnerable populations it targets. As a result, 48 state regulators obtained a consent order against Block, the operator of Cash App. The CSBS order required Block to pay \$80 million and “undertake corrective action for violations of the Bank Secrecy Act (BSA) and anti-money laundering (AML) laws that safeguard the financial system from illicit use.”²⁴ Similarly, the CFPB ordered Block to pay \$175 million and to fix its failures after finding that Block failed to take timely, appropriate, and effective measures to prevent, detect, limit, and address fraud on the Cash App platform.²⁵

Zelle is another popular P2P payment service, but users transfer funds between bank accounts directly.²⁶ As more and more consumers have used Zelle, the service also has become popular among criminals.²⁷ As a result of the many complaints relating to payment fraud on Zelle, the

Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16, (September 9, 2021), available at <https://bit.ly/FedNowCoalitionComments> (FedNow Comments).

²⁰ Morales, Mark, “Venmo and other payment app theft is ‘skyrocketing,’ Manhattan DA warns,” CNN, (January 23, 2024), available at https://www.cnn.com/2024/01/23/business/venmo-payment-app-theft?cid=ios_app; Johnson, Tia, “Kansas City woman warns others after losing nearly \$2,000 in rental home scam,” Fox4, (May 3, 2021), available at <https://fox4kc.com/news/kansas-city-woman-warns-others-after-losing-nearly-2000-in-rental-home-scam/>; Cioppa, Jordan, “James Island woman says rental scam cost her \$2,600,” WCBD News2, (January 10, 2023), available at <https://www.counton2.com/news/james-island-woman-says-rental-scam-cost-her-2600/>.

²¹ 11.3 percent of Black and 9.3 percent of Latino households are unbanked compared to only 2.1% of white households. See FDIC, *2021 FDIC National Survey of Unbanked and Underbanked Households*, at 2, available at <https://www.fdic.gov/analysis/household-survey/2021report.pdf> (last updated July 24, 2023).

²² Anderson, Monica, “Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users,” Pew Research Center, (September 8, 2022), available at <https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/>.

²³ Hindenburg Research, “Block: How Inflated User Metrics and ‘Frictionless’ Fraud Facilitation Enabled Insiders To Cash Out Over \$1 Billion,” (March 23, 2023), available at <https://hindenburesearch.com/block/>. (“Former employees estimated that 40%-75% of accounts they reviewed were fake, involved in fraud, or were additional accounts tied to a single individual”).

²⁴ CSBS, “State Regulators Issue \$80 Million Penalty to Block, Inc., Cash App for BSA/AML violations,” (Press Release) (January 15, 2025), available at <https://www.csbs.org/newsroom/state-regulators-issue-80-million-penalty-block-inc-cash-app-bsaaml-violations>.

²⁵ *In re. Block, Inc.*, CFPB No. 2025-CFPB-0001, (January 16, 2025) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_block-inc-consent-order_2025-01.pdf.

²⁶ The FTC designates Zelle transfers as part of the “bank transfer or payment” category, which also includes bank-to-bank wire transfers. See Section V.A of this testimony for FTC statistics on “bank transfer or payment,” also available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

²⁷ Cowley, Stacy and Nguyen, Lananh, “Senators question Zelle over how it is responding to reports of rising

CFPB filed suit against Early Warning Systems (EWS) (the operator of Zelle), Bank of America, JPMorgan Chase, and Wells Fargo, alleging violations of the EFTA and violations of the Consumer Financial Protection Act. The CFPB alleged these players knowingly rushed the launch of Zelle “without implementing effective consumer safeguards.”²⁸

However, with the change in Administration and the change of leadership at the Agency, the CFPB dismissed the suit. In the wake of the dismissal, the New York Attorney General filed suit against EWS on August 13, 2025.²⁹ The NY AG seeks restitution for New Yorkers who were harmed by Zelle, which “failed for years to set up anti-fraud features, allowing criminal fraudsters to steal more than \$1 billion from users between 2017-2023.”³⁰

B. How technology perpetuates P2P fraud and theft.

Fraudsters have extraordinary creativity; they are constantly developing creative ways to steal people’s money by setting up increasingly sophisticated schemes to obtain access to accounts or to fraudulently induce consumers into payment transactions.³¹ The Federal Communication Commission’s (FCC) website includes a Scam Glossary detailing dozens of different ways individuals and small businesses have lost money to these schemes,³² and the FCC specifically identified P2P apps as a primary means for executing scams and fraud.³³ Clearly, the warnings provided by the payment apps themselves to beware of scams and fraud are not adequate to protect consumers from the losses.

Additionally, with imposter scams topping the FTC’s category of fraud type for the last five years,³⁴ the use of deep fakes generated by artificial intelligence (AI) to perpetuate payment

fraud,” New York Times, (April 26, 2022), available at <https://www.nytimes.com/2022/04/26/business/zelle-fraud.html>; Pradelli, Chad, “‘I still don’t know how they got access’: Woman loses thousands after thief targets her Zelle app,” ABC Action News, WMPVI-TV Philadelphia, PA (June 2, 2023), available at <https://6abc.com/zelle-peer-to-peer-payment-apps-theft-auto-payments/13335405/>; See CBS This Morning, “Complaints against mobile payment apps like Zelle, Venmo surge 300% as consumers fall victim to more money scams,” CBS News, (June 23, 2021), available at <https://www.cbsnews.com/news/venmo-payal-zelle-cashapp-scams-mobile-payment-apps/>.

²⁸ CFPB, “CFPB Sues JPMorgan Chase, Bank of America, and Wells Fargo for Allowing Fraud to Fester on Zelle,” (Press Release) (December 20, 2024), available at <https://www.consumerfinance.gov/about-us/newsroom/cfpb-sues-jpmorgan-chase-bank-of-america-and-wells-fargo-for-allowing-fraud-to-fester-on-zelle/>.

²⁹ *People of the State of New York v. Early Warning Services*, (Supreme Court of the State of New York, Country of New York), complaint available at <https://ag.ny.gov/sites/default/files/court-filings/people-of-the-state-of-new-york-v-early-warning-services-llc-complaint-2025.pdf>.

³⁰ New York State Attorney General, *Attorney General James Sues Company Behind Zelle for Enabling Widespread Fraud*, (Press Release) (August 13, 2025), available at <https://ag.ny.gov/press-release/2025/attorney-general-james-sues-company-behind-zelle-enabling-widespread-fraud>.

³¹ See NCLC, EPIC report *Scam Robocalls: Telecom Providers Profit*, at 6-10, (June 2022), available at <https://www.nclc.org/wp-content/uploads/2023/02/Robocall-Rpt-23.pdf> for examples of the types of scams utilized by robocalls and scam texts; see also Testimony of Margot Saunders, NCLC “Protecting Americans from Robocalls,” Hearing Before the U.S. Senate Committee on Commerce, Science & Transportation, (October 24, 2023), available at <https://www.nclc.org/wp-content/uploads/2023/10/Testimony-of-NCLC-on-Robocalls-2023.pdf>.

³² Federal Communications Commission, Scam Glossary, available at <https://www.fcc.gov/scam-glossary>.

³³ Federal Communications Commission, “As More Consumers Adopt Payment Apps, Scammers Follow,” (updated February 25, 2021), available at <https://www.fcc.gov/more-consumers-adopt-payment-apps-scammers-follow>.

³⁴ Federal Trade Commission Fraud Reports by Report Type, Top Reports, available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses>.

fraud is disconcerting.³⁵ NCLC joined numerous nationwide and state advocacy organizations in sending a letter to the FTC and the CFPB on the threat of AI-generated deep fakes used for financial fraud.³⁶

C. Current ambiguity in the law leaves consumers insufficiently protected from P2P fraud.

The Electronic Fund Transfer Act (EFTA) and its implementing Regulation E protect consumers when problems with electronic funds transfers, such as P2P transactions, occur. The law provides consumers with remedies for P2P fraud when it is unauthorized, such as when a criminal defrauds a person into turning over account credentials and then the criminal commits an unauthorized transfer. The definition of “unauthorized transfer” under Regulation E is a 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.”³⁷

However, the response to consumer complaints about unauthorized payments by some of the largest players in the P2P market is inconsistent at best and possibly non-compliant.³⁸ It is unfortunately too common for financial institutions to fail to comply with the unauthorized use protections of the EFTA and deny reimbursement on improper grounds.³⁹

The response to P2P payment fraud becomes even more problematic when it involves claims of

³⁵ See FBI, Public Service Announcement Alert Number: I-120324-PSA “*Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*,” (December 3, 2024), available at <https://www.ic3.gov/PSA/2024/PSA241203>; U.S. Department of Homeland Security, *Increasing Threat from Deepfake Identities*, (2021), available at https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf. See also van der Linde, Ileana, *AI scams, deep fakes, impersonations ... oh my!* JPMorgan Wealth Management, (July 10, 2025), available at <https://www.jpmorgan.com/insights/fraud/fraud-protection/ai-scams-deep-fakes-impersonations-oh-my>; Schwartz, Christopher and Wright, Matthew, “*Voice Deepfakes Are Calling. Here’s How to Avoid Them*,” Gizmodo, (March 24, 2023), available at <https://gizmodo.com/ai-deepfake-voice-how-to-avoid-spam-phone-calls-1850245346>;

³⁶ NCLC et al., *Letter to CFPB and FTC on Threat of AI-Generated Deep Fakes Used for Financial Fraud*, (September 13, 2023), available at <https://www.nclc.org/wp-content/uploads/2023/10/Deepfake-based-financial-fraud-letter-to-CFPB-and-FTC.pdf>.

³⁷ 12 C.F.R. § 1005.2(m) (emphasis added).

³⁸ Brown, Sherrod, Elizabeth Warren, and Jake Reed, “*Brown, Reed, Warren Urge Venmo, Cash App to Reimburse Victims of Fraud and Scams | United States Committee on Banking, Housing, and Urban Affairs*,” (December 14, 2023), available at <https://www.banking.senate.gov/newsroom/majority/brown-reed-warren-urge-venmo-cash-app-to-reimburse-victims-of-fraud-and-scams>. See also Hindenburg Research Report, “*Block: How Inflated User Metrics and ‘Frictionless’ Fraud Facilitation Enabled Insiders to Cash Out Over \$1 Billion*,” (March 23, 2023), available at <https://hindenburgresearch.com/block/>.

³⁹ See, e.g., CFPB, Supervisory Highlights at 17, (Summer 2022) (“Examiners continued to find issues with financial institutions failing to follow Regulation E error resolution procedures.... A financial institution cannot require a consumer to file a police or other documentation as a condition of initiating or completing an error investigation.”); CFPB, Supervisory Highlights at 15, (Summer 2021), available at www.consumerfinance.gov (stating that “Supervision continues to find violations of EFTA and Regulation E that it previously discussed in the Fall 2014, Summer 2017, and Summer 2020 editions of Supervisory Highlights, respectively,” (Listing several violations)); Sonbuchner, Scott, Examiner, Fed. Reserve Bank of Minneapolis, *Consumer Compliance Outlook, Error Resolution and Liability Limitations Under Regulations E and Z; Regulatory Requirements, Common Violations, and Sound Practices*, (2d issue 2021), available at www.consumercomplianceoutlook.org.

fraudulently induced payments. P2P apps disclaim responsibility to protect consumers from fraudulently induced transactions, even though those payments go to accounts held at the same P2P app. Similarly, most banks will deny a claim of error for a fraudulently induced transaction, though Zelle has begun reimbursing consumers for some fraudulently induced transactions resulting from certain types of imposter scams.⁴⁰

The definition of “unauthorized transfer” under Regulation E as described above contemplates a transaction that was not initiated by the consumer. If the consumer initiated the transfer, even if the consumer was defrauded into initiating the payment, financial institutions are likely to dispute their liability and may even refuse to help.

Nevertheless, some fraudulently induced transactions may fall under Regulation E’s separate error protections, such as the protection against incorrect transactions – i.e., a payment that went to an imposter – or the right to obtain information.⁴¹ The CFPB also has authority to define additional categories of error.⁴²

The disparity of treatment between unauthorized and fraudulently induced payments under Regulation E is made clear in the following two scenarios:

- *Scenario A: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie gives the caller her bank account number and routing number, and the caller uses that information to initiate a preauthorized ACH debit against her account.*
- *Scenario B: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie takes out her smartphone and sends a P2P payment to the number or email given by the caller.*

Though there is very little difference in these two scenarios, Regulation E protects Laurie in Scenario A where she can contest the debit as unauthorized. In Scenario B, financial institutions will take the position that Laurie is unprotected because she initiated the payment. The difference between how the payment was initiated in Scenario A and B does not make a scammer any more entitled to the money or make the scammer’s bank any less responsible for banking a scammer.

D. Responsibility of receiving institutions.

As discussed earlier, payments often involve two institutions: the one that sent the payment (the consumer’s institution in the P2P context) and the one that received it. While the EFTA governs only the responsibilities of the consumer’s institution, other laws and network rules give the receiving institution obligations to prevent fraud.

Scenario A described above is unlikely to occur because scammers like the fake IRS caller would be deterred from using the ACH system. The ACH system vets and monitors who is

⁴⁰ Campisi, Natalie, “Scammed Out Of Money On Zelle? You Might Be Able To Get It Back,” Forbes, (November 13, 2023), available at <https://www.forbes.com/advisor/money-transfer/zelle-users-refunded-after-scams/>.

⁴¹ 15 U.S.C. § 1693f(f)(2), (6); 12 C.F.R. § 1005.11(a)((1)(ii), (vii).

⁴² 15 U.S.C. § 1693f(f)(7).

allowed to initiate ACH payments, and the liability of a bank that initiates and receives fraudulent debit payments under both Regulation E and NACHA rules leads to stronger controls that are more likely to keep the scammer from having an account or having access to the ACH system.

But with the growth of payment apps, online bank account opening, and identity theft, it is easier for scammers to obtain accounts – potentially using stolen or synthetic identities – that they can then use to receive payments (directly or through money mules). Yet at present, the payment service or bank receiving the fraudulent payment on behalf of the scammer has no direct liability for enabling the scammer to receive the payment. As a result, that institution has less incentive to prevent the scammer from obtaining an account, put a hold on access to suspicious payments, or shut down the account quickly.

If consumers had more remedies against fraudulently induced transactions, payment network rules could pass liability in whole or in part back to the institution that holds the fraudster or money mule account, which would help to correct these incentives. This is what the United Kingdom has done, as discussed below.

Consumer complaints of P2P fraud will continue to escalate because the current systems impose insufficient responsibility on system operators and financial institutions to protect consumers against fraudulent schemes. Given what we know about how fraudsters target opportunities with the least resistance, it stands to reason that fraudulently induced payment fraud will continue to plague P2P systems if payment systems and financial institutions are allowed to operate under the assumption that they are not liable.

E. Problems with P2P apps when consumers make mistakes.

Beyond fraudulently induced payments and unauthorized payments, P2P payment apps and financial institutions typically refuse to help consumers who accidentally send money to the wrong person or the wrong account – mistakes that are easy to make in payment services designed for convenience and speed over safety. For example, consumers can send money through P2P systems using nothing more than a cell phone number to identify the recipient.

Here are other examples:

- An employee of NCLC unexpectedly saw \$1,000 arrive in his bank account through Zelle. A few minutes later, he received a frantic phone call from a man telling him that he had put in the wrong cell phone number and asking for the money back. The NCLC employee wanted to return the money but asked his bank for assurances that it was not a scam. The man also called his bank. Both banks (each large top-10 institutions) refused to help correct the error. After weeks of getting nowhere, the NCLC employee returned the funds on faith.
- Arthur Walzer of New York City tried to send his granddaughter \$100 through Venmo as a birthday present, but instead sent it to a woman with the same first and last name. When he discovered the error, he told his bank to refuse payment of the \$100, and in response

Venmo froze his account and demanded that he pay them. Venmo eventually refunded him, but only after a journalist contacted the company on his behalf. It was the first time he had ever used Venmo – he set up an account specifically to give his granddaughter the gift.⁴³

Regulation E imposes the duty to investigate and resolve “errors,” which includes “an incorrect electronic fund transfer to or from the consumer’s account.”⁴⁴ Nothing in the EFTA excludes consumer errors, and Regulation E should be interpreted to cover them. When a payment is sent to the wrong person or in the wrong amount, the person receiving the payment is not more entitled to the payment because the error was caused by the sender. But today, most consumers are out of luck in this situation unless their bank decides to help and the receiving bank or payee is cooperative.

F. Potential remedies to address P2P payment fraud.

1. Update the Electronic Funds Transfer Act.

The EFTA was enacted 43 years ago and as described above does not directly address many of the most important issues in the current consumer payment ecosystem. The statute was initially adopted at a time when consumers were conducting business with their own financial institutions and were using payment systems that did not lead to the same types of problems that plague today’s P2P systems.

We support legislative efforts to address the many gaps and ambiguities in the Electronic Fund Transfer Act that leave consumers unprotected. Some of these problems could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

The problem of fraudulently induced electronic transfers in P2P payments could be addressed by amending the EFTA to protect consumers from liability when they are defrauded into initiating a transfer and allow the consumer’s financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

Problems when consumers make mistakes could also be addressed by clarifying that the EFTA’s error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient.

2. Consider the United Kingdom as an example.

The United Kingdom (UK) was early to launch real time payments, and fraudulently induced payment fraud (what the UK calls authorized push payment or APP fraud) immediately

⁴³ See Elliott, Christopher, “A Venmo user sent \$100 to the wrong person. Then the payment service froze his account,” Seattle Times, (November. 2, 2020), available at <https://www.seattletimes.com/life/travel/a-venmo-user-sent-100-to-the-wrong-person-then-the-payment-service-froze-his-account-travel-troubleshooter/>.

⁴⁴ 15 U.S.C. § 1683f(f)(2); 12 C.F.R. § 1005.11(a)(1)(ii).

followed. The UK has been formally considering how to tackle the problem of P2P fraud since 2016, when the consumers association “Which?” submitted a “super-complaint”⁴⁵ to the United Kingdom’s Payments Systems Regulator (PSR).⁴⁶ The complaint identified the problem of APP fraud, which happens when scammers deceive consumers or individuals at a business to send them payment under false pretenses to an account controlled by the scammer. Which? also identified the lack of consumer protection for victims of APP fraud.

In response, a steering group was formed, comprised of regulators, consumer advocates, financial services providers and industry representatives.⁴⁷ The result was the creation of an industry code called the Contingent Reimbursement Model (CRM) Code, launched in 2019. The CRM Code required signatories to reimburse consumers who were the victims of APP fraud under certain circumstances.⁴⁸ The CRM Code was voluntary and existed to help financial institutions in the UK, “detect, prevent and respond to APP scams.”⁴⁹

The voluntary decision of the leading UK payment industry players to develop a system to reimburse fraud victims shows the consensus that protecting consumers benefits industry players and the payment systems as a whole, not merely consumers. But the uneven implementation of the system – and the growing calls to make it mandatory – also show the limits of voluntary measures.

As reported in September 2021, very few victims of APP fraud were reimbursed under the CRM Code: “banks found victims at least partly responsible in 77% of cases assessed in the first 14 months following the introduction of a Contingent Reimbursement Model and voluntary code.”⁵⁰ Two banks found the customer fully liable in 90% of their decisions.⁵¹

Under the CRM code, consumers who were unhappy with their bank’s refusal to compensate them could appeal to the Financial Ombudsman Service, which reviewed denials of reimbursement requests for APP fraud. Data obtained by Which? found that in 73% of the complaints the ombudsman received about APP fraud from 2020-2021, the ombudsman concluded that banks were getting the decisions wrong, reversed the banks’ denials, and found in

⁴⁵ A super-complaint may be made by a designated consumer body where the body considers features of a market in the United Kingdom for payment systems that are or which may be significantly damaging to the interests of consumers. <https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator>.

⁴⁶ As part of the Financial Services (Banking Reform) Act of 2013, the Payment Systems Regulator (PSR) was established to promote competition, innovation, and responsiveness of payment systems and to receive and respond to super-complaints. <https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator>.

⁴⁷ Speech by the Lending Standards Board Chief Executive, Emma Lovell, “*International Perspective-Scams: Looking Forward: Priorities and opportunities*,” (March 15, 2022), available at <https://www.lendingstandardsboard.org.uk/scams-looking-forward-priorities-and-opportunities-international-perspective-speech/>.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ “*Banks called to account over ‘shockingly low’ rate of reimbursements for APP fraud*,” Finextra, (September 15, 2021), available at <https://www.finextra.com/newsarticle/38832/banks-called-to-account-over-shockingly-low-rate-of-reimbursements-for-app-fraud>

⁵¹ *Id.*

favor of the consumer.⁵² This level of reversals suggests that the banks' high rate of denials was inconsistent with both the letter and the spirit of the Code.⁵³

The Contingent Reimbursement Model as an industry response, though laudable and necessary, proved insufficient to address the growing number of scams and fraud. In the first half of 2021, APP fraud cases in the UK outnumbered credit card fraud for the first time.⁵⁴

Consequently, the UK Parliament's Treasury Committee recommended "mandatory refunds" to victims of APP fraud and discussion about whether to make "big technology companies liable to pay compensation when people are tricked by con-artists using their platforms."⁵⁵ As a result, the Payment Systems Regulator (PSR) undertook rulemaking, subject to a period of open comment ("consultation").

In June 2023, the PSR finalized a rule that requires mandatory reimbursement to victims of APP fraud.⁵⁶ Under the finalized rule as amended in 2024, victims are reimbursed up to a maximum of £85,000, with the victim's financial institution and the recipient's financial institution splitting the cost of reimbursement 50:50.⁵⁷

3. When liability is split between sending and receiving institutions and not pushed onto consumers, more will be done to protect consumers.

P2P apps must take more responsibility to protect consumers from the fraud committed on their platforms and from the scammers they allow to open accounts where they can receive stolen funds.⁵⁸ While consumer education is important and necessary, payment system providers' primary response to fraud and errors in P2P systems should not be to use old-fashioned disclosures and warnings to consumers to "be careful" and not to send payments to people they do not know—all while promoting their systems for broad use. Scammers prey on consumers'

⁵² Which?, "Banks wrongly denying fraud victims compensation in up to 8 in 10 cases," (November 11, 2021), available at <https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/>.

⁵³ Contingent Reimbursement Model Code for Authorised Push Payment Scams OP1 at 2, (April 20 2021), available at <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf>

⁵⁴ "UK Government to Legislate for Mandatory Reimbursement of App Fraud," (November 18, 2021), available at <https://www.finextra.com/newsarticle/39245/uk-government-to-legislate-for-mandatory-reimbursement-of-app-fraud>

⁵⁵ "Fraud: MPs seek overhaul to tackle financial scammers," (February 2, 2022), available at <https://www.bbc.com/news/business-60216076>.

⁵⁶ Press Release: "PSR confirms new requirements for APP fraud reimbursement," (July 6, 2023), available at <https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/>.

⁵⁷ To view a summary of the original rule and the feedback received during the open consultation, go to <https://www.psr.org.uk/media/iolpbw0u/ps23-3-app-fraud-reimbursement-policy-statement-final-june-2023.pdf>. See also Payment Systems Regulator, Cost benefit analysis, Faster Payments APP scams reimbursement requirement: changing the maximum level of reimbursement (Oct. 2024), available at <https://www.psr.org.uk/publications/policy-statements/ps247-faster-payments-app-scams-reimbursement-requirement-confirming-the-maximum-level-of-reimbursement/>.

⁵⁸ See Sanchez-Adams, Carla, "It is essential that we protect consumers from fraud over P2P networks," American Banker, Bank Think, (March 15, 2023), available at <https://www.americanbanker.com/opinion/it-is-essential-that-we-protect-consumers-from-fraud-over-p2p-networks>.

trust, and warnings are far less effective than sophisticated systems that payment providers can design.

The providers of P2P payment apps and payment systems as well as the financial institutions who utilize these applications make decisions about what safety features to install, when to protect consumers, and how to monitor and react to red flags of potentially fraudulent payments sent and received by their customers. Companies that are incentivized to prevent fraud and errors will use constantly improving technology and innovations to spot potential scams and errors and to aggregate reports of fraud. Because the UK's new rule will require financial institutions to compensate consumers affected by fraudulently induced transfers (APP scams), for example, nine of the UK's biggest banks have signed up to use a new AI-powered tool that helps banks more effectively spot if their customers are sending money to fraudsters.⁵⁹

Furthermore, financial institutions already have "Know Your Customer" (KYC) and account monitoring obligations under the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws, which should be reflected through their Customer Identification Program (CIP) and Customer Due Diligence (CDD) policies. Even P2P payment apps and fintech companies have certain obligations under the BSA. To comply with these laws, the institutions make decisions about who they allow to open an account and how to monitor and react to red flags of potentially fraudulent payments sent and received by their customers. When they fail in those responsibilities and allow a customer to use an account to receive stolen funds, it is appropriate for that institution to bear the costs if the funds cannot be recouped.

The responsibility of the payment service is even greater in "closed-loop" systems like Cash App, PayPal and Venmo, where one company has access to the accounts of both the consumer sending payment and the criminal fraudster receiving the payment. The P2P company benefits from having the business of both accounts and holds these funds until the consumer or the criminal fraudster chooses to move the funds. As a result, the P2P company has greater visibility into both ends of the transaction and a greater ability to assess whether the transaction is fraudulent. The company also controls the criminal fraudster's or money mule's account and can choose to freeze or hold funds while investigating a claim of fraud. The P2P company can ensure that the money stays within its system, and then reimburse the consumer who has been defrauded.

If fraud and error rates are low in the aggregate, the system can bear those costs and spread them. If rates are high, then the systems clearly have fundamental problems that must be addressed. But even a single instance of fraud or mistake can be devastating to a consumer. The equities strongly favor protecting consumers with the same type of strong protection they have in the credit card market.

⁵⁹ Solon, Olivia "Nine British Banks Sign Up to New AI Tool for Tackling Scams," Bloomberg (Jul. 25, 2023) available at <https://www.bloomberg.com/news/articles/2023-07-05/mastercard-s-ai-tool-helps-nine-british-banks-tackle-scams>.

4. Address the lack of oversight for certain parties involved in the payments market.

Newer fintech companies, including technology providers and payment apps, do not receive the same type of supervision as other financial institutions in the United States. Greater supervision of these companies would allow the supervising agency to ensure P2P companies comply with their Bank Secrecy Act obligations, are not enabling fraud, and respond appropriately to EFTA disputes by consumers, before widespread harm occurs. Greater supervision is important because compliance with basic EFTA obligations has been problematic even in supervised financial institutions, as noted above.

The CFPB had finalized a rule that would have enabled it to supervise large market participants who provide general-use digital consumer payment applications,⁶⁰ which NCLC vigorously supported.⁶¹ However, the final rule was overturned in May 2025 by a Congressional Review Act resolution.⁶² The CFPB has also all but ceased to function and has been actively dropping enforcement cases, halting supervision, and shedding responsibility over nonbanks. While state regulators have a role to play in supervising P2P companies, state regulators cannot ensure that consumers are safe in every state, have limited resources, do not have expertise in the EFTA and other federal laws, and do not have supervisory authority over national banks.

With the passage of the GENIUS Act, the Office of the Comptroller of the Currency (OCC) may have some oversight of these P2P companies in some circumstances. For example, PayPal, which operates as a P2P payment app, has also issued its own stablecoin, PayPal USD. It may very well apply for a license to be a federal qualified payment stablecoin issuer subject to supervision by the OCC. However, it is not clear if that supervision will extend to activities involving fiat payments or other types of crypto-assets, and the OCC is not focused on enforcing consumer protection laws.

IV. Fraud through Crypto-Assets.

A. Crypto-assets are a common payment method for criminal fraudsters.

According to the FTC, “cryptocurrency” is the second largest category of payment method reported by fraud victims in terms of number of dollars lost (after bank transfer or payment) for all of 2024 and the first two quarters of 2025.⁶³ Sometimes these two types of transactions are linked— for example, a fraud victim sends money to a criminal fraudster or the fraudster hacks into the victim’s account and sends the money via bank-to-bank wire transfer to an account on a

⁶⁰ The CFPB issued a final rule on November 21, 2024. It was published in the Federal Register on December 10, 2024 and the effective date was January 9, 2025. *See* 89 FR 99582 (December 10, 2024).

⁶¹ NCLC *et al.*, *Comments to the CFPB’s Proposed Rule Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications*, (January 8, 2024), available at <https://www.nclc.org/wp-content/uploads/2024/01/240108-CFPB-Payments-App-Comment-Final.pdf>.

⁶² S.J. Res. 28, signed by President Trump (P.L. 119-11).

⁶³ FTC fraud reports by payment method, available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>. The FTC can identify the payment method that the criminal used in only a small fraction of fraud reports, and fraud is underreported in general, so the FTC’s numbers vastly understate the amount of fraud facilitated by crypto-assets.

crypto exchange like Coinbase. NCLC has heard of various consumers being harmed by unauthorized wire transfers to crypto accounts due to account takeovers.

Another type of fraud involving crypto-assets involves cryptocurrency kiosks, also known as “crypto ATMs,” “BTMs,” or “virtual currency kiosks”. These can be found in supermarkets, convenience stores, gas stations, bars, and restaurants, and look like bank ATMs. The crypto ATMs allow people to conduct cryptocurrency transactions, such as sending money to digital wallets, but are increasingly used as a way for criminal fraudsters to receive funds from fraud victims. A criminal will instruct their victim to withdraw cash from their own bank and deposit it into a crypto kiosk to buy a crypto-asset (virtual currency) as part of a tech support, extortion, or government impersonator scam. The crypto-asset is then sent to the scammer’s digital wallet, where it can be difficult for the stolen funds to be recovered.

The FBI reported that it received more than 10,956 complaints reporting the use of crypto ATMs kiosks in 2024, with reported victim losses of approximately \$246.7 million, a 99% increase in the number of complaints and a 31% increase in reported victim losses from 2023.⁶⁴ Amy Nofziger, director of fraud victim support at the AARP Fraud Watch Network, said “the number of victim reports involving crypto kiosks that come through AARP’s fraud helpline is ‘just overwhelming.’”⁶⁵ Nofziger also related a story about a 76-year-old fraud victim who lost her entire savings to a crypto ATM.⁶⁶

B. Crypto companies must be subject to the same BSA requirements as banks.

I will not address the safety and soundness issues posed when banks engage with the crypto industry or questions about whether particular crypto firms should or should not be allowed bank accounts. However, as Congress considers legislation to regulate the market for crypto-assets, it is essential that crypto companies and platforms be required to conduct full BSA compliance. Crypto-assets are one of the top vectors for fraud and other illegal activity, and the growth of the crypto industry will only result in more fraud if strict controls are not built in.

⁶⁴ FBI, IC3, “Internet Crime Report 2024” (“2024 IC3 Report”) at 36, available at https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

⁶⁵ Paulin, Emily, and Snow, Molly, “*Scammers Are Using Crypto ATMS to Steal Millions. AARP Is Fighting Back*,” AARP (Published June 10, 2024, Updated June 10, 2025), available at <https://www.aarp.org/advocacy/states-crack-down-crypto-atm-2024/>.

⁶⁶ *Id.* “Attempting to access her recently deceased husband’s Apple account, the widow mistakenly contacted an Apple customer service impersonator who convinced her that her identity had been stolen. The impersonator told her to withdraw her savings and deposit the cash into a crypto kiosk for protection. The woman withdrew \$30,000, put it into the machine and hasn’t had access to the money since.”

Enforcement of BSA requirements is essential to prevent crypto-assets from being used to perpetrate criminal activity. Both federal⁶⁷ and state regulators⁶⁸ have appropriately brought enforcement actions against crypto players that had lax programs to conduct due diligence on their customers, monitor transactions, and report suspicious activities.

Vigilant BSA oversight of accounts involving crypto-assets is also important as crypto-assets make their way into the U.S. banking and payments system. Several large, well-capitalized crypto firms have made it clear that their business model is focused on making crypto and blockchain-based ledgers a mainstream payment method for American consumers. For example, at least one major payment provider has created a stablecoin expressly intended to facilitate consumers' purchase of household goods and services,⁶⁹ while another crypto "native" firm has created a platform where retail merchants are provided crypto wallets that can receive direct crypto payments from customers, without the need to convert crypto assets into fiat currency to settle the transaction.⁷⁰ Reports claim that the platform processes payments for thousands of merchants, for "on-chain" payments worth billions of dollars.⁷¹ BSA/AML compliance is essential to ensure that "purchases" using crypto-assets are not used to enable criminals to receive stolen funds or conduct criminal activity.

Although the GENIUS Act did provide that permitted payment stablecoin issuers will be treated as financial institutions under the Bank Secrecy Act,⁷² not all crypto-assets and crypto companies are covered by the GENIUS Act. Consumers also need protection when crypto-assets are used for payments,⁷³ as discussed below.

⁶⁷ See, e.g., U.S. Dep't of Treasury, Press Release, "U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws," (November 21, 2023), available at <https://home.treasury.gov/news/press-releases/jy1925>; FinCEN, *FinCEN Announces \$29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act*, (Press Release) (October 11, 2022), available at <https://www.fincen.gov/news/news-releases/fincen-announces-29-million-enforcement-action-against-virtual-asset-service>.

⁶⁸ See "Stablecoin Issuer Paxos to Pay Fine to New York for Binance Gaps," Bloomberg Law, (August 7, 2025), available at <https://news.bloomberglaw.com/crypto/stablecoin-issuer-paxos-to-pay-fine-to-new-york-for-binance-gaps> (\$48.5 million settlement for lapses in anti-money laundering adherence and other diligence failures in its partnership with Binance); N.Y. Department of Financial Services, "Superintendent Adrienne A. Harris Announces \$100 Million Settlement with Coinbase, Inc. after DFS Investigation Finds Significant Failings in the Company's Compliance Program," (Pres Release) (January 4, 2023), available at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041.

⁶⁹ PayPal, "Built for stable payments. 1 USD: 1 PYUSD on PayPal," (accessed September 11, 2025), available at <https://www.paypal.com/us/webapps/mpp/digital-wallet/manage-money/crypto/pyusd>.

⁷⁰ Coinbase, "A new standard for onchain payments," (accessed September 11, 2025), available at <https://www.coinbase.com/commerce>.

⁷¹ Akolkar, Bhushan, "New Payments Protocol for Coinbase Commerce to Facilitate Instant Crypto Settlements," CoinGape (blog), (November 17, 2023), available at <https://coingape.com/new-payments-protocol-for-coinbasecommerce-to-facilitate-instant-crypto-settlements/>.

⁷² 12 USC § 5903(a)(5)(A).

⁷³ Any consumer payments made using crypto-assets should come with the full protections given to accounts under the Electronic Fund Transfer Act.

C. Stablecoins and crypto-assets must be subject to consumer protection statutes such as the EFTA when used for consumer payments.

When stablecoins or other forms of crypto-assets are used for consumer payments, they should be subject to consumer protection laws like the EFTA. In fact, some courts have found that crypto-assets are “funds” within the meaning of the EFTA. The GENIUS Act does not say otherwise, and thus does not preempt the EFTA’s protection against unauthorized transfers and errors.

Applying EFTA to the use of payment stablecoins would provide people with greater protections from payment fraud, the ability to dispute or reverse fake or erroneous transactions, and other safeguards that they have when using conventional payment instruments, such as credit cards. The CFPB should also play a role in preventing and remedying fraud that involves stablecoins and other crypto-assets.

In addition to the EFTA, consumers would also benefit from state and federal legislation aimed at addressing the harms caused to consumers from fraud schemes associated with payment by crypto ATMs, including S.710, the Crypto ATM Fraud Prevention Act of 2025. Over 20 states have already passed legislation or regulations to improve consumer protections for crypto ATMs with varying degrees of effectiveness.⁷⁴

V. Bank-to-Bank Wire Transfer Fraud.

A. Consumers are devastated by bank-to-bank wire transfer fraud.

The FTC’s latest fraud data show that “Bank Transfer or Payment” is the payment method used by criminal fraudsters to receive the largest amount of money.⁷⁵ In 2024, consumers reported losing nearly \$2.1 billion through bank transfer or payment.⁷⁶ It also seems safe to assume that the lion’s share of those losses by dollar volume are through bank-to-bank wire transfers, which can process very large transfers, rather than through Zelle, although Zelle is increasingly used for larger transfers. (The FTC’s “Wire Transfer” category includes only nonbank transfers like Western Union and MoneyGram.)

Moreover, some of the over \$1.4 billion reported lost through cryptocurrency may have started as bank-to-bank wire transfers to crypto banks or exchanges.⁷⁷ For example, Marjorie Bloom of Chevy Chase, Maryland, a 77-year-old retired civil servant, lost her life savings, \$661,000, through a bank-to-bank wire transfer into cryptocurrency.⁷⁸

⁷⁴ See AARP Comment to the Senate Banking Committee Digital Asset Market Structure Request for Information, (September 9, 2025), available at <https://www.aarp.org/content/dam/aarp/politics/advocacy/2025/09/aarp-response-to-banking-rfc.pdf>.

⁷⁵ FTC fraud reports by payment method available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

⁷⁶ *Id.*

⁷⁷ See Paluska, Michael, “Cryptocurrency scam drains retired St. Pete victim’s life savings How to spot online scams,” ABC Action News (Florida), (June 19, 2023), available at <https://www.abcactionnews.com/news/region-pinellas/cryptocurrency-scam-drains-retired-st-pete-victims-life-savings>.

⁷⁸ Iacurci, Greg, “How this 77-year old widow lost \$661,000 in a common tech scam: ‘I realized I had been

2024 Fraud Reports to FTC Consumer Sentinel Network by Payment Method

FTC CONSUMER SENTINEL NETWORK

Published August 15, 2025
(data as of June 30, 2025)

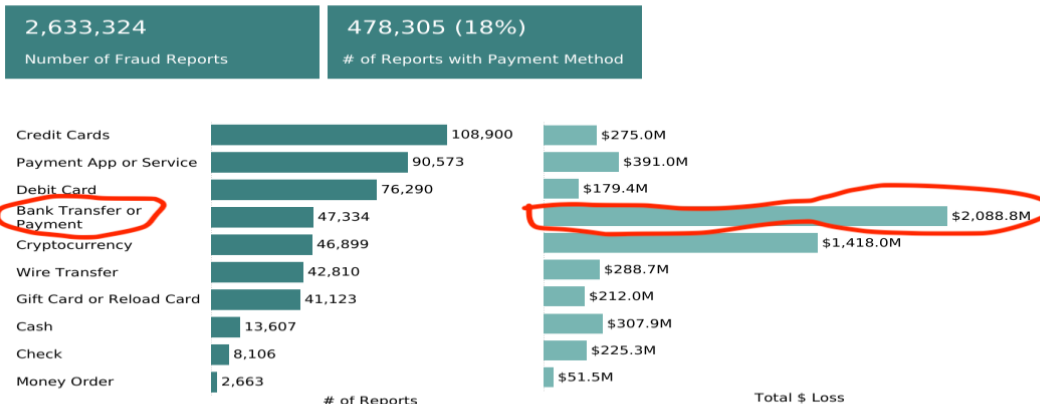
All Fraud Reports by Payment Method
Year: 2024

All
FTC
Data Contribu..

Contact Method
Payment Meth..

Year
2024

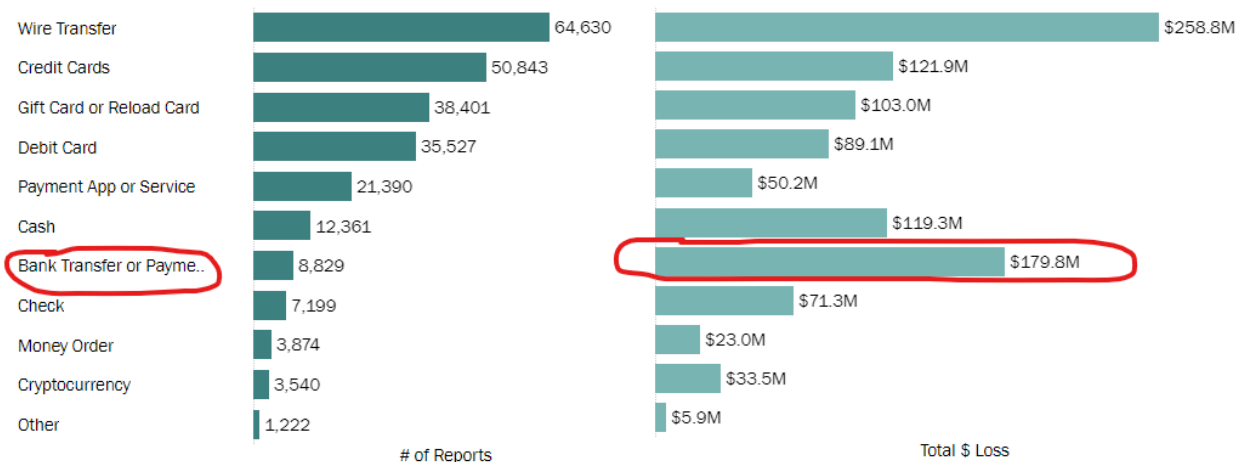
Quarter
All



Other payment methods includes Payroll Allotment and Telephone Bill.
FEDERAL TRADE COMMISSION · ftc.gov/exploredata

Compared to 2019, it is especially dramatic to note how the bank transfer category has overtaken nonbank wire transfers, and how astronomically it has grown – from roughly \$180 million to almost \$2.1 billion in six years.⁷⁹

2019 Fraud Reports to FTC by Payment Method



Over the last several years, NCLC has received numerous inquiries on behalf of consumers and heard devastating reports about how criminals have used bank-to-bank wire transfers to take

defrauded of everything’,” CNBC, (October 8, 2023), available at <https://www.cnbc.com/2023/10/08/how-one-retired-woman-lost-her-life-savings-in-a-common-elder-fraud-scheme.html>.

⁷⁹ The dollar losses in these two charts significantly understate actual losses, as only 12% (2019) to 18% (2024) of reports included information on payment method, and many fraud losses are not reported to the FTC.

hundreds of thousands of dollars from people. In one case, an older woman lost her home as a result. Here are other examples:

- A college student lost his entire savings account after someone with two fake identification cards went into a bank and wired \$16,500 to another individual. Busy with college, he did not notice missing money for a month and a half, but the bank refused to return the money.⁸⁰
- After a consumer was the victim of a SIM swap, a wire transfer was used to transfer \$35,000 from his bank account to an account in another state.⁸¹ He is a cancer patient and navigating the bank appeal process has been extremely stressful. These SIM swaps are increasingly common.⁸²
- A low-income consumer in New York lost over \$26,000 – all her savings, which she had carefully saved over many years – after someone transferred money from her savings account to her checking account and then made an outgoing wire transfer to another state.⁸³
- A man lost \$15,000 that was wired to another account by someone who gained access to his account. The bank spotted suspicious activity as the fraud was taking place and called the man, who alerted them to the fraud, but the bank still refused to return the money claiming that the EFTA did not apply to these fraudulent electronic transactions.
- A fraudster hacked a retiree's online banking account and made a cash advance from the retiree's credit card to his linked bank account. The fraudster then immediately wired that amount from the retiree's bank account to his own. The bank denied any relief.⁸⁴
- A small business had its online banking account hacked and its \$60,000.00 checking account balance emptied over the course of two days and six transactions. The bank denied relief because its banking agreement generally states that customers are responsible for unauthorized transactions.⁸⁵

Wire fraud has become so problematic that even large news outlets like Good Morning America have run stories about the perils and lack of protection available to impacted consumers.⁸⁶

⁸⁰ Inquiry received by KPRC (Houston NBC station) reporter Amy Davis.

⁸¹ Email from attorney on file with NCLC.

⁸² See Barr, Luke, ABC News, “*SIM swap’ scams netted \$68 million in 2021: FBI*” (February 15, 2022), available at <https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169>.

⁸³ Email from CAMBDA Legal Services to NCLC, on file with NCLC.

⁸⁴ Pending arbitration before AAA (Wells Fargo).

⁸⁵ *Lawrence and Louis Company d/b/a Hidden Oasis Salon v. Truist Bank*, No. 1:22-cv-200-RDA-JFA (E.D. Va.).

⁸⁶ ABC News, Good Morning America, “*Woman sounds alarm on sophisticated wire transfer fraud*,” (July 21, 2023), available at <https://abcnews.go.com/GMA/Living/video/woman-sounds-alarm-sophisticated-wire-transfer-fraud-101547100>.

All the examples provided above were for unauthorized wire transfers. However, we have also heard stories where the consumer was fraudulently induced into sending a wire transfer. For example:

- Three Ohio residents were all defrauded into making a bank-to-bank wire transfer by a Chase impersonation scam.
 - Jeff Phipps from Columbus, Ohio lost \$8,500 after the fraudster, impersonating a bank employee, called and convinced the man that his account had been hacked into and he needed to provide login information to protect it. “They asked him if he had authorized a wire transfer and he replied, 'no'. They kept him on the phone for an hour and 47 minutes. They said, ‘Well, we want to deactivate your account. Can you send us your username and your passcode?’ And he did thinking it was Chase.” The fraudster took \$8,500 with this information and Chase refused to refund the victim's money since he had given information to the scammer, "authorizing" it.⁸⁷
 - Kelli Hinton, 7 months pregnant at the time, received a text about a fraudulent wire transfer from her account, then a follow-up call from a fraudster posing as a Chase fraud agent, spoofing Chase’s real phone number. The fraudster kept her on the line for an hour and convinced her to change her username and password, allowing him to drain \$15,000 from her account.⁸⁸
 - Just months after experiencing a near fatal collision that left him in a wheelchair, Todd Evans from West Chester Township was called by a fake Chase fraud protection agent. The fraudster told him about a fraudulent purchase from his account, which Todd confirmed was appearing on his account and which neither he nor his wife had made. The fraudster then mentioned a \$45,000 fraudulent wire transfer from the account. Todd and his wife were nervous about addressing the fraud and asked the caller to verify his identity. He asked the couple to look at the number he was calling from and verify it matched the number on their debit card. Based on this confirmation, the couple allowed the fraudster to guide them through a "wire reversal process". Hours later they were out \$63,000.⁸⁹
- A couple in South Carolina received an email from their attorney at the time of closing their home purchase with instructions on where to send the down payment via bank-to-bank wire transfer. Their attorney had been the victim of a phishing scam, and the fraudster used a legitimate email copying an actual employee of the attorney. The couple lost \$108,000.⁹⁰

⁸⁷ Gordon, Clay, “Central Ohio man loses \$8,500 in Chase bank impersonation scam,” 10 WBNS, (March 30, 2023), available at <https://www.10tv.com/article/money/consumer/wire-fraud-scam-warning/530-7af76f5c-ccc0-4dcc-98a3-5c740a9043bd>.

⁸⁸ McCormick, Erin “Gone in seconds: rising text scams are draining US bank accounts,” The Guardian, (April 22, 2023), available at <https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts>.

⁸⁹ Johnson, Karin “West Chester couple swindled out of thousands of dollars by crooks spoofing bank’s phone number,” WLWT5 news, (November 16, 2023), available at <https://www.wlwt.com/article/west-chester-chase-bank-spoofing-phone-number/45866051>.

⁹⁰ Lee, Diane, “Upstate couple warns of wire fraud that cost them \$108,000,” CBS7 News, (May 19, 2023),

Even in instances where consumers realize they have fallen prey to a fraud scheme, banks are sometimes unwilling or unable to assist consumers or stop a wire transfer. For example, Ann Booras from San Ramon, California received a call from a fraudster impersonating a Wells Fargo employee asking if she had wired \$20,000 from her savings account. In response to the directions provided by the fake employee, Ann wired the \$20,000 sum to the “bank’s fraud department” where it would be safe. The fraudster then continued asking about other supposedly fraudulent transactions, and panicking, Ann “drove to the nearest Wells Fargo branch, with the man still on the phone, and told a teller someone was attacking her accounts. Silently, the teller warned her - the thief was actually the man on the phone. ‘I had tears running down my face, I was literally shaking because I realized I had just sent \$25,000 to who knows where.’” Ann “pleaded with bank employees to stop those wire transfers -- fast. But to her shock, no one would help.” She was told, “I’m sorry we’re all busy. We’re backed up with appointments back to back. You need to go to another branch, but we can’t help you here.”⁹¹

B. Technology enables more bank-to-bank wire transfer fraud.

As the previous stories all illustrate, fraudsters have taken advantage of the technology needed to send texts and make calls to consumers whose information has been obtained through phishing schemes or purchased from the dark web. Technology also enables fraudsters and hackers the ease to take over accounts and initiate transactions through online or mobile banking.

Previously, wire transfers had to be conducted through a cumbersome process of walking into a bank for a time-consuming, in-person transaction. In-person identification would prevent unauthorized transfers, and there were some speed bumps for fraudulently induced transactions as well—the consumer would have time to think about the situation, call a family member, and talk to the bank teller, who could potentially talk them out of it.

But increasingly, bank-to-bank wire transfers are a service offered and permitted through mobile and online banking. As a result, fraudsters have an easy method of using unauthorized or fraudulently induced transfers to steal and send large sums of money, often not possible through P2P apps that set daily transaction limits. The lack of friction that was found in in-person transactions has undoubtedly contributed to the explosion of bank-to-bank wire transfer losses.

C. Banks claim bank-to-bank wire transfers are exempt from the EFTA, leaving consumers exposed to losing thousands of dollars.

The EFTA does not directly exempt wire transfers; it exempts electronic transfers, other than ACH transfers, made “by means of a service that transfers funds held at either Federal Reserve

available at <https://www.wspa.com/news/upstate-couple-warns-of-wire-fraud-that-cost-them-108000/>.

⁹¹ Finney, Michael and Koury, Renee, “Wells Fargo bankers tell East Bay customer they’re too busy to stop wire scam,” ABC7, (June 21, 2023), available at <https://abc7news.com/bank-impostor-scam-wells-fargo-wire-transfer-fraud-scammer-pretends-to-be/13407340/#:~:text=Wells%20Fargo%20bankers%20tell%20East.busy%20to%20stop%20wire%20scam&text=The%20victim%20was%20still%20on.SAN%20RAMON%2C%20Calif.>

banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer.”⁹² However, Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using Fedwire or through a similar wire transfer system, like SWIFT, CHIPS, and Telex, that is used primarily for transfers between financial institutions or between businesses.⁹³

Fraudulent wire transfers can cause consumers to lose their entire life’s savings. Banks claim that even if a criminal impersonates the consumer and makes a completely unauthorized wire transfer, the EFTA and Regulation E protections do not apply; instead, they assert that bank-to-bank wire transfers are covered under state law, more specifically a state’s adopted version of Uniform Commercial Code Article 4A (UCC Article 4A).

But the UCC was not designed as a consumer protection statute and was instead designed to govern commercial-to-commercial transactions. UCC Article 4A offers very weak or no protection for consumers who have suffered harm due to bank-to-bank wire transfer fraud. In essence, the consumer is deemed to have authorized a wire transfer if the bank utilized a commercially reasonable security procedure that the bank and the consumer agreed to beforehand and if the bank acted in good faith. Yet consumers have no understanding of or control over those security procedures and no choice but to click “I agree” to the fine print of an agreement. Banks also claim that their procedures are commercially reasonable even when they are inadequate.

For example, the New York Attorney General recently filed a lawsuit against Citibank alleging it failed to protect and reimburse victims of electronic fraud when it used “poor security and anti-fraud protocols” that consumers had not negotiated with Citibank.⁹⁴ According to the lawsuit, Citibank connected wire transfer services to consumers’ online and mobile banking apps in recent years— allowing direct electronic access to the wire transfer networks— but employed lax security protocols and procedures; had ineffective monitoring systems; failed to respond in real-time; and failed to properly investigate fraud claims.⁹⁵ As a result, New Yorkers lost millions of dollars in life savings, their children’s college funds, and even money needed to support their day-to-day lives.

I have also heard numerous other reports of banks failing to reimburse unauthorized wire transfers, even when the consumer did not agree to any commercially reasonable security procedure. Consumers do not have the resources to fight the bank in court or arbitration to enforce their right to a reimbursement when this occurs.

UCC Article 4A does not provide a consumer with any other remedies besides reimbursement (and possible interest) of the unauthorized wire amount, and the consumer’s attorney is not entitled to recover attorneys’ fees from the bank. As a practical matter, it means that a consumer

⁹² 15 U.S.C. §1693a(7)(B).

⁹³ Reg. E, 12 C.F.R. § 1005.3(c)(3).

⁹⁴ New York State Attorney General, “*Attorney General James Sues Citibank for Failing to Protect and Reimburse Victims of Electronic Fraud*,” (Press Release) (January 30, 2024), available at <https://ag.ny.gov/press-release/2024/attorney-general-james-sues-citibank-failing-protect-and-reimburse-victims>.

⁹⁵ See Complaint, *People of the State of New York v. Citibank*, No. 1:24-cv-00659 (S.D.N.Y. filed January 30, 2024), available at <https://ag.ny.gov/sites/default/files/2024-01/citi-complaint.pdf>.

would have to pay out of pocket to fight in court or in arbitration just to get their money back, while a financial institution with deep pockets can afford to fight a claim. As a result, in most cases financial institutions will reject a consumer's unauthorized wire transfer claim because the consumer cannot afford to fight the decision.

With respect to fraudulently induced wire transfers, the UCC provides no remedy.

D. Potential remedies to address bank-to-bank wire fraud.

The exemption in Regulation E should be eliminated, and until it is, it should be interpreted narrowly. When the EFTA was written in 1978, bank-to-bank wire transfers were rarely used by consumers and required an in-person visit to the bank. That has clearly changed— bank-to-bank wire transfer services are now incorporated into consumer mobile and online banking services and electronic fund transfers are generally far more common among consumers today than in 1978. For large payments, bank-to-bank wire transfers are the primary way consumers can conduct electronic transfers.

In its suit against Citibank mentioned above, the New York AG alleged that the unauthorized wire transfers that occurred by electronic requests initiated by scammers via online banking or mobile app are covered by the EFTA. The court agreed with the New York AG, holding that the wire exemption does not cover the transfer between the consumer and their bank before a service like Fedwire is used to transfer the funds.⁹⁶

As previously stated, we also support legislative efforts to address gaps in the Electronic Fund Transfer Act that leave consumers unprotected.

The EFTA can be amended to address specific problems of unauthorized consumer bank-to-bank wire transfers as well as fraudulently induced consumer bank-to-bank wire transfers by:

- Eliminating the exemption for bank wire transfers and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Protecting consumers from liability when they are defrauded into initiating a transfer, and
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

The consumer bank-to-bank wire transfer loophole and inclusion of fraudulently induced transfers could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

⁹⁶ *New York v. Citibank*, 763 F.Supp.3d 496 (S.D.N.Y. 2025).

VI. Check Fraud.

A. Check alteration fraud is on the rise.

Although checks are an old payment system, new technology is leading to a rise in fraud using checks. In particular, new technology makes it easier for criminals who steal checks to engage in “check washing” – changing the payee and payment amount on a check – and harder for banks or consumers to spot those alterations.⁹⁷ Criminals can also create fake checks from stolen account information. These altered or fabricated checks can then be deposited remotely through mobile devices, made easier through the increased ability to open fraudulent accounts into which those checks can be deposited.

Although checks are near the bottom of payment types in terms of number of fraud reports, the total dollar loss by check fraud reported to the FTC in 2024 is actually higher than for debit cards, gift cards or reload cards, and money orders. But this reported dollar loss is vastly understated;⁹⁸ one report from 2023 puts annual check fraud losses at \$815 million.⁹⁹

Also in 2023, FinCEN issued an alert about a nationwide surge in mail theft-related check fraud schemes and urged financial institutions to “be vigilant in identifying and reporting such activity.”¹⁰⁰ The report indicated that there were over 680,000 cases of possible check fraud reported to FinCEN in 2022 through the use of SARs (Suspicious Activity Reports), an increase from a little over 350,000 check fraud-related SARs sent to FinCEN in 2021, which itself was a 23% increase from 2020.¹⁰¹ The statistics for check-fraud related SARs were not specific to mail-theft related check fraud.¹⁰²

Technology also enables criminal organizations to traffic stolen checks. As a 2023 New York Times article¹⁰³ conveyed:

“The cons may start with stealing pieces of paper, but they leverage technology and social media to commit fraud on a grander scale, banking insiders and fraud experts said. In the past, criminals needed a special internet browser that would grant entry into the

⁹⁷ DePompa, Rachel, “‘Check washing’ scams still on the rise,” Fox10 News, (January 25, 2024), available at <https://www.fox10tv.com/2024/01/25/check-washing-scams-still-rise/>.

⁹⁸ Of the 2.5 million reports of fraud received by the FTC in 2022, only 17% specified the payment method for the fraud. FTC fraud reports by payment method available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

⁹⁹ Nadelle, David, “Check Washing Is an \$815M Per Year Scam — How It Works and Ways To Prevent It,” GoBanking Rates, (February 22, 2023), available at [https://www.nasdaq.com/articles/check-washing-is-an-\\$815m-per-year-scam-how-it-works-and-ways-to-prevent-it](https://www.nasdaq.com/articles/check-washing-is-an-$815m-per-year-scam-how-it-works-and-ways-to-prevent-it).

¹⁰⁰ FinCEN, FIN-2023-Alert003, *FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail*, (February 27, 2023) available at <https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf>

¹⁰¹ *Id.* citing FinCEN SAR Stats available at <https://www.fincen.gov/reports/sar-stats>

¹⁰² *Id.* See FN 10.

¹⁰³ Barnard, Tara Seigel, “We Can’t Stop Writing Paper Checks. Thieves Love That,” (December 9, 2023), available at https://www.nytimes.com/2023/12/09/business/check-fraud.html?unlocked_article_code=1.QU0.O8_m.7j3dyrD0mzvX&smid=url-share

dark web marketplace of stolen checks, maybe even someone to vouch for them. Now all they need is an account from Telegram, a messaging app.

“You can buy checks on the internet for \$45, with a perfectly good signature,” said John Ravita, director of business development at SQN Banking Systems, which provides check fraud detection software. “There is one website that offers a money-back guarantee. It’s like Nordstrom.”

NCLC spoke with Larry Smith, an attorney in Chicago, whose clients did not even have checks issued to their associated bank account, yet a fraudster somehow obtained their bank account and routing number and created fake checks.¹⁰⁴ The fraudster deposited these checks in various bank accounts from December 2021 and January 2022, stealing around \$14,000 from the consumers. Though the consumers disputed the fraudulent checks with their bank and have filed a lawsuit, their bank has not reccredited their account for the stolen amount.

B. Though some protections exist for consumers harmed by check fraud, they are often left scrambling.

Checks are largely governed by state law through the Uniform Commercial Code (UCC). If a consumer timely reports the problem, the UCC protects them if their checks are altered or if a fraudulent check is presented against their account.¹⁰⁵

Yet as the previous example demonstrates, consumers are often left scrambling, waiting for their banks to recredit their account even when state law provides remedies for the consumer when a check is altered or forged. One consumer in Los Angeles was unable to get his account reccredited for over two years. The consumer had written a check to the IRS and sent it by mail. The check was stolen from the mail and deposited into an account that was not the U.S. Treasury.¹⁰⁶ The consumer’s bank kept insisting it would not reccredit his account until the fraudster’s bank sent them reimbursement.

While a bank’s obligation to reimburse a consumer for an altered check is not dependent on the bank’s ability to be repaid by the depository bank, the failure to timely resolve check fraud between institutions has also been the subject of complaint by community banks against their large-bank counterparts.¹⁰⁷ Consumers turn to their own bank for reimbursement when a check is altered or forged, and that bank in turn will request reimbursement from the bank into which the check was fraudulently deposited. As previously described in more detail in Section III. F. 3., the depository bank has “know-your-customer” responsibilities that are important to prevent fraud, but there is insufficient incentive to be diligent if there is no liability. As Steven Gonzalo,

¹⁰⁴ *Arroyo and Ramos v. Fifth Third Bank, N.A.*, Cause No. 2023L004163, Cook County, IL.

¹⁰⁵ See U.C.C. §§ 3-407(b), (c) cmt. 2, 4-401(d)(1) for a consumer’s rights when a check is altered; see U.C.C. §§ 4-401; 4-406(f) for a consumer’s rights when a check is forged.

¹⁰⁶ See Lazar, Kristine, “*On Your Side: Check fraud is on the rise- here’s how to protect your money*,” CBS News Story, KCAL News, (April 17, 2023), available at <https://www.cbsnews.com/losangeles/news/on-your-side-check-fraud-is-on-the-rise-heres-how-to-protect-your-money/>.

¹⁰⁷ Berry, Kate, “*Small banks urge crackdown on big banks with lax check-fraud controls*,” American Banker, (February 9, 2023), available at <https://www.americanbanker.com/news/small-banks-urge-crackdown-on-big-banks-with-lax-check-fraud-controls>

president and CEO of American Commercial Bank & Trust, stated: “From a deposit perspective, some banks do not perform the same level of due diligence because the bank assumes the risk of loss to them is zero or minimal, and fails to consider losses due to fraud incurred by the counterparty banks. And therein lies the failure.”¹⁰⁸

Furthermore, even though the UCC provides consumers up to a year to inform their bank of a fraudulent or altered check, it allows banks to shorten that notification time in the fine print of account agreements. Many bank account agreements shorten that time for notification to anywhere between 14 and 30 days.

Yet check alterations can be hard to spot. If the payee has been changed but not the amount, the consumer might have no reason to think that anything is amiss. For example, one consumer reported to NCLC that he had no idea his check had been altered until his landlord – a family friend – eventually told him months later that he had not received the rent.

Most banks no longer return physical checks to consumers and have also engaged in an aggressive push to eliminate paper statements. Bank websites and mobile apps focus on listing transactions but make it more cumbersome to review actual statements. The grainy photocopies of checks included with statements can be hard to read, consumers may not expect to have any reason to look at them, and those images are not even available to review on some mobile banking apps.

But if the consumer does not inform their bank about the check fraud before the end of the 14- to 30-day time period, they may be left with absolutely no recourse at all.

C. Potential remedies to address check fraud.

While the UCC provides remedies to consumers if a check is altered or forged check, if the drawee bank is unable to get compensation from the depository bank, the drawee bank may delay in, or sometimes even fail to comply with, their obligations under the Uniform Commercial Code (UCC) to credit the consumer’s account for a check that was not properly payable.¹⁰⁹ Thus, federal regulators should require the depository bank to swiftly compensate the drawee bank. At the same time, the federal regulators should be vigilant to ensure that drawee banks fulfill their obligations to their customers even if they have a dispute with the depository bank.

We also note that consumers need to have sufficient time to dispute a check as altered or forged. The UCC only requires that the consumer act with reasonable promptness in examining the bank statement and must promptly notify their bank¹¹⁰ no later than one year after the statement is made available.¹¹¹ But many banks shorten those timelines in the account agreement, sometimes to as short as 30 days. Yet most consumers have never heard of check washing and reasonably do not expect that they should have to examine checks for alterations or forgeries. Moreover, most banks no longer return original checks and instead make check images available, often at a

¹⁰⁸ *Id.*

¹⁰⁹ UCC § 3-407(b), (c) cmt. 2; § 4-401(d)(1); § 4-401 cmt. 1.

¹¹⁰ UCC § 4-406(c).

¹¹¹ UCC § 4-406(f).

reduced size. Those images can be extremely hard to read. That problem is compounded by the widespread elimination of paper statements, with consumers only getting an email that an online statement is available, and bank websites are generally set up to encourage viewing transactions but not statements. If the amount has not changed, the consumer may have no reason to suspect anything is wrong. Thus, we encourage federal regulators to insist that financial institutions give consumers a reasonable time to identify and report check alterations and forgeries, which may be longer than 30 days.

We also suggest that the federal Reserve Board make certain changes to Regulation CC, concerning the availability of funds from check deposits.¹¹²

In summary, to protect consumers from check fraud:

- Federal bank regulators should examine institutions to ensure that they are complying with their responsibility to reimburse consumers for altered or forged checks, and that depository banks are appropriately reimbursing drawee banks.
- Federal bank regulators should step up enforcement of BSA/AML obligations and scrutinize the institutions into which fraudulent checks are deposited.
- States should amend their UCC laws to remove the ability of banks to shorten the time period provided by the UCC to report altered or forged checks.
- Improvements in the protections for P2P payments would also give consumers more confidence in using those systems instead of checks.

We should also give consideration to moving consumer protections for checks within the EFTA, which provides a clearer framework than the UCC for consumer protection including error resolution timelines and procedures and consumer rights.

The Federal Reserve Banks should also explore collecting information on check fraud, which may help to identify institutions that need to do a better job with their BSA/AML obligations.

VII. Electronic Benefit Transfer (EBT) Card Fraud.

A. EBT card skimming and theft leave cardholders without any protections.

Supplemental Nutrition Assistance Program (SNAP) benefits are distributed and administered through the Electronic Benefit Transfer (EBT) system to eligible participants. EBT has been the sole method of SNAP issuance in all states since June of 2004,¹¹³ and some states also use EBT cards to issue Temporary Assistance for Needy Families (TANF) or other state-administered financial assistance. EBT accounts perform the same function for low-income households as do

¹¹² See NCLC, *Comments regarding the Request for Information on Potential Actions to Address Payments Fraud by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation*, (September 15, 2025), available at https://www.nclc.org/wp-content/uploads/2025/09/2025.09.15_Comments_Fraud-RFI-on-Payments-Fraud.pdf.

¹¹³ U.S. Department of Agriculture, Food and Nutrition Service, <https://www.fns.usda.gov/snap/ebt> (last accessed September 15, 2025).

checking accounts—the accounts power daily, or near daily, transactions. People who receive these benefits typically spend down the account balance to \$0 each month.

In 2020, about 39.9 million people across the country received SNAP benefits;¹¹⁴ 38% of whom were white, 25.5% Black, and 15% Hispanic.¹¹⁵ As of 2022, nearly 2 million Americans receive Temporary Assistance for Needy Families (“TANF”) benefits to support their families.¹¹⁶ In FY 2021, 35% of TANF recipients were Hispanic, 29% were Black, and 27% were white.¹¹⁷ These public benefit programs are focused entirely on low-income families.

During the past several years, EBT cardholders have been targeted by criminals who “skim” account information and PINs and then deplete the accounts of all funds belonging to the recipients. This problem is so endemic that even the USDA issued a policy memo on EBT card skimming prevention with tools and resources to prevent and identify the fraud,¹¹⁸ and Congress provided for reimbursement of these stolen funds for the period of October 1, 2022, to September 30, 2024.¹¹⁹

However, while other consumers have also been victimized by skimming, EBT consumers are particularly vulnerable and left with little to no recourse. Unlike other cardholders whose funds may be stolen in the same way, EBT cardholders – the lowest-income and most vulnerable consumers – do not have protections afforded to other consumers by the Electronic Funds Transfer Act or Regulation E. Even if the consumer did not lose their card, was not responsible for providing card information to the criminal, and immediately reported missing funds, they are completely out of luck. These lost funds come out of the pockets of the poorest families who cannot afford to lose a single dollar.

B. Potential remedy to address EBT card fraud.

We support legislative efforts to address gaps in the Electronic Fund Transfer Act that leave consumers unprotected. The EFTA and SNAP statute can be amended to address the specific problem of EBT card fraud by eliminating the exclusion of EBT cards from the EFTA and

¹¹⁴ U.S. Department of Agriculture, Food and Nutrition Service, “*Characteristics of SNAP Households: FY 2020 and Early Months of the Covid-19 Pandemic: Characteristics of SNAP Households*,” available at <https://www.fns.usda.gov/snap/characteristics-snap-households-fy-2020-and-early-months-covid-19-pandemic-characteristics> (last accessed September 15, 2025).

¹¹⁵ Cronquist, Kathryn and Eiffes, Brett, “*Characteristics of Supplemental Nutrition Assistance Program Households: Fiscal Year 2020, Table B.4.b. Distribution of participating households by shelter-related characteristics and by State, waiver period*,” Washington: U.S. Department of Agriculture, (2022), available at <https://fns-prod.azureedge.us/sites/default/files/resource-files/Characteristics2020.pdf>; 7 C.F.R. § 273.10(c)(2)(i).

¹¹⁶ Office of Family Administration, Administration for Children and Families, “TANF Caseload Data 2022,” (August 2022) available at, <https://www.acf.hhs.gov/ofa/data/tanf-caseload-data-2022>.

¹¹⁷ U.S. Department of Health and Human Services, Office of Family Assistance, “*Characteristics and Financial Circumstances of TANF Recipients, Fiscal Year 2021*,” updated February 2023, available at <https://www.acf.hhs.gov/ofa/data/characteristics-and-financial-circumstances-tanf-recipients-fiscal-year-2021>.

¹¹⁸ U.S. Department of Agriculture, Food and Nutrition Service, *Supplemental Nutrition Assistance Program (SNAP) and Temporary Assistance for Needy Families (TANF) Electronic Benefit Transfer (EBT) Card Skimming Prevention – Tools and Resources*, (Policy memo) (October 31, 2022), available at <https://www.fns.usda.gov/snap/snap-tanf-ebt-card-skimming-prevention>.

¹¹⁹ See the Consolidated Appropriations Act (CAA) of 2023, Title IV, Section 501.

providing protection against unauthorized transfers. As a result, consumers who are impacted by EBT card theft will be able to avail themselves of the EFTA unauthorized use provision and error resolution procedures.

VIII. Problems with the Collection of Accurate Payment Fraud Data Create an Additional Barrier to Addressing Payment Fraud.

A. The problem of fragmented data collection on payment fraud.

In the United States, regulatory oversight and supervision of actors in the payments space depends on several factors including the size, type, and nature of a financial institution,¹²⁰ as well as the extent to which the activities undertaken by an institution are covered by existing law. As a result, no centralized federal agency receives or collects all data about payment fraud.¹²¹ Additionally, defrauded consumers may report fraud to the Federal Trade Commission, the FBI's internet crimes division, and/or the Consumer Financial Protection Bureau, among other local law enforcement agencies, leading to differing and incomplete snapshots of payment fraud. Although these agencies may share fraud data with each other or the general public, there is no mandate to do so.¹²²

Furthermore, financial institutions, payment processors, and payment operators are not required to report the incidents of payment fraud experienced by their customers/consumers to any federal agency. The institutions are required to file a Suspicious Activity Report (SAR) for large transactions in certain circumstances if they suspect their customer is engaged in fraudulent activity, but they are not required to report smaller fraudulent transactions or instances where their clients have been victimized by fraud.¹²³ Even with SARs mandatory reporting, the

¹²⁰ Depending on the size and activity, a financial institution engaging in payment activity could be subject to supervision by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and/or the Consumer Financial Protection Bureau. Otherwise, the institution could be subject to state regulatory supervision under a state bank charter or money transmitter license. Some payment stablecoin issuers will be supervised by the OCC, while others may choose to continue to be licensed by states and subject to state supervision. It is still unclear what federal agency will supervise crypto companies engaging in payments. Some payment actors may not be subject to any supervision, though they are still required to comply with all laws.

¹²¹ Of any type, including fraud through P2P apps, bank-to-bank transfers, or check fraud.

¹²² Though certain fraudulent activity is required to be reported to FinCEN, and the Federal Reserve Board will collect fraud data through FedNow. However, FinCEN does not publicly share the data it collects, and it is unclear how the Federal Reserve Board will utilize and disseminate the data it will collect for FedNow.

¹²³ "Dollar Amount Thresholds- Banks are required to file a SAR in the following circumstances: insider abuse involving any amount; transactions aggregating \$5,000 or more where a suspect can be identified; transactions aggregating \$25,000 or more regardless of potential suspects; and transactions aggregating \$5,000 or more that involve potential money laundering or violations of the BSA. It is recognized, however, that with respect to instances of possible terrorism, identity theft, and computer intrusions, the dollar thresholds for filing may not always be met. Financial institutions are encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce. Even when the dollar thresholds of the regulations are not met, financial institutions have the discretion to file a SAR and are protected by the safe harbor provided for in the statute." From FDIC *"Connecting the Dots ... The Importance of Timely and Effective Suspicious Activity Reports"* Supervisory Insights, (Updated July 10, 2023), available at <https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/siwinter2007-article03.html#:~:text=Dollar%20Amount%20Thresholds%20%E2%80%93%20Banks%20are,and%20transactions%20aggregating%20%245%2C000%20or.>

information collected by FinCEN relies heavily on the discretion of a financial institution, whether the fraud or potential fraud is discovered/flagged by the reporting institution, and if the transaction is large enough to warrant reporting.¹²⁴

Players in the payment industry have recognized the need for fraud information sharing, and some payment operators do collect data about fraud. The Federal Reserve Board collects reports of fraud on FedNow as specified under Regulation J, Subpart C and keeps a “Negative List” of suspicious accounts that is shared with its participants.¹²⁵ The Clearing House also collects fraud reports for RTP® (their real time payments platform) and Early Warning Systems (EWS), owner of Zelle, collects reports of fraud occurring on Zelle, though it is unclear if this information is shared widely among users.¹²⁶ Even initiatives such as Sonar¹²⁷ and Beacon¹²⁸ were launched in response to increased fraud in digital payments and real-time payment systems. However, the information shared is not available to the public and may be industry or payment specific. For example, if a bad actor is flagged in one payment system (i.e. Zelle), that does not mean a financial institution will have that bad actor flagged when allowing a fraudulent wire transfer to be released.¹²⁹

The fragmentation described above prevents a clear and cohesive picture of the payment fraud landscape, actors, and trends and poses a barrier to forming effective strategies to combat fraud.

B. Potential remedies to address the problem of fragmented payment fraud data collection.

1. Interagency collaboration.

The importance of information sharing and collaboration between state and federal law enforcement agencies charged with protecting the public from fraud and other unfair, deceptive, and abusive business practices cannot be overstated. Collaboration is essential not only to identify illegal practices that harm consumers, but to facilitate a comprehensive and effective

¹²⁴ See Mansfield, Cathy, “It Takes a Thief.... and a Bank: Protecting Consumers From Fraud and Scams on P2P Payment Platforms,” 57 U. Mich. J.L. Reform (2024).

¹²⁵ See Operating Circular 8: Funds Transfers through the FedNow Service, (September 21, 2022), available at <https://www.frbervices.org/binaries/content/assets/crsocms/resources/rules-regulations/operating-circular-8.pdf>.

¹²⁶ See *Faster Payments Fraud Trends and Mitigation Opportunities*, Faster Payments Council, Fraud Work Group Bulletin.01 at 5, (January 2024), available at

https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

¹²⁷ <https://www.joinsonar.com/>, (last accessed September 15, 2025). Sonar is “an independent data consortium for sharing real-time insights into First-Party Fraud and Counterparty Risk.... By monitoring transactions across banks, merchants, fintechs, and crypto, you’re always a step ahead in detecting financial crime.”

¹²⁸ Meier, Alain “Introducing Beacon, the Anti-Fraud Network,” Plaid, (June 22, 2023), available at <https://plaid.com/blog/introducing-plaid-beacon/>. Beacon, launched by Plaid, is intended as an anti-fraud network enabling financial institutions and fintech companies to share critical fraud intelligence via API across Plaid. Members contribute by reporting instances of fraud and can use the network to detect if a specific identify has already been associated with fraud.

¹²⁹ Any private database of suspected fraud actors could be considered a “consumer reporting agency” (CRA) under the Fair Credit Reporting Act (FCRA). Early Warning Services already acknowledges it is a CRA. See CFPB, List of Consumer Reporting Companies at 28, (2023), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2023.pdf. As such, these databases would be subject to the file disclosure, accuracy, and dispute resolution rights under the FCRA.

strategy to stop fraudsters before they have stolen money from individuals and families. Criminals know no boundaries; they leverage technology to perpetrate their schemes quickly and are oftentimes unknown until it is too late. Staying ahead of these players requires rigorous and easy lines of communication between partners—including private attorneys and non-profit organizations—who are often the first to hear about scams on the ground.

NCLC provided many of the recommendations that follow in comments to the FTC Collaboration Act of 2021.¹³⁰ One of these recommendations is that the FTC develop a Fraud Task Force to ensure more regular information sharing and cooperation among all the various agencies that see and deal with individual pieces of the fraud landscape.

We therefore support legislation¹³¹ that encourages partnerships among various stakeholders, including regulators, industry representatives, consumer groups, and victim support groups. These kinds of task forces will not solve the problem of payment fraud, but will be an important first step to broaden information sharing.

2. Simplify fraud reporting.

Since reportfraud.ftc.gov and ic3.gov are two of the most used sites to report fraud, the FTC and the FBI should work with the CFPB, banking regulators, and state Attorneys General (AGs) and local law enforcement to simplify fraud reporting for consumers. Consumers may report fraud to many different places – the local police department, the FBI, an AG, the CFPB, or the FTC. Sometimes police refuse to take fraud reports, viewing fraud as a civil matter. Once a consumer is turned away once place, they may give up. We advise consumers to file a complaint in as many places as possible, but that is cumbersome and not always realistic. Consumers may also find that they are asked for the same information multiple times from different agencies. We urge these agencies to:

- Develop standardized complaint intake forms that can be used by many different agencies.
- Provide a range of easily accessible channels (e.g. in person, phone, e-mail, web, mobile app) for consumers to submit complaints and grievances.
- Include options to report fraud and other complaints in multiple languages.

Fraud reporting must be as simple and universal as possible to be effective.

¹³⁰ See NCLC *et al.*, *Comments regarding the FTC Collaboration Act of 2021*, (August 14, 2023), available at https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final3-Lauren-Saunders.pdf.

¹³¹ See, e.g., the Taskforce for Recognizing and Averting Payment Scams Act (TRAPS ACT), 2025. (S. 2019) available at <https://www.congress.gov/bill/119th-congress/senate-bill/2019/text>; Financial Services and General Government Appropriations Bill, 2024. (S. 2309), Title I. Department of the Treasury, “Financial Fraud” at 10, available at https://www.appropriations.senate.gov/imo/media/doc/fy24_fsgg_report.pdf.

3. Require fraud reporting within payment systems.

As previously mentioned, the operators of FedNow, RTP®, and Zelle already collect reports of fraud, and they should analyze those reports, follow up on patterns, and develop preventive measures if they are not already doing so.

It is critical for every entity participating in payments, such as payment providers, financial institutions, and network providers, like the Federal Reserve Board, to:

- Develop and constantly improve measures to prevent fraud in the first place;
- Detect and stop fraud as soon as possible;
- Share information about fraudulent actors;
- Build in incentives and processes for consumers to report fraud; and
- Develop and include in the system rules methods to compensate victims and correct errors wherever possible.

We especially urge the Federal Reserve Board, the operators of other wire transfer services, and other bank regulators to devote attention to bank-to-bank wire transfers. While there is a fair amount of knowledge about how consumers are defrauded into sending funds through wire transfers, no one seems to be collecting or analyzing information about the accounts into which funds are sent. Some of these questions can only be answered by the banks, bank regulators, or wire transfer operators. We understand that the Federal Reserve Board does not receive fraud reports from institutions utilizing Fedwire, though it may be exploring doing so. We do not know what fraud information is collected on other wire transfer services, such as The Clearing House's CHIPS system. NCLC provided suggestions on how the Reserve Banks and the Federal Reserve Board can build protections into Fedwire operations and impose requirements on Fedwire users to help detect fraud, prevent it from spreading, and recover money sent due to fraud or error when possible.¹³²

As previously mentioned, the Federal Reserve Banks should also explore collecting information on check fraud.

The more information law enforcement, payment system operators, and regulators have about fraud committed through these platforms, and the more that agencies work together to identify trends, the more avenues there will be for stopping fraud.

4. Require FinCEN to update the Suspicious Activity Report (SAR) to capture information about accounts that receive fraudulent funds.

FinCEN can help in the fight against payment fraud by updating the suspicious activity report (SAR) to encompass information about the accounts used to receive ill-gotten funds. The current SAR form only accommodates accounts related to the reporting institution. In fraud cases where

¹³² NCLC, *Comments regarding the Request for Information on Potential Actions to Address Payments Fraud by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation*, at 26-31 (September 15, 2025), available at https://www.nclc.org/wp-content/uploads/2025/09/2025.09.15_Comments_Fraud-RFI-on-Payments-Fraud.pdf.

the destination account of the perpetrator is known, reporting institutions relegate the destination account to the narrative. This makes identification and aggregation of fraudulent activity more difficult for law enforcement.

When a consumer's financial institution files a SAR following an incident of payment fraud, if the payment was sent through a system that identifies the recipient (such as a wire transfer, ACH, or P2P system), the SAR should identify the recipient institution and account. Allowing accounts not domiciled at the reporting institution to be reported and designated appropriately would assist FinCEN and law enforcement in identifying, aggregating, and prioritizing fraud investigations to better protect consumers.

Since fraud schemes affect many victims at various reporting institutions, fraud often results in a hub-and-spoke relationship with one account receiving funds from many different, unrelated accounts. This typology is recognized in the FFIEC Exam Manual and should be supported at FinCEN by enhancing the SAR reporting process to include the fraud perpetrator's account at the receiving institution.

5. Ensure consumers are protected from false positives.

Although there are legal obstacles to sharing specific PII (personal identifying information) about an accountholder who may be engaging in payment fraud, this information is critical to stop criminal fraudsters from opening accounts that are then used to receive fraudulent payments. Account numbers without the accountholder's individual or business information are not as useful in preventing future fraud by that same individual or business.

At the same time, if current legal regimes are interpreted or amended to allow for this type of information sharing (including changes to the BSA or the Gramm-Leach-Bliley Act),¹³³ then innocent consumers who are negatively impacted by the sharing of this information need adequate protection. Consumers who experience an account closure, account freeze, or the inability to open a new bank account after a closure due to suspected fraud (an adverse action) based on the shared information should have protections like those already provided under the Fair Credit Reporting Act. These protections should ensure, at a minimum, that:

- Any shared information is accurate and not misleading;
- A consumer is given notice if the shared information leads to an adverse action;
- A consumer is given the opportunity to dispute the inaccuracy of any shared information and have the information be corrected if inaccurate; and

¹³³ For additional feedback on the consumer protections needed in the context of information sharing and privacy, see EPIC and NCLC, *Comments to the U.S. House Committee on Financial Services In re: Request for Feedback on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals*, (August 28, 2025), available at <https://epic.org/wp-content/uploads/2025/09/EPIC-NCLC-HFSC-financial-privacy-comment.pdf>.

- The entity that took the adverse action against the consumer investigates the consumer's dispute and takes any remedial action if the adverse action was based on inaccurate information.

In other words, Congress and regulators should encourage information sharing to prevent and stop fraud, but only when adequate guardrails are in place to address false positives and provide relief when innocent consumers are harmed by the false positives.

As discussed in more detail below, impacted consumers should have an avenue for disputing account closures and freezes through the EFTA's error resolution procedures.

IX. Challenges with Account Freezes, Closures, and Holds Due to Fraud Lead to Debanking Consumers.

In recent years, many consumers have raised concerns about bank account closures and/or freezes that seem to occur without any sudden change of behavior by the consumer or in response to a fraud dispute by the consumer (when the consumer reports that some unauthorized use has occurred in their account). Some consumers have also reported that even when a financial institution temporarily credits an account for a fund transfer that a consumer has disputed as unauthorized, the financial institution will then refreeze that amount or the entire account within hours after the recredit. Consumers report frustration and uncertainty tied to account closures and freezes— primarily due to the lack of information regarding why the closure or freeze occurred and the inability to access funds in a timely manner.

The number of consumers who have complained about checking and savings account closures to the CFPB more than doubled since 2017.¹³⁴ In 2022, the CFPB ordered Wells Fargo to pay \$160 million to over one million people for improperly freezing or closing bank accounts from 2011 to 2016 when it “believed that a fraudulent deposit had been made into a consumer deposit account based largely on an automated fraud detection system.”¹³⁵

There have also been stories featured by reporters detailing the devastating impact sudden account closures and freezes can have on consumers, especially when they are deprived access to their funds, are not provided with any information about the reason for the institution's actions, and are not provided an opportunity to address any perceived risk.¹³⁶

¹³⁴ Consumer Financial Protection Bureau, Consumer Complaint Database, trends data for complaints received due to checking or savings account closure, https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&dateRange=All&date_received_max=2024-01-27&date_received_min=2011-12-01&has_narrative=true&issue=Closing%20an%20account%E2%80%A2Company%20closed%20your%20account&lens=Product&product=Checking%20or%20savings%20account&searchField=all&subLens=sub_product&tab=Trends, (last visited February 20, 2024).

¹³⁵ *In re. Wells Fargo Bank, N.A.*, CFPB No. 2022-CFPB-0011 (December 20, 2022) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

¹³⁶ Barnard, Tara Siegel and Lieber, Ron, “Banks Are Closing Customer Accounts, With Little Explanation,” New York Times, (April 8, 2023), available at https://www.nytimes.com/2023/04/08/your-money/bank-account-suspicious-activity.html?unlocked_article_code=1.QU0.szRm.kfoZRQdD7-O6&smid=url-share; Kessler, Carson, “A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers’ Money,” ProPublica, (July 6, 2021), available at <https://www.propublica.org/article/chime>; McGreevy, Patrick, “Bank of America must

One of the reasons for the increase in account closures and freezes has to do with the increased adoption of tools utilized by financial institutions to combat payment fraud and detect suspicious activity, including adoption of artificial intelligence (AI) and machine learning technologies. Fraud vigilance is critical, and new technologies can play an important role. However, these tools may harm innocent consumers if not utilized properly and if institutions do not have clear procedures and timelines in place to restore access to funds that are improperly frozen.

A. Overaggressive fraud algorithms can shut out innocent consumers from access to their bank accounts and funds, and overly broad BSA programs prevent these consumers from understanding why those actions were taken.

Financial institutions have an obligation under the BSA to ensure that they maintain and follow internal ongoing Customer Due Diligence (CDD) programs and policies. The CDD program's policies must allow the institution to understand "the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and [c]onducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."¹³⁷

Because of the CDD obligation and the ongoing problem of payment fraud, sometimes the appropriate response by an institution that suspects its customer is engaging in fraudulent or other illicit activity is to freeze a transaction or close an account that is being used to receive fraudulent funds before the funds are gone and more consumers can be defrauded. But sometimes financial institutions get it wrong, especially when automated tools are used. No law requires a financial institution to take these actions; it is up to the risk tolerance of the company and the internal policies set in place by the company. The only required response to potential fraud a company may need to undertake under BSA/AML law is to file a SAR if the transaction is large enough to meet the threshold reporting requirements and update their customer risk profile.¹³⁸

According to the Bank Policy Institute, "a sample of the largest banks reviewed approximately 16 million alerts, filed over 640,000 SARs, and received feedback from law enforcement on a median of 4% of those SARs. Ultimately, this means that 90-95% of the individuals that banks report on were likely innocent."¹³⁹ As these numbers demonstrate, even activity that leads to the filing of a SAR may ultimately not warrant an account freeze or closure.

provide more proof of fraud before freezing EDD accounts, court orders," Los Angeles Times, (June 1, 2021), available at <https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california>; KCAL News, "Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud," (October 29, 2020), available at <https://www.cbsnews.com/losangeles/news/bank-of-america-freezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/>.

¹³⁷ 31 C.F.R. § 1020.210(a)(2)(v);(b)(2)(v).

¹³⁸ Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, Final Rule, 81 Fed. Reg. 29398 (May 11, 2016); 31 C.F.R. 1020.210(b)(i); Office of the Comptroller of the Currency, *Bank Secrecy Act (BSA)*, available at <https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html/>.

¹³⁹ Bank Policy Institute, "The Truth About Suspicious Activity Reports," (September 22, 2020), available at

To compound matters, many financial institutions believe that if an account was closed or frozen and a SAR was filed, they are not allowed to disclose the reason why the account was closed or frozen, because it would lead to the assumption that a SAR was filed. As a result, consumers are not told why their account is closed or funds are frozen, or they are given the run-around. Many consumers have reported that financial institutions reply that they cannot disclose any information as to why the account was closed or frozen. Yet financial institutions are only prohibited from disclosing the existence of the SAR, not responding to consumer concerns that their account was frozen or closed improperly.

The impact of sudden account closures in response to potential fraud on innocent consumers cannot be overstated. Often, the most vulnerable people have been denied access to their money, rendering them unable to eat or pay rent. Some impact on innocent individuals may be impossible to avoid, as banks may need to act quickly on imperfect information. But that is why it is imperative to have procedures in place to enable people to dispute account freezes and closures and get their money back as soon as possible.

If people cannot access the money they need based on red flags triggered by automated fraud tracking systems, then they need a timely solution, not another obstacle. Yet that is what occurs; consumers face obstacles upon obstacles. When a consumer complains about an account closure or freeze, the complaint is often not followed by a reasonable investigation by the financial institution that includes a discussion with the consumer or that provides any clear timeline to unfreeze their money.

NCLC has assisted many impacted consumers with complaints to the OCC, Treasury (when an impacted account was through the Direct Express program), or by leveraging connections within large financial institutions to look into an account and resolve the issue. However, this is not a sustainable solution for all impacted consumers. Policies need to change. Crude AML/CFT compliance policies and overly broad fraud responses can shut consumers out of our banking system.

The EFTA has clear error resolution timelines and procedures, and those should be used when consumers cannot access their funds. When a consumer is unable to make an electronic withdrawal or transfer because of an account closure or freeze based on suspected fraud, that action should be viewed as an error – an incorrect transfer of zero instead of the requested amount – triggering the error resolution rights, duties, timelines, and investigation procedures of the EFTA. The EFTA’s error resolution procedures can also be triggered by the consumer’s request for information about a failed EFT, which is another enumerated error under the EFTA.¹⁴⁰ However, financial institutions and payment apps seem to believe the EFTA does not apply in this situation.

<https://bpi.com/the-truth-about-suspicious-activity-reports/> (citing, Bank Pol’y Inst., *Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance*, (October 29, 2018) available at https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf).

¹⁴⁰ 15 U.S.C. § 1693f(f)(6).

B. Potential remedies to address improper freezes or account closures due to the use of automated fraud detection.

The problem with account closures and freezes could be addressed by rulemaking or guidance from the CFPB, though that is not necessary. Regulators should interpret the EFTA's error resolution procedures to apply to disputes from consumers when EFTs fail because of an account freeze or closure. The EFTA's error resolution procedures allow financial institutions to continue using automated fraud detection systems while ensuring that there are procedures in place for resolving disputes in a reasonable time and give consumers remedies when those systems get it wrong. This would ensure a consumer receives information about why their account was frozen or closed and get more timely access to their funds if the bank was in error.

Even apart from the EFTA, the CFPB and bank regulators should also provide guidance to financial institutions about the importance of having clear procedures to enable consumers to quickly regain access to their funds when they are frozen due to concerns of suspicious activity, provide guidance as to the timeliness of returning an account holder's funds after account closure, and specify that failing to have clear procedures and provide timely return of any funds may constitute an unfair, deceptive, or abusive business practice.

Bank regulators, along with FinCEN, should provide guidance to financial institutions about what information they may and should provide to account holders regarding freezes and account closures while still complying with the BSA. For example, they could clarify in an FAQ that, while financial institutions are not allowed to disclose that a SAR was filed, they are allowed to describe the specific activities that raised concerns, giving the consumer an opportunity to respond and appeal a decision that was made in error, or based on false assumptions or false red flags. They should also clarify that if a SAR does not lead to criminal prosecution or involvement by law enforcement for suspected money laundering/financing of terrorism activity, then a financial institution should not automatically take derisking measures and close the account based solely on the filing of a SAR, but the institution should instead take a measured, case-by-case, risk-based approach.

Finally, regulators should investigate the reasons that deposit accounts are closed or frozen and develop a strategy to minimize the number of account closures for innocent consumers.

X. Fraud Traverses Many Industries and Sectors, and the Federal Government Must Take a Holistic Approach to Combatting Fraud.

A. Criminal Fraudsters rely heavily on text messages to initiate fraud schemes.

Calls and text messages are a significant and increasing contact method for fraud. In 2022, victims reported losses of over \$1.1 billion from phone and text message-based scams.¹⁴¹ Reported losses have been increasing steadily and substantially to over \$1.4 billion in 2024.¹⁴²

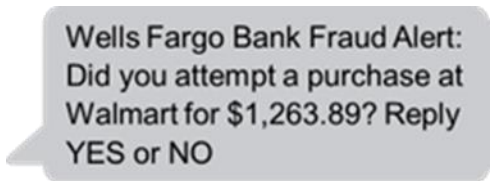
¹⁴¹ FTC Consumer Sentinel Network, Fraud Reports by Contact Method, Reports and Amount Lost by Contact Method, Year: 2021, (updated Feb. 22, 2022), available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>.

¹⁴² [Consumer Sentinel Network Data Book 2024](#), at pg. 12.

Scammers are attracted to calls and texts because they can use them inexpensively and anonymously through complicit service providers that know they are transmitting scam calls to consumers. These providers make money connecting scammers to their victims, and given the steadily increasing losses from phone and text scams, it is clear that existing laws and regulations do not have a sufficient deterrent effect.

Increased collaboration among the prudential regulators, the Federal Communications Commission (FCC), and other stakeholders could help prevent payments fraud resulting from imposter scams. Imposter scams occur when a criminal fraudster pretends to be a government agency, financial institution, or legitimate business. The criminal then contacts a consumer to alert them to a fake and urgent problem and attempts to persuade them to transfer their money under these false pretenses.¹⁴³ Imposter scams are a rapidly intensifying problem that disproportionately impacts older adults. Indeed, “combined losses reported by older adults who lost more than \$100,000 increased eight-fold, from \$55 million in 2020 to \$445 million in 2024.”¹⁴⁴

Financial institutions as well as consumers are harmed by these scams, which often start as robocalls or texts that appear to be from banks, with text messages like this:



Wells Fargo Bank Fraud Alert:
Did you attempt a purchase at
Walmart for \$1,263.89? Reply
YES or NO

A reply to the text will precipitate a call from the (fake) fraud department. Victims 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 \$3,000. The FTC announced that in

2023, these scams accounted for \$330 million in reported losses.¹⁴⁵

B. Recommendations to address scams initiated by text.

NCLC has previously urged the OCC to address imposter scams and the resulting payments fraud by encouraging or requiring banks to employ safe texting protocols, which allow consumers to easily differentiate between legitimate communications from their financial institutions and dangerous imposter scam texts.¹⁴⁶ Additional collaboration with the FCC to identify and promulgate measures to address the role of scam calls and texts in imposter scams will help to detect and prevent payments fraud.

Additionally, prudential regulators should consider collaboration with law enforcement agencies and state attorneys general and regulators to prosecute companies that facilitate and profit from

¹⁴³ See “FTC Data Show a More Than Four-Fold Increase in Reports of Impersonation Scammers Stealing Tens and Even Hundreds of Thousands from Older Adults,” (August 7, 2025), available at: <https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-data-show-more-four-fold-increase-reports-impersonation-scammers-stealing-tens-even-hundreds>.

¹⁴⁴ *Id.*

¹⁴⁵ FTC, “New FTC Data Analysis Shows Bank Impersonation is Most-Reported Text Message Scam,” (June 8, 2023), available at <https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam>.

¹⁴⁶ See NCLC’s letter to the OCC available at: https://www.nclc.org/wp-content/uploads/2024/10/2024.03.29_Letter_OCC-and-Texts.pdf

imposter scams and other fraud. For example, the Social Security Administration's (SSA) Office of the Inspector General and the Department of Justice partnered with several law enforcement agencies, the FCC, and the Federal Trade Commission to bring enforcement actions against several communications providers that knowingly transmitted scam calls impersonating the SSA.¹⁴⁷

Congress should also pass legislation and work with the FCC to address fraud facilitated by texts and calls.¹⁴⁸ Some of these include:

- Requiring a bond for transmitters of phone calls and texts.¹⁴⁹ This will force providers to either post a substantial sum or convince a third-party bond company that it is a legitimate company that does not intend to transmit fraudulent calls to U.S. consumers.
- Fixing any uncertainty as to whether the FCC has a legal pathway to assess civil penalties by restoring the FCC's enforcement ability. Congress should specifically authorize the FCC to file actions for civil penalties in federal district courts.
- Requiring rigorous know-your-customer and know-your-traffic procedures that force carriers to vet callers and calls that transit their network.
- Requiring record-keeping for call originators to ensure that information about callers is available for government or private enforcement efforts.
- Requiring carriers to investigate call traffic that displays suspicious characteristics, like a high percentage of short-duration calls and other indicia of fraud.
- Adopting federal regulations for phone number resellers to address phone number rotation schemes that allow callers to undermine the goals of the STIR/SHAKEN framework.¹⁵⁰
- Strengthening the Telephone Consumer Protection Act (TCPA) to encourage robust enforcement against scam callers and those who facilitate fraud by:
 - including an explicit cause of action for assisting and facilitating callers who violate the TCPA;
 - amending the definition of "telephone solicitation" and telemarketing in the TCPA and regulations to cover scam calls, for instance, by explicitly extending existing definitions to cover calls that attempt to defraud, cause harm, or wrongfully obtain anything of value;

¹⁴⁷ Office of the Inspector General, Social Security Administration, "Civil Action to Prevent Social Security Scam Calls from Reaching Consumers," available at <https://oig.ssa.gov/scam-alerts/2025-07-17-civil-action-to-prevent-social-security-scam-calls-from-reaching-consumers/> (last accessed September 16, 2025).

¹⁴⁸ See NCLC, *Letter to the Joint Economic Committee regarding the problems caused by scam calls and texts*, (June 16, 2025), available at <https://www.nclc.org/wp-content/uploads/2025/07/Email-to-JEC-6-16-25.pdf>.

¹⁴⁹ VoIP providers should be required to obtain a bond from a third-party and show proof of the bond before they can obtain the certifications necessary to sign calls under the STIR/SHAKEN framework. Bond amounts could ensure that there are funds available to satisfy judgements obtained in government or private enforcement actions related to illegal calls. Bond issuers would have an economic incentive to vet bond applicants thoroughly to make sure they are identifiable and unlikely to transmit illegal calls that would result in damages that the bond issuer would have to pay out of the bond amount. Originating carriers would risk losing their bond if they provided false STIR/SHAKEN attestations or allow unknown entities to place calls through their network.

¹⁵⁰ Phone number resellers who do not keep records that identify the end user of a phone number should be held liable for any losses caused by calls using the phone number. And a fee for short term use of phone numbers should be instituted to make it deter the purchase temporary phone numbers for use in rotation schemes by making it economically infeasible.

- extending the existing cause of action for violation of the TCPA's do-not-call regulations to allow individuals to bring a suit after receiving one violative call;
- creating a private cause of action for violations of the technical and procedural restrictions in the TCPA; and
- allowing for recovery of attorney's fees for a prevailing plaintiff in a TCPA suit.
- Strengthening the Telemarketing Sales Rule (TSR) to expand enforcement by:
 - Reducing or removing the requirement of \$50,000 in individual damages for private suits under the TSR;
 - expanding the definition of "telemarketing" in the TSR to cover scam calls, for instance, by explicitly extending existing definitions to cover calls that attempt to defraud, cause harm, or wrongfully obtain anything of value; and
 - specifying that short-term use of telephone numbers in rotation schemes is a deceptive telemarketing practice.

XI. Fraud Prevention Education Is Necessary in the Fight Against Fraud, But It Will Not Solve the Problem.

Although consumer and business education is important, it alone will not solve the problem of payment fraud. Criminal fraudsters have extraordinary creativity;¹⁵¹ they are constantly developing ways to steal people's money by setting up increasingly sophisticated schemes to obtain access to accounts or to fraudulently induce consumers into payment transactions.¹⁵²

¹⁵¹ For examples of the types of scams utilized by robocalls and scam texts, see NCLC, EPIC report *Scam Robocalls: Telecom Providers Profit*, at 6-10 (June 2022), available at <https://www.nclc.org/wp-content/uploads/2023/02/Robocall-Rpt-23.pdf>; see also Testimony of Margot Saunders, NCLC "Protecting Americans from Robocalls," Hearing Before the U.S. Senate Committee on Commerce, Science & Transportation, (October 24, 2023), available at <https://www.nclc.org/wp-content/uploads/2023/10/Testimony-of-NCLC-on-Robocalls-2023.pdf>.

¹⁵² See the scam warning below which also involves impersonation of law enforcement.

This Fake App Takes the Cake

This recent scam is impressively complex. The cybercriminals start by impersonating law enforcement officers. They contact you, claiming that your bank account may have been involved in financial fraud. You're then asked to download a mobile app to help them investigate further. If you download the app, the cybercriminal walks you through the steps to set this scam in motion.

First, you are given a case number. When you search for that number in the app, you'll find legal-looking documents with your name on them. These documents make the scam feel more legitimate. Once your guard is down, the app asks you to select your bank from a list and then enter your account number and other personal information.

As soon as consumers receive notice and information about one type of scam, the criminal fraudsters will develop new avenues and methods to defraud them. As a result, we recommend in-app and real-time education by payment providers and financial institutions, as well as social media and telecommunications providers. For example, simply requiring “confirmation of payee” prompts and pop-ups with questions about transactions and red flags may prevent consumers from sending payment to a criminal fraudster.

Consumers and businesses should also receive broader education about cybersecurity instead of just scams and fraud. Better education about internet safety, phishing, vishing, ransomware, and business email compromise would also reduce the amount of account takeovers and fraud schemes that lead to monetary loss from payments fraud.

With respect to check fraud, we support consumer education about safer ways to make payments.¹⁵³ For example, as we described in our comments to the Treasury Department’s Request for Information on Modernizing Payments,¹⁵⁴ the goal of reducing the number of paper

The most clever part of this scam is what the app does in the background. When you first install the app, it blocks all incoming calls and text messages. That way, you won’t be alerted if your bank attempts to contact you about unusual behavior on your account. If all goes as planned, the cybercriminals will steal your money and sensitive information before you know what happened.

No matter how advanced the app is, you can stay safe from scams like this by following the tips below.

- Only download apps from trusted publishers. Anyone can publish an app on official app stores or sites—including cybercriminals.
- Be cautious of scare tactics that play with your emotions. Cyberattacks are designed to catch you off guard and trigger you to reveal sensitive information.
- If you’re contacted by someone claiming to be in a position of authority, like law enforcement, ask them to confirm their identity. Real officials will understand your concerns and can provide information that doesn’t require you to download an app.

The KnowBe4 Security Team

KnowBe4.com

¹⁵³ See, e.g., AARP, “Should You Stop Using Paper Checks?” (August 14, 2023), available at <https://www.aarp.org/money/scams-fraud/prevent-stolen-checks-mail-theft/>.

¹⁵⁴ NCLC, *Comments to the Department of Treasury’s Request for Information on Modernizing Payments*, (June 30, 2025), available at https://www.nclc.org/wp-content/uploads/2025/07/2025.06.30_Comments_Modernizing-Payments-To-and-From-Americas-Bank-Account.pdf.

checks sent by and to the federal government is a worthy one. We support outreach to identify the reasons that people use paper checks, to address those reasons, and to encourage people to send and receive money through safer electronic payments. However, we oppose simply ending all use of checks to and from the federal government on a given date, which will only harm consumers.

At the same time, the fear of fraud in electronic payments is one of the reasons that people use checks today. Even if electronic payments are safer than checks (we do not know if that is actually true on a percentage basis, especially if you include fraudulently induced payments), reports of fraud on electronic payment platforms and the lack of consumer remedies make many people hesitant to use those platforms. Thus, we need to both reduce fraud in electronic payments and improve remedies for consumers as part of the transition away from checks.

We also support consumer education about safer ways to pay by check, such as the use of permanent ink and taking mail directly to the post office. AARP has put out materials on that topic.¹⁵⁵ The Agencies and financial institutions can educate consumers on these methods – which will also serve the goal of making people aware of check washing and encourage the use of electronic payments.

Finally, any education that is provided to consumers (including in-app pop-ups or notifications) should be done in a language that is chosen by the consumer and with considerations for individuals with disabilities. Individuals with limited English proficiency or disabilities are often targeted by criminal fraudsters and are the most vulnerable to fraud schemes that take advantage of the lack of access to information that is available in a form that can be understood.

XII. Conclusion

Payment fraud is a pervasive problem impacting U.S. consumers, especially those most vulnerable to the loss of income caused by unauthorized and fraudulently induced transactions. However, Congress can take steps to address these problems by utilizing a holistic approach to the problems caused by fraud and scams instead of just relying on consumer education and information dissemination.

With any questions, please contact Carla Sanchez-Adams, Senior Attorney at the National Consumer Law Center, at csanchezadams@nclc.org.

Thank you for the opportunity to provide this statement for the record.

Yours very truly,

National Consumer Law Center (on behalf of its low-income clients)

¹⁵⁵ See AARP, “6 Ways You Can Thwart Check Washers,” (March 2, 2023), available at <https://www.aarp.org/money/scams-fraud/stop-check-washers/>.