“Examining Scams and Fraud in the Banking System and Their Impact on Consumers”

U.S. Senate Committee on Banking, Housing, and Urban Affairs

Thursday, February 1, 2024

Testimony of Carla Sanchez-Adams

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

National Consumer Law Center

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

U.S. Senate Committee on Banking, Housing, and Urban Affairs

Testimony of Carla Sanchez-Adams

Thursday, February 1, 2024

Chairman Brown, Ranking Member Scott, and Members of the Committee, thank you for inviting me to testify today regarding scams and fraud in the banking system and their impact on consumers. 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 and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people 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, regulation, 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.

Payment fraud impacts all Americans across many communities— young, old, those highly educated, and those that are not. But the impacts of fraud are most keenly felt by certain vulnerable populations such as older Americans, low-income consumers, and minorities.

Consumers are plagued by problems with unauthorized transactions as well as fraudulently induced transactions over peer-to-peer payment applications, bank-to-bank wire transfers, check alterations and forgeries, and Electronic Benefits Transfer card skimming. The increasing ease

[1] *See* 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.govinfo.gov/content/pkg/CHRG-117hhrg47649/pdf/CHRG-117hhrg47649.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 (Sept. 23, 2021) available at https://www.nclc.org/wp-content/uploads/2022/08/Testimony_Covid_Aging-1.pdf.

[2] *See* NCLC *et al.*, Comments regarding the FTC Collaboration Act of 2021, (Aug. 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, (Aug. 10, 2022) available at https://www.nclc.org/wp-content/uploads/2022/09/FedNow_fraud_ltr.pdf; 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 Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), https://bit.ly/FedNowCoalitionComments ("FedNow Comments").

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 this data.

The financial institutions that design and run these payment systems, including the financial institutions that hold the accounts of scammers 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, as they are doing in the United Kingdom, they will have the incentive to leverage the latest innovative technologies to prevent and detect fraud, 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.

To combat payment fraud, we recommend addressing the current gaps and ambiguities in the Electronic Funds Transfer Act 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 scammer to receive the fraudulent payment;
- 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;
- Eliminating the exclusion of Electronic Benefit Transfer 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 aggressive fraud reporting. For example, federal regulators should:

- 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; and
- Provide guidance to financial institutions about the timelines and procedures for consumers to regain access to improperly frozen funds and clarify what information can and should be given to accountholders regarding account closures and freezes.

I. Fraud is Exploding and Affects Everyone.

Fraud continues to climb and devastates millions of consumers across the country each year. In 2022, the Federal Trade Commission (FTC) received over 2.5 million reports of fraud with reported losses totaling almost $9 billion ($8,996,000). Those losses are up a shocking 46.7% over 2021. Losses for 2023, which have not yet been fully reported, are on track to exceed 2022.

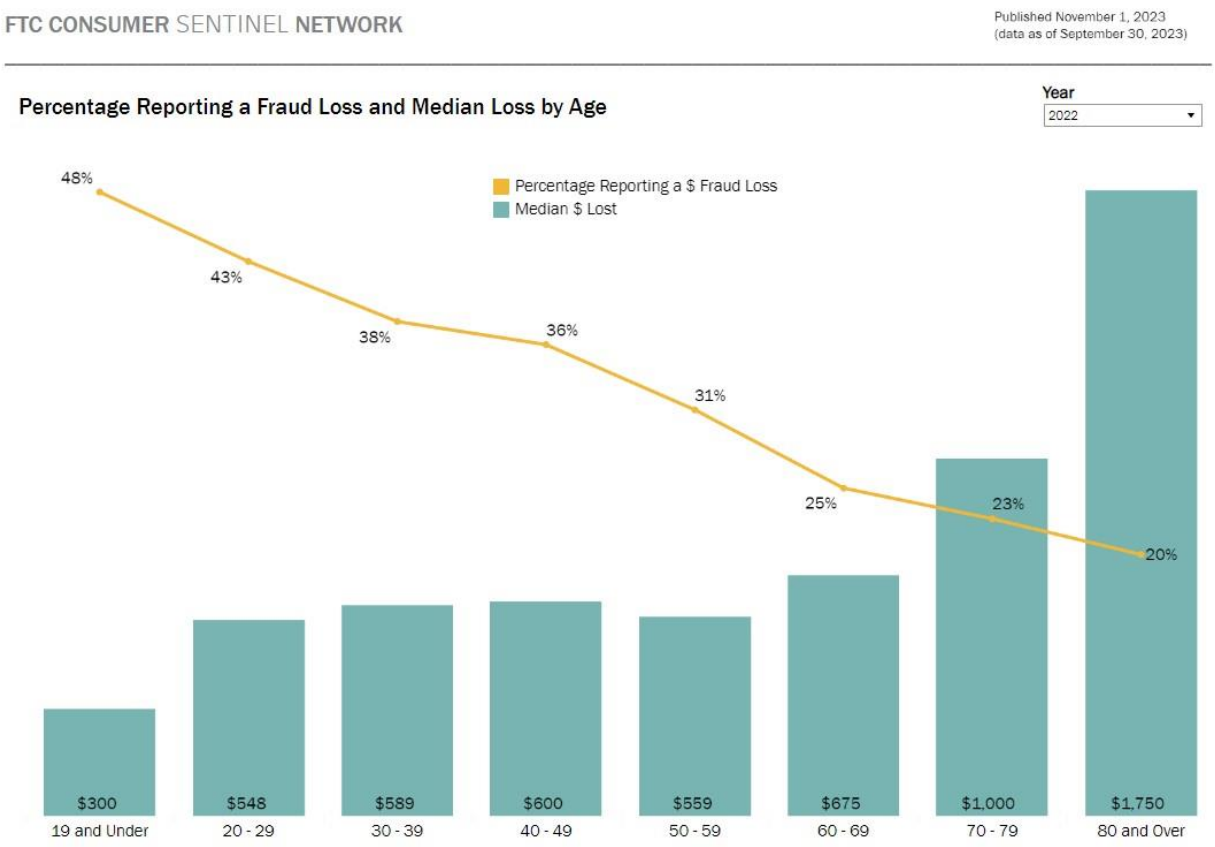
Additionally, the FTC numbers reflect only fraud cases reported to the FTC. Fraud is substantially underreported; only an estimated 15% of U.S. fraud victims report the fraud to law enforcement.[3]

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."[4]

Fraud impacts all of us, across every community— the young and the old, those highly educated and those that are not.[5] While the common belief is that older consumers are more likely to be susceptible, in fact younger people are significantly more likely to experience fraud. But when older people suffer fraud, they lose far more money, as shown by the following FTC chart:[6]

[3] Department of Justice, U.S. District Attorney's Office, District of Alaska, Financial Crime Fraud Victims (2020), https://www.justice.gov/usao-ak/financial-fraud-crimes.
[4] Williams, Alicia R., "*Americans Are Aware of Fraud's Pervasiveness but Remain Vulnerable*," AARP Research (May 17, 2023); *see* Department of Justice, U.S. District Attorney's Office, District of Alaska, Financial Crime Fraud Victims (2020), https://www.justice.gov/usao-ak/financial-fraud-crimes.
[5] Levinthal, Dave, "*Cyberthieves stole $186,000 from a Republican member of Congress as fraud epidemic plagues political committees*," Business Insider (Nov. 29, 2022) available at https://www.businessinsider.com/online-fraud-congress-diana-harshbarger-cybertheft-2022-11.
[6] FTC, Percentage Reporting a Fraud Loss and Median Loss by Age (2022), *available at* https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses.



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 Play an Important Role in Enabling or Preventing Fraud and in Protecting Consumers.

Criminals who steal money through fraud schemes need a way to obtain a victim's money. They use a variety of payment systems to receive that money, including person-to-person (P2P) transfer services, wire transfers, checks, and gift cards. Each of those payment systems has a role to play in keeping criminals out, preventing fraud, and protecting consumers. Fraud does not succeed 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 two institutions – the institution that holds the consumer's account (the consumer's institution) and the institution 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.

In the testimony below I will focus on four payment vehicles that have seen increasing fraud: person-to-person payments, 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 the need for more data sharing in the effort to combat fraud.

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. Seventy-six percent of households use Venmo or Cash App.[7] In addition to P2P payment services, consumers are also increasingly adopting other forms of technology to make payments.[8]

According to the FTC,[9] "payment app or service" is the third largest category of payment method specified by fraud victims in terms of number of reports (after credit cards and debit cards), and the dollar volume of losses by payment app or service increased 25% from 2021 to 2022.[10] Though the final figures of fraud reports are unavailable for 2023, the FTC received reports during the first three quarters of 2023 that are on path for another 25% increase by dollar amount of losses.[11] The Consumer Financial Protection Bureau (CFPB) has also seen high growth in complaints about fraud in P2P apps and digital wallets.[12]

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

---

[7] Anderson, Monica, "*Payment Apps like Venmo and Cash App Bring Convenience – and Security Concerns – to Some Users*," Pew Research Center (blog), (Sept. 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/.
[8] Chen, Jane, Deepa Mahajan, Marie-Claude Nadeau, and Roshan Varadarajan, "*Consumer Digital Payments: Already Mainstream, Increasingly Embedded, Still Evolving*," Digital Payments Consumer Survey, (Oct. 20, 2023), available at https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving.
[9] Reports of fraud to the FTC do not always specify the payment method utilized to perpetuate the fraud; however, the FTC does collect and report data on payment method when available.
[10] FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods. Only 429,264 (17%) of 2,563,959 fraud reports received by the FTC specified the payment method.
[11] *Id.*
[12] 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.

are not safe for consumers to use.[13]

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 minorities are also unbanked or underbanked,[14] 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.[15] Yet Cash App has also been subject to reports of widespread fraud,[16] failing to protect the very vulnerable populations it targets.

The news media has reported many of the fraudulent schemes enabled by the P2P systems. Generally, these scams and theft would not have been possible without the payment apps.

- Manhattan District Attorney Alvin Bragg explains how criminals have utilized deception, violence, or threat of violence to steal funds from consumers through payment apps like Cash App.[17]

- Mary Jones of Kansas City paid $1,700 through Venmo in "rent" to a man who claimed to own the house she wanted to move into. He even gave them access to tour the house before she signed the lease. After she saw a "For Lease" sign in the front yard, she called the rental company and discovered that she had paid a scammer. She filed a police report but has not been able to retrieve her money.[18]

- In a similar fraud scheme, a single mom in South Carolina looking for housing paid a deposit, cleaning fee, and first month's rent on a condo listed on Redfin.com through a payment app and lost $2,600.[19]

---

[13] *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 (Dec. 21, 2021), 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 Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), https://bit.ly/FedNowCoalitionComments (FedNow Comments).

[14] 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, https://www.fdic.gov/analysis/household-survey/2021report.pdf (last updated July 24, 2023).

[15] Anderson, Monica, "*Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users,*" Pew Research Center (Sept. 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/.

[16] Hindenburg Research, "*Block: How Inflated User Metrics and 'Frictionless' Fraud Facilitation Enabled Insiders To Cash Out Over $1 Billion*," (Mar. 23, 2023), available at https://hindenburgresearch.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").

[17] Morales, Mark, "*Venmo and other payment app theft is 'skyrocketing,' Manhattan DA warns*," CNN (Jan. 23, 2024), available at https://www.cnn.com/2024/01/23/business/venmo-payment-app-theft?cid=ios_app.

[18] 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/.

[19] Cioppa, Jordan, "*James Island woman says rental scam cost her $2,600*," WCBD News2 (Jan. 10, 2023), available at https://www.counton2.com/news/james-island-woman-says-rental-scam-cost-her-2600/.

Zelle is another popular P2P payment service, but users transfer funds between bank accounts directly.[20] As more and more consumers use Zelle, the service has also become popular among criminals.[21] For example:

- Maria Glover from Philadelphia had thousands of dollars stolen from her Citibank account via Zelle. She was contacted by the fraudsters through texts though she never provided any password or personal information to them. She further explains that the transactions stolen were for more than her $2,500 daily withdrawal limit, and Citibank could not even explain how the fraud occurred.[22]

- Luke Krafka, a professional musician in Long Island, lost almost $1,000 dollars through Zelle when a fake client "hired" him to play at a wedding. The man sent him a large check and asked him to pay part of the money back through Zelle. The check bounced after Krafka had already sent the money. His bank refused to refund his payment.[23]

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.

B. How technology perpetuates P2P fraud and theft.

Fraudsters have extraordinary creativity;[24] 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.[25] The Federal Communication

---

[20] The FTC designates Zelle transfers as part of the "bank transfer or payment" category, which also includes bank-to-bank wire transfers. *See* Section IV.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.

[21] Cowley, Stacy and Nguyen, Lananh, "*Senators question Zelle over how it is responding to reports of rising fraud*," New York Times (Apr. 26, 2022), available at https://www.nytimes.com/2022/04/26/business/zelle-fraud.html.

[22] 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 (Jun. 2, 2023), available at https://6abc.com/zelle-peer-to-peer-payment-apps-theft-auto-payments/13335405/.

[23] *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/ .

[24] *See* NCLC, EPIC report *Scam Robocalls: Telecom Providers Profit*, at 6-10 (Jun, 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 (Oct. 24, 2023) available at https://www.nclc.org/wp-content/uploads/2023/10/Testimony-of-NCLC-on-Robocalls-2023.pdf.

[25] *See the latest scam warning below which also involves impersonation of law enforcement.*

SCAM OF THE WEEK:
This Fake App Takes the Cake

Commission's (FCC) website includes a Scam Glossary detailing dozens of different ways individuals and small businesses have lost money to these schemes, [26] and the FCC specifically identified P2P apps as a primary means for executing scams and fraud.[27] Clearly, the warnings provided by the payment apps themselves to beware of scams and fraud are not adequate to protect consumers from the losses.

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.

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

[26] Federal Commc'ns Comm'n, Scam Glossary, *available at* https://www.fcc.gov/scam-glossary.
[27] Federal Commc'ns Comm'n, *As More Consumers Adopt Payment Apps, Scammers Follow* (updated Feb. 25, 2021), available at https://www.fcc.gov/more-consumers-adopt-payment-apps-scammers-follow.

Additionally, with imposter scams topping the FTC's category of fraud type in 2022,[28] the use of deep fakes generated by artificial intelligence (AI) to perpetuate payment fraud is disconcerting.[29] 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.[30]

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."[31]

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.[32] 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.[33]

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

---

[28] *See* Federal Trade Commission, *New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022,* (press release) (Feb. 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.

[29] *See* 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; 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.

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

[31] 12 C.F.R. § 1005.2(m) (emphasis added).

[32] 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*," (Dec. 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/.

[33] *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.[34]

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.[35] The CFPB also has authority to define additional categories of error.[36]

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

[34] Campisi, Natalie, "*Scammed Out Of Money On Zelle? You Might Be Able To Get It Back*," Forbes (Nov. 13, 2023), available at https://www.forbes.com/advisor/money-transfer/zelle-users-refunded-after-scams/.
[35] 15 U.S.C. § 1693f(f)(2), (6); 12 C.F.R. § 1005.11(a)((1)(ii), (vii).
[36] 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.[37]

Regulation E imposes the duty to investigate and resolve "errors," which includes "an incorrect electronic fund transfer to or from the consumer's account."[38] 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

---

[37] *See* Elliott, Christopher, "*A Venmo user sent $100 to the wrong person. Then the payment service froze his account*," Seattle Times (Nov. 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/.

[38] 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"[39] to the United Kingdom's Payments Systems Regulator (PSR).[40] 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.[41] 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.[42] The CRM Code was voluntary and existed to help financial institutions in the UK, "detect, prevent and respond to APP scams."[43]

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."[44] Two banks found the customer fully liable in 90% of their decisions.[45]

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

[39] 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.
[40] 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.
[41] Speech by the Lending Standards Board Chief Executive, Emma Lovell, "*International Perspective-Scams: Looking Forward: Priorities and opportunities*," (Mar. 15, 2022) available at https://www.lendingstandardsboard.org.uk/scams-looking-forward-priorities-and-opportunities-international-perspective-speech/.
[42] *Id.*
[43] *Id.*
[44] "*Banks called to account over 'shockingly low' rate of reimbursements for APP fraud*," Finextra (Sept. 15, 2021) available at https://www.finextra.com/newsarticle/38832/banks-called-to-account-over-shockingly-low-rate-of-reimbursements-for-app-fraud
[45] *Id.*

favor of the consumer.[46] This level of reversals suggests that the banks' high rate of denials was inconsistent with both the letter and the spirit of the Code.[47]

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.[48]

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."[49] 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.[50] Under the finalized rule, the victim's financial institution and the recipient's financial institution split the cost of reimbursement 50:50.[51]

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.[52] 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' 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

---

[46] Which?, "*Banks wrongly denying fraud victims compensation in up to 8 in 10 cases*," (Nov. 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/.

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

[48] "*UK Government to Legislate for Mandatory Reimbursement of App Fraud*," (Nov. 18, 2021), available at https://www.finextra.com/newsarticle/39245/uk-government-to-legislate-for-mandatory-reimbursement-of-app-fraud

[49] "*Fraud: MPs seek overhaul to tackle financial scammers*," (Feb. 2, 2022), available at https://www.bbc.com/news/business-60216076.

[50] Press Release: "*PSR confirms new requirements for APP fraud reimbursement*," available at https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/.

[51] To view a summary of the new 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.

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

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.[53]

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.

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.

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. But the CFPB has proposed a rule that will enable it to supervise large market participants who provide general-use digital consumer payment applications.[54] Greater supervision is important because compliance with basic EFTA obligations has been problematic even in supervised financial institutions, as noted above. The CFPB should swiftly finalize that rule and expand it to encompass the larger participants on the debit and prepaid card markets and domestic money transfer markets as well.

[53] 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.

[54] The CFPB issued a proposed rule to define larger participants of a market for general-use digital consumer payment applications which closed on January 8, 2024. The proposed rule may lead to greater supervision of some nonbank payment services, though not all. *See* NCLC *et al*., Comments to the CFPB's Proposed Rule Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, (Jan. 8, 2024) available at https://www.nclc.org/wp-content/uploads/2024/01/240108-CFPB-Payments-App-Comment-Final.pdf.

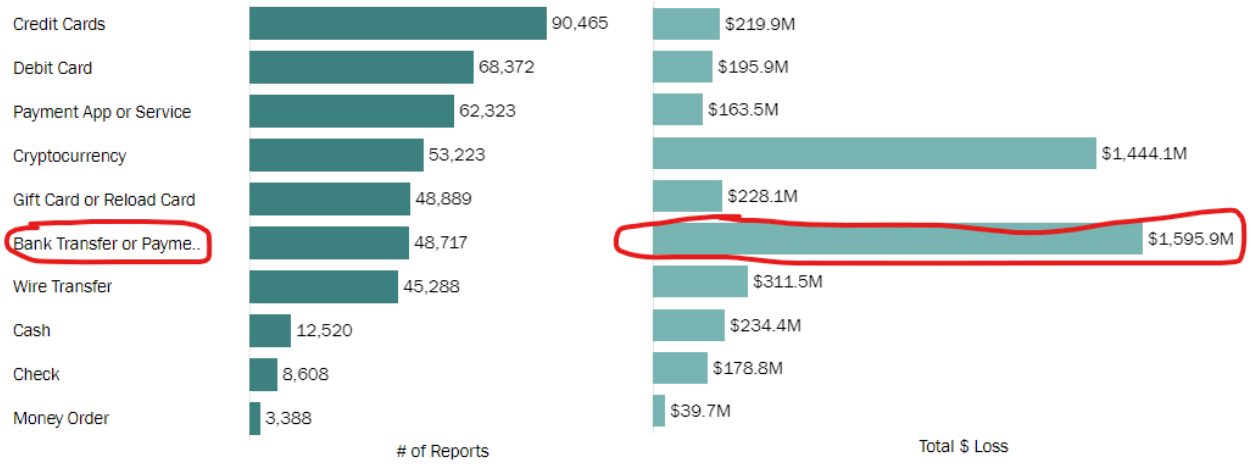
IV. Bank-to-Bank Wire Transfer Fraud.

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

The FTC's latest fraud data show that, in terms of dollars lost, "Bank Transfer or Payment" is the largest payment method used by fraudsters.[55] 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. (The FTC's "Wire Transfer" category includes only nonbank transfers like Western Union and MoneyGram.)

Cryptocurrency is a close second to bank transfer in total dollar amount of fraud losses reported to the FTC, and some losses through cryptocurrencies may start as bank-to-bank wire transfers to crypto banks or exchanges.[56] 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.[57]

2022 Fraud Reports to FTC by Payment Method



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 – nearly ninefold in five years.[58]

2019 Fraud Reports to FTC by Payment Method

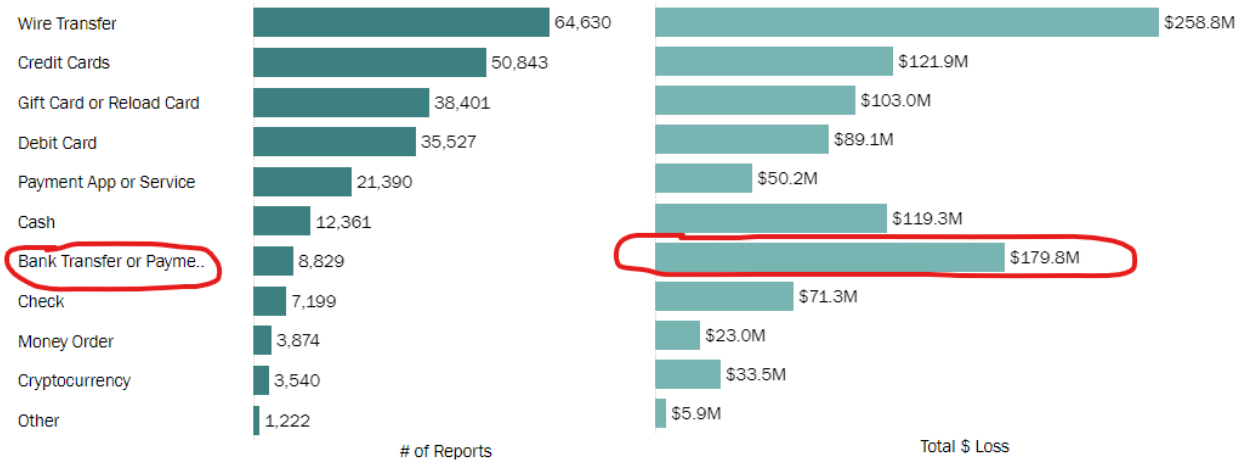
---

[55] FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[56] *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.

[57] Iacurci, Greg, "*How this 77-year old widow lost $661,000 in a common tech scam: 'I realized I had been defrauded of everything'*," CNBC (Oct. 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.

[58] The dollar losses in these two charts significantly understate actual losses, as only 12% (2019) to 17% (2022) of reports included information on payment method, and many fraud losses are not reported to the FTC.



For the first three quarters of 2023, the dollar amount of fraud losses due to bank transfer or payment reported to the FTC are on pace to exceed 2022 dollar losses by 14%.[59]

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

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.[60]

- 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.[61] He is a cancer patient and navigating the bank appeal process has been extremely stressful. These SIM swaps are increasingly common.[62]

- 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.[63]

- 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

[59] FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.
[60] Inquiry received by KPRC (Houston NBC station) reporter Amy Davis.
[61] Email from attorney on file with NCLC.
[62] *See* Barr, Luke, ABC News, "*'SIM swap' scams netted $68 million in 2021: FBI*" (Feb. 15, 2022), available at https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169.
[63] Email from CAMBDA Legal Services to NCLC, on file with NCLC.

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.[64]

- 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.[65]

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.[66]

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.[67]
    - 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

[64] Pending arbitration before AAA (Wells Fargo).
[65] Lawrence and Louis Company d/b/a Hidden Oasis Salon v. Truist Bank, No. 1:22-cv-200-RDA-JFA (E.D. Va.).
[66] ABC News, Good Morning America "*Woman sounds alarm on sophisticated wire transfer fraud*," (Jul. 21, 2023), available at https://abcnews.go.com/GMA/Living/video/woman-sounds-alarm-sophisticated-wire-transfer-fraud-101547100.
[67] Gordon, Clay, "*Central Ohio man loses $8,500 in Chase bank impersonation scam*," 10 WBNS (Mar. 30, 2023), available at https://www.10tv.com/article/money/consumer/wire-fraud-scam-warning/530-7af76f5c-cce0-4dcc-98a3-5c740a9043bd.

password, allowing him to drain $15,000 from her account.[68]

- 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.[69]

- 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.[70]

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."[71]

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

---

[68] McCormick, Erin "*Gone in seconds: rising text scams are draining US bank accounts*," The Guardian (Apr. 22, 2023), available at https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts.

[69] Johnson, Karin "*West Chester couple swindled out of thousands of dollars by crooks spoofing bank's phone number*," WLWT5 news (Nov. 16, 2023), available at https://www.wlwt.com/article/west-chester-chase-bank-spoofing-phone-number/45866051.

[70] Lee, Diane, "*Upstate couple warns of wire fraud that cost them $108,000*," CBS7 News, (May 19, 2023), available at https://www.wspa.com/news/upstate-couple-warns-of-wire-fraud-that-cost-them-108000/.

[71] Finney, Michael and Koury, Renee, "*Wells Fargo bankers tell East Bay customer they're too busy to stop wire scam*," ABC7 (Jun. 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.

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

The EFTA exempts electronic transfers, other than ACH transfers, made "by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer."[72] Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using FedWire, SWIFT, CHIPS, and Telex.[73] Thus, even if a criminal impersonates the consumer and makes a completely unauthorized wire transfer, the consumer may have no protection under Regulation E.[74]

At the time the EFTA was written in 1978, bank-to-bank wire transfer services were not viewed as a consumer payment system. 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.

Instead of the clear consumer protections provided by the EFTA, which was designed to protect consumers with clear rights and procedures, 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). The UCC was not designed as a consumer protection statute and was instead

[72] 15 U.S.C. §1693a(7)(B).
[73] 12 C.F.R. §1005.3(c)(3) (exempting FedWire or similar systems); Official Interpretation of 3(c)(3)-3 ("Fund transfer systems that are similar to Fedwire include the Clearing House Interbank Payments System (CHIPS), Society for Worldwide Interbank Financial Telecommunication (SWIFT), Telex, and transfers made on the books of correspondent banks.").
[74] However, as discussed in FN 77 below, some bank wire transfers may be within the EFTA's protection.

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.

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.[75] 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.[76] 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 if 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 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.

As previously stated, we 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

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

[76] *See* Complaint, People of the State of New York v. Citibank, No. 1:24-cv-00659 (S.D.N.Y. filed Jan. 30, 2024), *available at* https://ag.ny.gov/sites/default/files/2024-01/citi-complaint.pdf. The New York AG also alleges that the unauthorized wire transfers that occurred by electronic requests initiated by scammers via online banking or mobile app are covered by the EFTA. They are electronic instructions that do not come from the actual consumers who are Citi account holders and under the EFTA are unauthorized.

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.

V. 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.[77] 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, as described in Section III.D above.

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 is actually higher than for payment apps and services: $177.4 million in 2022 for checks compared to $163.5 million for payment apps and services. But this reported dollar loss is vastly understated;[78] one report a year ago puts annual check fraud losses at $815 million.[79]

Check fraud loss reported to the FTC increased by over 15% from 2021 to 2022.[80] Based on the first three quarters of 2023, check fraud losses are on pace to exceed 2022 numbers by 40%.[81]

In February 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

---

[77] DePompa, Rachel, '*Check washing' scams still on the rise*," Fox10 News (Jan. 25, 2024), *available at* https://www.fox10tv.com/2024/01/25/check-washing-scams-still-rise/.
[78] 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.
[79] Nadelle, David, "*Check Washing Is an $815M Per Year Scam — How It Works and Ways To Prevent It*," GoBanking Rates, (Feb. 22, 2023), https://www.nasdaq.com/articles/check-washing-is-an-$815m-per-year-scam-how-it-works-and-ways-to-prevent-it.
[80] *Id.*
[81] *Id.*

activity."[82] 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.[83] The statistics for check-fraud related SARs were not specific to mail-theft related check fraud.[84]

Technology also enables criminal organizations to traffic stolen checks. As a recent New York Times article[85] 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 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.[86] 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 recredited 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.[87]

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

---

[82] FIN-2023-Alert003 available at https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf

[83] *Id. citing* FinCEN SAR Stats available at https://www.fincen.gov/reports/sar-stats

[84] *Id. See* FN 10.

[85] Barnard, Tara Seigel, "*We Can't Stop Writing Paper Checks. Thieves Love That*," (Dec. 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

[86] Arroyo and Ramos v. Fifth Third Bank, N.A., Cause No. 2023L004163, Cook County, IL.

[87] *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.

check is altered or forged. One consumer in Los Angeles was unable to get his account recredited 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.[88] The consumer's bank kept insisting it would not recredit 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.[89] 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, 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."[90]

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.

[88] *See* Lazar, Kristine, "*On Your Side: Check fraud is on the rise- here's how to protect your* money," CBS News Story, KCAL News (Apr. 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/.
[89] Berry, Kate, "*Small banks urge crackdown on big banks with lax check-fraud controls*," American Banker (Feb. 9, 2023), available at https://www.americanbanker.com/news/small-banks-urge-crackdown-on-big-banks-with-lax-check-fraud-controls
[90] *Id.*

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.
- 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.

VI. 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,[91] and some states also use EBT cards to issue Temporary Assistance for Needy Families (TANF) or other state administered financial assistance.[92] EBT accounts perform the same function for low-income households as do 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;[93] 38% of whom were white, 25.5% Black, and 15% Hispanic.[94] As of 2022, nearly 2 million Americans receive Temporary Assistance for Needy Families ("TANF") benefits to support their families.[95] In FY

[91] https://www.fns.usda.gov/snap/ebt
[92] https://fns-prod.azureedge.us/sites/default/files/resource-files/ebt-contract-procurement-summary-20221215.pdf
[93] 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.
[94] 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).
[95] Office of Family Administration, Administration for Children and Families, "TANF Caseload Data 2022," August 2022, https://www.acf.hhs.gov/ofa/data/tanf-caseload-data-2022.

2021, 35% of TANF recipients were Hispanic, 29% were Black, and 27% were white.[96] These public benefit programs are focused entirely on low-income families.

During the past two 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,[97] and Congress recently provided for reimbursement of these stolen funds for the period of October 1, 2022, to September 30, 2024.[98]

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 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.

VII. Problems with the collection of accurate payment fraud data create an additional barrier in 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,[99] as well

[96] 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.
[97] https://www.fns.usda.gov/snap/snap-tanf-ebt-card-skimming-prevention
[98] *See* the Consolidated Appropriations Act (CAA) of 2023, Title IV, Section 501.
[99] 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 actors may not be subject to any supervision, though they are still required to comply with all laws.

as the extent to which the activities[100] undertaken by an institution are covered by existing law. As a result, no centralized federal agency receives or collects all data about payment fraud.[101] 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. [102]

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.[103] Even with SARs mandatory reporting, the 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.[104]

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.[105] 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

---

[100] Though not covered by this testimony, institutions engaged in payments through cryptocurrency and/or stablecoin face the possibility of oversight by the prudential regulators as well as Commodities Futures Trading Commission, the Securities and Exchange Commission, and/or the Consumer Financial Protection Bureau.

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

[102] 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.

[103] "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 Important of Timely and Effective Suspicious Activity Reports"* Supervisory Insights (Updated Jul. 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.

[104] *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).

[105] *See* Operating Circular 8: Funds Transfers through the FedNow Service (Sept. 21, 2022) available at https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/operating-circular-8.pdf.

shared widely among users.[106] Even initiatives such as SardineX[107] and Beacon[108] 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.[109]

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 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.

Indeed, NCLC provided many of the recommendations that follow in comments to the FTC Collaboration Act of 2021.[110] 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.

---

[106] *See Faster Payments Fraud Trends and Mitigation Opportunities*, Faster Payments Council, Fraud Work Group Bulletin.01 at 5 (Jan 2024), available at https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

[107] *Join sardineX*, Sardine, available at https://go.sardine.ai/sardinex. SardineX is intended as a real-time fraud detection network made up of a consortium of financial institutions and fintech organizations, including banks, card networks, payment processors, and fintechs, which will include a shared database where participants can access fraud data on entities transacting across the network.

[108] 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.

[109] 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, 2023, at 28, 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.

[110] *See* NCLC *et al.*, Comments regarding the FTC Collaboration Act of 2021, (Aug. 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.

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.

We also support the provision in Title I of the Senate Appropriation Committee's Financial Services and General Government bill on financial fraud, which directs the Treasury Department to "facilitate a public-private partnership to enhance Americans' financial security and prevent the proliferation of financial fraud and scam schemes… (including) the relevant Federal and State financial regulators, consumer protection agencies, law enforcement, financial institutions, trade associations, consumer and privacy advocates, and other stakeholders."[111] That partnership would "encourage information sharing among participants, develop best practices for relevant stakeholders, including the larger public, develop educational materials to enhance awareness of financial fraud schemes across sectors, share leading practices and tools, and encourage innovations in counter-fraud technologies, data-analytics, and approaches."[112]

2. 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.

But 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

[111] 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.
[112] *Id.*

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.

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.

VIII. The use of AI and automated tools to combat payment fraud is important, but consumers need clear rights when innocent consumers are negatively impacted.

A. Overaggressive algorithms can shut out innocent consumers from access to their accounts and funds.

Most parties who engage in payments, (financial institutions, payment processors, card networks, money service businesses, and fintechs) utilize tools to combat payment fraud, including AI and machine learning technologies. Financial institutions who hold consumer deposits may also utilize these same kinds of technologies to comply with their BSA/AML obligations. 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.

Sometimes the appropriate response by a company who suspects its customer is engaging in fraudulent 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. However, no law requires the company 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 responses to potential fraud a company may need to undertake under BSA/AML law is to file a Suspicious Activity Report (SAR) if the transaction is large enough to meet the threshold reporting requirements and update their customer risk profile.[113]

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."[114] As a result, even the filing of a SAR alone should not automatically trigger an account closure.

---

[113] 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/.

[114] Bank Policy Institute "*The Truth About Suspicious Activity Reports*," (Sept. 22, 2020) available at https://bpi.com/the-truth-about-suspicious-activity-reports/ and citing to, "*Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance*," Bank Policy Institute (Oct. 29, 2018) available at https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf.

But financial institutions have broad discretion in how they respond to perceived risk threats and have sometimes overreacted to fraud waves, catching innocent consumers in the process. Often, the most vulnerable people have been denied access to their money.

After Chime embarked on a marketing campaign to convince people to open Chime accounts to receive their stimulus payments, its inadequate identity verification led to a wave of fraud. Chime then froze numerous accounts, leaving some people without their money for months on end:

- "Chime stole my entire unemployment backpay…. I'm a single mom of 4 kids and they stolen $1400 from me and refuse to give it back and now we are about to be evicted."[115]

Similarly, Bank of America froze 350,000 unemployment debit cards in California after extensive fraud reports. But the freezes caught many legitimately unemployed workers, and the bank failed to respond in a timely fashion to their complaints:

- "Heather Hauri got a text from Bank of America that suggested her debit card may have been compromised too. When she responded that she had not made the transactions in question, she was locked out of her account. 'The whole account is frozen,' she said. 'You can't get your own money.'"[116]

Months later, after a lawsuit was filed, a judge prohibited the bank from freezing accounts for California unemployment benefits based solely on an automated fraud filter and required it to do a better job of responding when jobless people say their benefits were stolen.[117]
The CFPB ultimately brought an enforcement action against Bank of America,[118] and also against U.S. Bank[119] for similar conduct in indiscriminately freezing accounts and leaving them frozen for long periods of time. This conduct harmed the most vulnerable consumers – those who had lost their jobs and were relying on unemployment benefits.

The amount of accountholders who have complained about checking and savings account closures to the CFPB more than doubled since 2017,[120] and in 2022 the CFPB ordered Wells

---

[115] 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.
[116] KCAL News, "*Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud*," (Oct. 29, 2020), available at https://www.cbsnews.com/losangeles/news/bank-of-america-freezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/.
[117] McGreevy, Patrick, "*Bank of America must provide more proof of fraud before freezing EDD accounts, court orders,*" Los Angeles Times (Jun. 1, 2021), available at https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california.
[118] CFPB, "*Federal Regulators Fine Bank of America $225 Million Over Botched Disbursement of State Unemployment Benefits at Height of Pandemic*," (Press Release) (July 14, 2022), available at https://www.consumerfinance.gov/about-us/newsroom/federal-regulators-fine-bank-of-america-225-million-over-botched-disbursement-of-state-unemployment-benefits-at-height-of-pandemic/.
[119] CFPB, "*CFPB Orders U.S. Bank to Pay $21 Million for Illegal Conduct During COVID-19 Pandemic*," (Press Release) (Dec. 19, 2023), available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-us-bank-to-pay-21-million-for-illegal-conduct-during-covid-19-pandemic/#:~:text=The%20CFPB%20and%20OCC%20together,411%2DCFPB%20(2372).
[120] CFPB Consumer Complaint Database trends data for complaints received due to checking or savings account

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."[121]

There have been other 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.

Following are a few examples from a New York Times article detailing the responses consumers received after discovering their accounts were either frozen or closed and the attempts to communicate with their financial institutions about it: [122]

- Naafeh Dhillon, 28 from Brooklyn, NY, learned his account had been closed after his debit card and credit card were declined. He was later told by a Chase representative that the "bank's global security and investigation team had ultimately made the decision. Would the representative transfer him to that department? Nope… Since he wasn't given a specific reason for the closure, he couldn't disprove whatever raised suspicions in the first place."

- Todd Zolecki, 47 of Media, PA, did not have his account closed, but they did lock him out of access to his account. "They said your account has been suspended for further review," Why? "We can't tell you that. The only thing we can tell you is it can take up to 60 days for this review."

When people cannot access money they need based on red flags triggered by automated fraud tracking systems alone, that problem is compounded when a consumer's complaint is not followed up with any reasonable investigation by the financial institution involving any discussion with the accountholder or any clear timeline to unfreeze their money.

The EFTA has clear error resolution timelines and procedures, and those should be used when consumers cannot access their funds. If 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. But financial institutions and payment apps seem to believe the EFTA does not apply in this

---

closure available at 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.

[121] *In the Matter of Wells Fargo Bank, N.A.*, CFPB No. 2022-CFPB-0011 (Dec. 20, 2022) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

[122] Barnard, Tara Siegel and Lieber, Ron, "*Banks Are Closing Customer Accounts, With Little Explanation*," New York Times (Apr. 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.

situation.

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

We support legislative efforts to address the many gaps and ambiguities in the Electronic Fund Transfer Act that leave consumers unprotected. The EFTA can be amended to address the specific problem of improper freezes and account closures by 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. When a consumer contacts their financial institution complaining about the inability to access funds or an account closure, the institution would have to perform a reasonable investigation and provide a resolution to the consumer within 10 days or provide a provisional, unfrozen, credit pending a longer investigation. After a reasonable investigation, the consumer's financial institution would have to release the frozen funds or reopen a closed account if it was done in error—except in cases where the consumer obtained the funds through unlawful or fraudulent means or was denied access due to a court order or as directed by law enforcement.

The EFTA's error resolution procedures allow financial institutions to continue using automated fraud detection systems while ensuring that consumers have 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.

The problem with account closures and freezes could also be addressed by rulemaking or guidance from the CFPB.

FinCEN and bank regulators should also provide guidance to financial institutions about what information they may and should provide to accountholders regarding freezes and account closures while still complying with the BSA. For example, they could clarify in a FAQ that, while financial institutions are not allowed to disclose that a SAR was filed, they are allowed to disclose that an account was frozen or closed due to suspicious activity and/or describe the specific activities that raised concerns.

As shown by the CFPB's recent enforcement actions and in light of risks of unfair, deceptive, or abusive practices when consumers' funds are held indefinitely, 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 and provide guidance as to the timeliness of returning an accountholder's funds after account closure.

IX. 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)