National Consumer Law Center
Fighting Together for Economic Justice

NATIONAL HEADQUARTERS
7 Winthrop Square, Boston, MA 02110
(617) 542-8010

WASHINGTON OFFICE
Spanogle Institute for Consumer Advocacy
1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
(202) 452-6252

NCLC.ORG

September 6, 2024

Ann Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW,
Washington, DC 20551

Re: Expansion of Fedwire Funds Service and National Settlement Service Operating Hours, Docket No. OP-1831, 88 Fed. Reg. 39613 (May 9, 2024)

Dear Ms. Misback,

The National Consumer Law Center, on behalf of its low-income clients, submits these comments on the Federal Reserve Board's (FRB's) proposal to expand the operation hours of the Fedwire Funds Service (Fedwire) and the National Settlement Service (NSS).

We support the proposed rule to expand the operating hours of the NSS but urge the Federal Reserve Board to take additional measures to address and prevent fraud occurring via Fedwire before expanding its operating hours.

1. Benefits of the expansion of the NSS

Every bank and credit union in the nation receives ACH payments. ACH payments are used by millions to pay their mortgages, rent, student loans, credit cards, and many other payments. But one big gap slows some ACH payments down by as much as three days. While the ACH Network currently processes payments 23¼ hours every business day (and some file processing occurs on weekends), ACH payments get held up when the Federal Reserve is closed (currently on weekends and holidays). This is a problem for many low-income consumers who live paycheck to paycheck and need fast access to their income and to paying bills without incurring late fees.

Expanding NSS operating hours means American workers could get paid on weekends and holidays, which is especially important for those who work shifts or gigs over weekends and holidays. They could receive Direct Deposits to their bank accounts sooner than the next banking day.

Receiving their pay over the weekend also means consumers would be able to make timely payments over the weekend. In addition to paying their credit cards or bills, they would be able

to transfer funds between their own accounts or send money to family and friends more quickly. These transfers could all be settled over weekends and holidays, resulting in faster use of those funds.

Because a faster payment option over the ACH network is not currently available, many American consumers have turned to other payment platforms that promise faster, and instantaneous payments. Seventy-six percent of households use Venmo or Cash App.[1] Zelle, a P2P platform owned and operated by Early Warning Services, LLC ("EWS"), has outpaced competitors like Cash App and Venmo to become the dominant P2P platform in the United States.[2] But these platforms have become fertile ground for fraudsters and organized crime, posing risks to consumers and law enforcement.

According to the FTC,[3] "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) for all of 2023, and the second largest category of payment method specified by fraud victims in terms of number of reports (after credit cards) for the first two quarters of 2024. [4] The Consumer Financial Protection Bureau (CFPB) has also seen high growth in complaints about fraud in P2P apps and digital wallets.[5]

P2P fraud has a particularly harsh impact on low-income families and communities of color. For example, a September 2022 Pew Research Center survey shows that 59% of Cash App users are Black and 37% are Hispanic.[6] Cash App has been subject to reports of widespread fraud,[7] failing to protect the very vulnerable populations it targets. Zelle also suffers from widespread fraud and

---

[1] 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/.

[2] Mason, Emily, "*Despite a Late Start, Bank-Owned Zelle Moves More Money than Venmo and Cash App Combined*," FORBES (Sept. 8, 2022), available at https://www.forbes.com/sites/emilymason/2022/09/08/despite-a-late-startbank-owned-zelle-moves-more-money-than-venmo-and-cash-app-combined.

[3] 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.

[4] FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods. For 2023, only 474,328 (18%) of 2,606,042 fraud reports received by the FTC specified the payment method. For the first two quarters of 2024, only 222,540 (21%) of 1,085,474 fraud reports received by the FTC specified the payment method.

[5] 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.

[6] 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/.

[7] 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").

scams, causing tremendous consumer harm.[8] The existing P2P payment systems of large technology companies and financial institutions simply are not safe for consumers to use.[9]

Expanding the hours of the NSS to allow faster settlement over ACH will allow consumers to choose a payment option made through their bank and the ACH network which has proven to be safer than faster payments from a P2P payment system.

2. Risks of the expansion of the Fedwire Funds Service

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.[10] It 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. For the first two quarters of 2024, the dollar amount of fraud losses due to bank transfer or payment reported to the FTC was slightly under $1 billion,[11] whereas the dollar amount of fraud losses due to cryptocurrency was $678.8 million. For all of 2023, the dollar amount of fraud losses due to bank transfer or payment was slightly under $2 billion, and the dollar amount of fraud losses due to cryptocurrency was a little under $1.5 billion. Some losses through cryptocurrencies may start as bank-to-bank wire transfers to crypto banks or exchanges.[12] 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.[13]

---

[8] *See* United States Senate, Permanent Subcommittee on Investigations, Majority Staff Report, "*A FAST AND EASY WAY TO LOSE MONEY: Insufficient Consumer Protection on the Zelle Network*" (Jul. 23, 2024), available at https://www.hsgac.senate.gov/wp-content/uploads/2024.7.23-PSI-Majority-Staff-Report-on-Zelle.pdf (detailing the prevalence of fraud and scams over Zelle and the high rates at which consumers fail to be reimbursed for even unauthorized transactions).

[9] *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), available at https://bit.ly/CFPB-BTPS-comment ("CFPB Big Tech Payment Platform Comments"); Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750, RIN 7100-AG16 (Sept. 9, 2021), available at https://bit.ly/FedNowCoalitionComments (FedNow Comments). *See also* Rocha, Polo, "*P2P payments surged during pandemic. So did the complaints about them.*", AMERICAN BANKER (Jun. 22, 2021), available at https://www.americanbanker.com/news/p2p-payments-surged-during-pandemic-so-did-the-complaints-about-them.

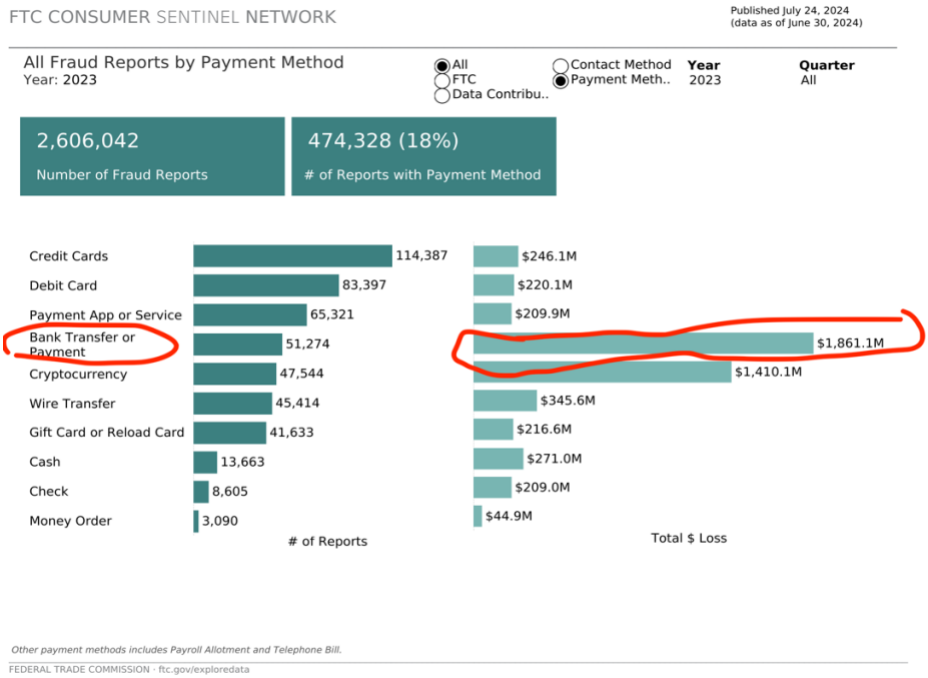
[10] FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[11] Specifically, $996.2 million. FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[12] *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.

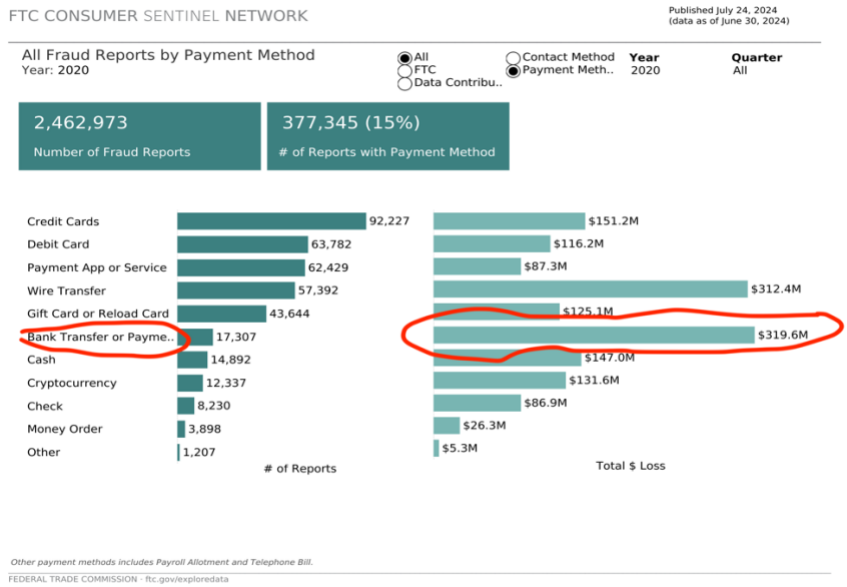
[13] Iacurci, Greg, "*How this 77-year old widow lost $661,000 in a common tech scam: 'I realized I had been defrauded of everything'*," CNBC (Oct. 8, 2023) available at https://www.cnbc.com/2023/10/08/how-one-retired-woman-lost-her-life-savings-in-a-common-elder-fraud-scheme.html.

2023 Fraud Reports to FTC by Payment Method



Compared to 2020, it is especially dramatic to note how the bank transfer category has grown astronomically – nearly sixfold in three years.[14]

2020 Fraud Reports to FTC by Payment Method



[14] The dollar losses in these two charts significantly understate actual losses, as only 15% (2020) to 18% (2023) of reports included information on payment method, and many fraud losses are not reported to the FTC.

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.[15] 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. The bank refused to return the money.[16]

- 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.[17] He is a cancer patient and navigating the bank appeal process has been extremely stressful. These SIM swaps are increasingly common.[18]

- 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.[19]

- A man lost $15,000 that was wired to another account by someone who gained access to his account. The bank spotted suspicious activity as the fraud was taking place and called the man, who alerted them to the fraud, but the bank still refused to return the money claiming that the EFTA did not apply to these fraudulent electronic transactions.

- A fraudster hacked a retiree's online banking account and made a cash advance from the retiree's credit card to the retiree's linked bank account. The fraudster then immediately wired that amount from the retiree's bank account to his own. The bank denied any relief.[20]

- 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.[21]

[15] Inquiry received by ABC News producer, Kaitlyn Morris.
[16] Inquiry received by KPRC (Houston NBC station) reporter Amy Davis.
[17] Email from attorney on file with NCLC.
[18] *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.
[19] Email from CAMBDA Legal Services to NCLC, on file with NCLC.
[20] Pending arbitration before AAA (Wells Fargo).
[21] Lawrence and Louis Company d/b/a Hidden Oasis Salon v. Truist Bank, No. 1:22-cv-200-RDA-JFA (E.D. Va.).

Large news outlets like Good Morning America and CBS Mornings have run stories about the perils and lack of protection available to consumers impacted by wire fraud.[22]

All the examples provided above involved unauthorized wire transfers. However, consumers have also been 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.[23]
    - Kelli Hinton, 7 months pregnant at the time, received a text about a fraudulent wire transfer from her account, then a follow-up call from a fraudster posing as a Chase fraud agent, spoofing Chase's real phone number. The fraudster kept her on the line for an hour and convinced her to change her username and password, allowing him to drain $15,000 from her account.[24]
    - 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.[25]

---

[22] 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; CBS Mornings, "*New efforts to stop wire transfer scams*" (Apr. 18, 2024), available at https://www.cbs.com/shows/video/yjF_XAcxwks9vCj5pnXq84pNEJf2nY8Z/.

[23] 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.

[24] 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.

[25] 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.

- 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.[26]

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."[27]

We have heard similar stories from other consumers who were impacted by fraud schemes and the inability of bank staff to help cancel or stop a bank-to-bank wire transfer even minutes after an order was submitted online.

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

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

Previously, wire transfers had to be conducted by walking into a bank for an in-person transaction that was slower and safer. 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

---

[26] 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/.

[27] 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.

fraudulently induced transfers to steal and send large sums of money, often not possible through P2P apps that set daily transaction limits. The absence of friction that was found in in-person transactions has undoubtedly contributed to the explosion of bank-to-bank wire transfer losses.

C. Banks take the position that all 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."[28] Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using Fedwire, SWIFT, CHIPS, and Telex.[29] In a recent amicus brief, the CFPB asserted that parts of a wire transfer can be considered an EFT covered by the EFTA,[30] namely the portions of the transaction that are conducted electronically through an online browser or mobile banking app when a consumer or fraudster initiates the transaction. However, the court has not ruled on that issue to date and banks take the position that even consumer bank-to-bank wire transfers are governed by UCC Article 4A. Thus, even if a criminal impersonates the consumer and makes a completely unauthorized wire transfer, banks will not provide consumers with the strong unauthorized use protections available under the EFTA.

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 the state's version of Uniform Commercial Code Article 4A (UCC Article 4A). The UCC was not designed as a consumer protection statute and was instead designed to govern commercial-to-commercial transactions. UCC Article 4A offers very weak or no protection for consumers who have suffered harm due to bank-to-bank wire transfer fraud. In essence, the consumer is deemed to have authorized a wire transfer if the bank utilized a commercially reasonable security procedure that the bank and the consumer agreed to beforehand and if the bank acted in good faith. Yet consumers have no understanding of or control over those security procedures and no choice but to click "I agree" to the fine print of an agreement.

For example, in the case in which the CFPB filed its amicus brief, the New York Attorney

---

[28] 15 U.S.C. §1693a(7)(B).

[29] 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.").

[30] *See* https://www.consumerfinance.gov/compliance/amicus/briefs/new-york-v-citibank-na/. Statement of interest available at https://files.consumerfinance.gov/f/documents/cfpb_ny-v-citibank-amicus-brief_2024-05.pdf.

General alleged Citibank failed to protect and reimburse victims of electronic fraud when it used "poor security and anti-fraud protocols," which consumers had not negotiated with Citibank.[31] According to the lawsuit, Citibank connected wire transfer services to consumers' online and mobile banking apps— 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.[32] 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.

We 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 often lack 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 give a consumer any remedies other than reimbursement of the unauthorized wire amount (possibly with interest), 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, financial institutions can reject a consumer's unauthorized wire transfer claim with little fear that the consumer will have the resources to fight the decision. And, for fraudulently induced wire transfers, the UCC provides no remedy.

For all these reasons, the Federal Reserve Board must do more to protect consumers from payment fraud that occurs via Fedwire.

3. Implementation considerations for the expansion of Fedwire and potential remedies to address bank-to-bank wire fraud.

We appreciate the Board's statement that it is "committed to promoting the development and implementation of industry-wide measures to help financial institutions detect and prevent fraud."[33] Adopting measures to prevent and remedy fraud and errors will not only protect consumers and other users of Fedwire but will also be crucial in protecting the integrity of and confidence in the system.

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

---

[31] 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.

[32] *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 electronic fund transfers covered by the EFTA because they are electronic instructions that do not come from the actual consumers who are Citi account holders.

[33] FRB, Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, 87 Fed Reg 34350, 34352-53 (June 6, 2022).

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

The Federal Reserve Board (FRB) has an opportunity to impose requirements on users of Fedwire and to develop tools to assist financial institutions in keeping the system safe to prevent, detect, and respond to fraud and errors. Beyond Regulation J, we encourage Reserve Banks to issue operating circulars and other materials to guide financial institutions. We offer some suggestions below on how the Reserve Banks and the FRB can build protections into Fedwire operations and impose requirements on Fedwire users to help detect fraud, prevent it from spreading, and recover money sent due to fraud or error when possible.

A. The Federal Reserve Board should develop a system to receive mandatory reporting of fraudulent and fraudulently induced Fedwire payments, regardless of whether the amount transferred meets the SARS threshold.

To address the widespread problem of bank-to-bank wire transfer fraud, solid, up-to-date information is essential. Without information about the extent and types of fraud committed through bank-to-bank wire transfers, law enforcement, banks, and regulators will not be able to identify trends, the fraudsters' methods, or develop avenues to stop the fraud.

Other payment operators like FedNow, RTP®, and Zelle collect reports of fraud. Yet there is no systematic collection of information about fraudulent bank-to-bank wire transfers. Specifically, we understand that the FRB does not receive fraud reports from institutions utilizing Fedwire, and we do not know what fraud information, if any, is collected on other wire transfer services, such as The Clearing House's CHIPS system. It also appears that there is no ongoing collection of information about the accounts into which fraudulent funds are sent.

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

Financial institutions utilizing Fedwire should be required to report all complaints of fraud and scams asserted by consumers and businesses to a centralized database, even if a Suspicious Activities Report (SAR) is not required. Participants in Fedwire, not just regulators, need access to fraud information, and fraud suspicions should be reported and collected even if they do not reach the $5,000 threshold for mandatory SARs.

The FRB should develop a central database that permits the participants in the payment chain to share information to combat fraud, similar to the database developed for FedNow, and the Fedwire operating circular should require that all entities in the payment chain participate in that database. A scammer who has defrauded one consumer is likely to have defrauded others and to

continue to do so until stopped. However, patterns that reveal fraud cannot be detected if information is not reported and collected. Similarly, if one bank closes an account but the scammer just creates a new account, fraud will continue. A centralized fraud reporting system/database will ensure that all financial institutions participating in Fedwire have access to information about accounts suspected of fraud or scam, just like many current participants in Zelle have when accessing Early Warning Systems information.

Another reason for creating a fraud database is to ensure that participants have access to information about individuals or entities and can take measures to bar these participants from using the Fedwire system because of fraudulent activity. NACHA, for example, has a terminated originator list that serves a similar function.

Finally, as discussed in more detail below, receiving banks should be required to send a request to a beneficiary bank that a consumer alleges received fraudulently induced funds to return the fraudulently induced payments. If the receiving bank's response to a consumer who complains about a fraudulent payment is simply, "Too bad; you sent it; we warned you it was final," then the information about the fraud may never make it to the beneficiary's bank or a fraud database. It is essential to collect and share as much information as possible about fraudulent actors to keep the system safe.

B. Banks should make it easy for customers to report fraud and should be required to respond to suspected fraud in specific ways.

In our suggestions below, we mirror Regulation J's terminology and refer to the "receiving bank" as the bank that receives a sender's order to send money and then sends that money to the beneficiary's bank. The sender is also referred to as the originator, customer, or consumer. The "beneficiary" is the individual or entity to be paid and is a customer of the "beneficiary bank."

i. Actions that receiving banks should be required to take.

a. The receiving bank should be required to have an easy and accessible way for consumers to report payments sent in error or due to fraud.

Financial institutions need to have a mechanism to receive reports of problems and to assist senders in resolving them wherever possible.[34] Despite the completion of a payment, it may be possible to recover the fraudulently transferred funds in some instances. In addition, it is important to encourage reports of fraud to monitor problems, stop them from spreading, and develop solutions. None of that can happen if users are discouraged from making reports and that information is not collected.

[34] Business accounts are not governed by the EFTA, and financial institutions may incorrectly assume that a dispute is not covered by the EFTA. *See* https://www.consumerfinance.gov/compliance/amicus/briefs/new-york-v-citibank-na/. Statement of interest available at https://files.consumerfinance.gov/f/documents/cfpb_ny-v-citibank-amicus-brief_2024-05.pdf.

The Reserve Banks should require receiving banks to accept reports of fraud and make it easy for payment originators to make such reports. An operating circular should make it a condition of participation in Fedwire that each participant who interacts with a payment running over Fedwire accept reports of fraud in a prominent place on the participant's website, app, and any other user interface offered to payment originators. Receiving banks should also be required to forward information in these reports to the beneficiary bank alleged to have received fraudulent funds, as discussed below.

b. When a payment originator reports having been fraudulently induced into sending money, the receiving bank should initiate a request to return the funds.

When a customer reports a fraudulently induced fund transfer, the receiving bank should be required to ask the beneficiary's bank to return the money. The request should go through the database that the Federal Reserve Board develops to report fraud.

This should also be the case when a payment order contains a misdescription of a beneficiary. For example, many business email compromise schemes trap innocent consumers in sending money via bank-to-bank transfers to the wrong account number even though the name of the beneficiary is accurate. This happens in heartbreaking situations when a consumer is attempting to close on a home purchase and is expecting to send money to their agent or title company but is instructed by a fraudster posing as the agent to send it to another account.[35]

Though the receiving bank's request to return funds may be ineffective if the funds are already gone (for example, when the beneficiary has removed the funds and the account has been closed), that may not always be the case; sometimes the beneficiary's bank may have put a hold on the funds if fraud was suspected. Moreover, a request for a return of funds is an important way to alert the beneficiary's bank that its customer may be using an account unlawfully, which should lead to placing such a hold on further transactions and preventing the use of the account for future fraud. It would also trigger other actions discussed below. As a result, the Reserve Banks should require receiving banks to make an immediate request to return funds on behalf of a consumer when fraud in the inducement has been reported.

ii. Actions that beneficiary banks should be required to take.

When a beneficiary's bank receives credible information that its customer has received a fraudulently induced payment, the Reserve Banks should require the beneficiary bank to investigate, cooperate in any investigation by the receiving bank or other parties, and, where the circumstances warrant, delay acceptance of the payment order or put a hold on any funds.

---

[35] District of Columbia Department of Insurance, Securities and Banking, "*Beware of Real Estate Wire Transfer Scams*," (last accessed Sept. 3, 2024), available at https://disb.dc.gov/page/beware-real-estate-wire-transfer-scams; Araj, Victoria, "*How To Beware Of Mortgage Wire Fraud During Closing*," Rocket Mortgage, (Jan. 25, 2024), available at https://www.rocketmortgage.com/learn/mortgage-wire-fraud; Egan, John, "*How to Avoid Mortgage Wire Fraud*," Experian (Mar.8, 2024), available at https://www.experian.com/blogs/ask-experian/how-to-avoid-mortgage-wire fraud/#:~:text=Mortgage%20wire%20fraud%20typically%20happens,to%20get%20the%20money%20back.

Millions of consumers and small businesses are hurt by scammers who fraudulently induce them to send payments to beneficiaries who are not entitled to those payments. The beneficiary could be the actual scammer; could have used a stolen or synthetic identity to open the account used to receive the payment; or could be a money mule (witting or unwitting) that sends the money on to the ultimate scammer.

Regardless of which of these categories the beneficiary falls into, the beneficiary's bank has responsibilities under know-your-customer and anti-money laundering laws to ensure that accounts are not opened with fraudulent identities and that accounts are not being used for illegal purposes.[36] Under the Bank Secrecy Act, banks are required to verify customer identities using prescribed procedures at the time of account opening.[37] Banks must also have a program with appropriate risk-based procedures for conducting ongoing customer due diligence (including understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile), conducting ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, maintaining and updating customer information.[38] Banks are also required to have red flag programs to detect ID theft under the Fair Credit Reporting Act (FCRA).[39]

Financial institutions that ignore their Bank Secrecy Act, know-your-customer, and due diligence obligations could face regulatory or enforcement actions. Those who overlook warning signs of fraud may also face other legal repercussions if they are found complicit in helping scammers.[40]

As a result, when a beneficiary bank receives information that its customer has, or may have, received a Fedwire payment for one of its account holders through fraud, the beneficiary bank should be required to investigate any allegation of fraud.

The beneficiary bank will likely receive notice of the alleged fraud from the defrauded consumer's bank (the receiving bank) instead of from the consumer directly. In addition to conducting its own investigation, the beneficiary's bank should be required to cooperate in any investigation by the receiving bank.

Pending the outcome of the investigation, when there are significant signs that the account may have been opened under a false or stolen identity or that the beneficiary is complicit in fraud, the Reserve Banks should encourage the beneficiary's bank to delay acceptance. More specifically, the Reserve Banks should utilize operating circulars to instruct beneficiary banks to delay acceptance of payment orders (and not make the funds immediately available to the beneficiary) if the bank has reasonable cause to believe that the beneficiary is not entitled or permitted to receive the payment. An operating circular could elaborate on this option and encourage banks to

---

[36] See, e.g., Fed. Fin. Inst. Examinations Council (FFEIC), Bank Secrecy Act/Anti-Money Laundering Examination Manual, 56–59 (2014), available at www.occ.treas.gov
[37] 31 U.S.C. § 5318; 31 C.F.R. § 1020.220.
[38] *See* 31 CFR 1020.210(a)(2)(v).
[39] 16 C.F.R. § 681.1(d). *See also* 17 C.F.R. § 162.30(d)(1) (CFTC); 17 C.F.R. § 248.201(d)(1) (SEC).
[40] *See, e.g.,* Evans v. ZB, N.A. dba California Bank & Trust, 779 Fed. Appx. 443 (9th Cir. 2019) (plaintiffs stated claims for aiding and abetting fraud, aiding and abetting breach of fiduciary duty, and conspiracy to commit fraud); Reyes v. Zion First Nat'l Bank, 2012 WL 947139 (E.D. Pa. Mar. 21, 2012); OCC Consent Order for a Civil Penalty, In re Wachovia Bank, 2008-027 (Apr. 24, 2008).

exercise it to investigate a fraud report based on a claim of fraudulent inducement. Where circumstances warrant, the beneficiary's bank should consider freezing the account. Moreover, even where the payment order is accepted and funds have been made available, if there has been a report of fraudulent inducement, the bank should still investigate to assess whether its customer is engaged in unlawful activity and the account should be closed.

C. The Federal Reserve should assist both receiving and beneficiary banks in identifying red flags of fraudulent transactions.

The Federal Reserve should issue operating circulars strongly encouraging receiving banks to identify red flags of potentially fraudulent transactions and warn payment originators before payments are sent. As discussed above, beneficiary banks already have a responsibility to monitor accounts to ensure they are not used for unlawful purposes, and the beneficiary's bank should delay acceptance of payment orders and possibly close accounts in some circumstances.

To assist both efforts, the Federal Reserve Board should use the fraud reports it receives to help banks identify red flags of fraud. For example, FinCEN has recently identified red flags of financial elder exploitation, some of which are more broadly relevant to identifying fraudulent transactions on either the sending or receiving end.[41] The FRB should identify red flags that are specific to Fedwire payments.

The red flags should focus not only on suspicious Fedwire transactions but also signs that an account may be one opened for fraudulent purposes. For example, new accounts opened online that then begin receiving wire transfers or other unusual payments, or that quickly disperse funds received, might warrant attention.

Additionally, the FRB should publish anonymized data regarding the number of cases and types of suspected fraud and/or scams that have been reported by banks participating in Fedwire. This will help inform regulators, policymakers, industry, and consumer groups about trends and challenges unique to bank-to-bank transfers.

4. Conclusion

The expansion of the NSS will be a boon to both consumers and businesses, providing a safer alternative to other faster payment platforms like Venmo, PayPal, the Cash App, or Zelle.

However, consumers may be harmed by the expansion of Fedwire operating hours because of the high prevalence of fraud and the lack of strong consumer protections for bank-to-bank wire transfers. If the Federal Reserve Board decides to expand the operating hours for Fedwire, we urge it to also take measures to prevent and address fraud.

Thank you for the opportunity to submit these comments. For questions, please contact Carla Sanchez-Adams at csanchezadams@nclc.org.

---

[41] *See* FinCEN Advisory, FIN-2022-A002, Advisory on Elder Financial Exploitation (June 15, 2022), https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf.

Respectfully submitted,

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