Testimony of Carla Sanchez-Adams
Senior Attorney, National Consumer Law Center
In Support of HB 1156 / SB 930
The Elder Fraud Prevention Act of 2024
Before the Economic Matters Committee
Maryland House of Delegates

February 23, 2024

Chairman Wilson, Vice Chair Crosby, and Members of the Economic Matters Committee:

I am Carla Sanchez-Adams, a Senior Attorney at the National Consumer Law Center, and am pleased to submit this testimony in support of HB 1156 / SB 930.

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, which covers the laws governing bank accounts and payment systems, including the laws that protect, or do not protect, consumers when they are defrauded. 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, including Maryland. It is from this vantage point that I supply this testimony.

Payment fraud impacts all Americans across many communities, but the impacts of fraud are most keenly felt by certain vulnerable populations such as older Americans, low-income

consumers, and communities of color. Additionally, Maryland ranks fifth in the nation for 2023 fraud reports per capita.[1]

One of the primary ways used by criminals to steal tens and even hundreds of thousands of dollars from people is through bank-to-bank wire transfer systems. Yet the consumer protection laws that govern bank wire transfers are woefully inadequate.

We are pleased to support HB 1156/SB 930 because it would close two critical gaps in consumer protection laws. First, the bill would require a bank to follow the same rules under the Electronic Fund Transfer Act that apply to other forms of electronic payments when a consumer disputes an unauthorized wire transfer taken out of their account. Second, the bill would protect consumers who are defrauded by a criminal into sending money through wire transfers.

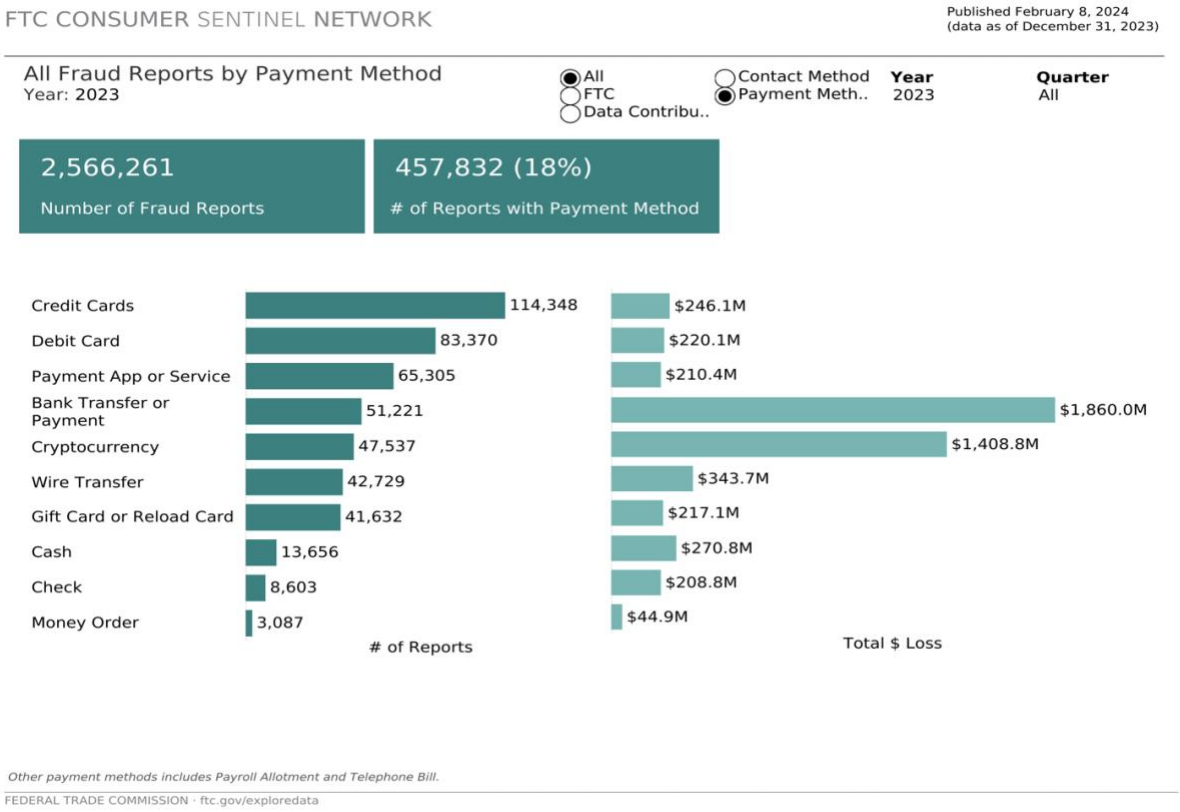
I. Consumers are devastated by bank-to-bank wire transfer fraud.

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.[2] 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, which allows a maximum transfer of $5,000 or less, depending on the bank. (The FTC's "Wire Transfer" category includes only nonbank transfers like Western Union and MoneyGram.)

[1] *See* FTC fraud reports state by state available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods. *See also* Wilson, Katharine, "Experts urge senators to act in the fight against financial fraud; Data show Maryland was fifth in nation for 2023 fraud reports per capita," Capital News Service (Feb. 2, 2024).

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

2023 Fraud Reports to FTC by Payment Method



Cryptocurrency is a close second to bank transfer in total dollar amount of fraud losses reported to the FTC, but some losses through cryptocurrencies may start as bank-to-bank wire transfers to crypto banks or exchanges.[3] 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.[4]

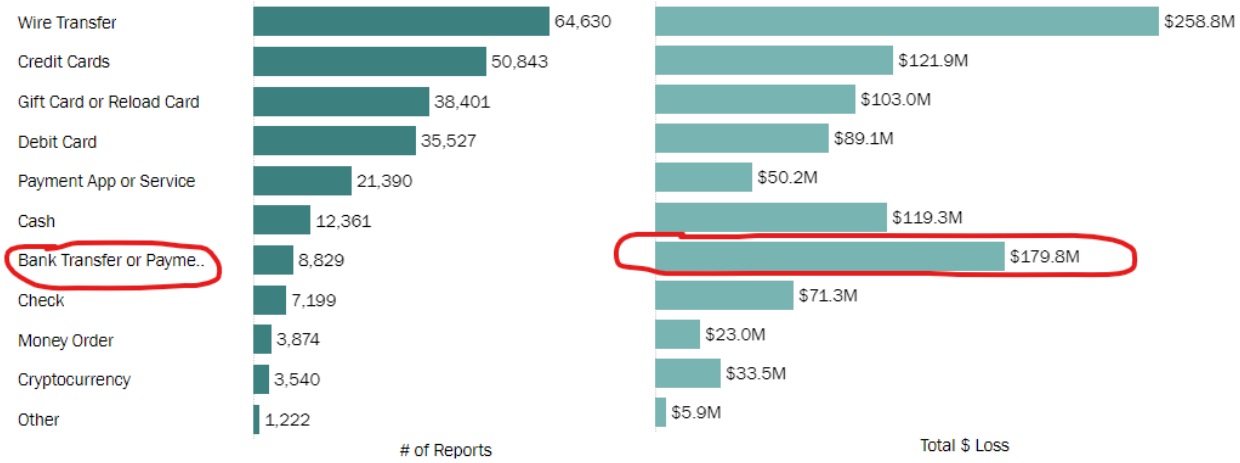
Compared to 2019, it is especially dramatic to note how the bank transfer category has overtaken nonbank wire transfers, and how astronomically it has grown – over tenfold in four years.[5]

[3] *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.

[4] 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.

[5] Compare a total of $179.8 million reported as lost to bank transfer or payment in 2019 with $1,860.0 million reported as lost in 2023. The dollar losses in these two charts significantly understate actual losses, as only 12% (2019) to 18% (2023) of reports included information on payment method, and many fraud losses are not reported to the FTC.

2019 Fraud Reports to FTC by Payment Method



Over the last several years, NCLC has received numerous inquiries on behalf of consumers and heard devastating reports about how criminals have used bank-to-bank wire transfers to take 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.[6]

- 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.[7] He is a cancer patient and navigating the bank appeal process has been extremely stressful. These SIM swaps are increasingly common.[8]

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

- A fraudster hacked a retiree's online banking account and made a cash advance from the retiree's credit card to his linked bank account. The fraudster then immediately wired that amount from the retiree's bank account to his own. The bank denied any relief.[9]

---

[6] Inquiry received by KPRC (Houston NBC station) reporter Amy Davis.
[7] Email from attorney on file with NCLC.
[8] *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.
[9] Pending arbitration before AAA (Wells Fargo).

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.[10]

All the examples provided above were for unauthorized wire transfers that the consumer did not initiate. 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.[11]
    - 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.[12]
    - 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.[13]

---

[10] 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.

[11] 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.

[12] 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.

[13] 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-

- 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.[14]

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."[15]

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

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

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

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

---

spoofing-phone-number/45866051.

[14] 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/.

[15] 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.

transactions has undoubtedly contributed to the explosion of bank-to-bank wire transfer losses.

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

The Electronic Fund Transfer Act (EFTA) is the primary federal law that protects our bank accounts and payments. It provides a right to protection against unauthorized electronic fund transfers and errors and provides specific procedures that banks must follow when a consumer disputes a transfer as unauthorized or another error.

But the EFTA does not cover 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."[16] Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using FedWire, SWIFT, CHIPS, and Telex.[17] Thus, even if a criminal impersonates the consumer and makes a completely unauthorized wire transfer, the consumer may have no protection under Regulation E.[18]

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 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.[19] According to the

[16] 15 U.S.C. §1693a(7)(B).
[17] 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.").
[18] However, as discussed in FN 77 below, some bank wire transfers may be within the EFTA's protection.
[19] New York State Attorney General, Press Release, Attorney General James Sues Citibank for Failing to Protect

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.[20] 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.

IV. Maryland consumers need remedies to address bank-to-bank wire fraud.

We support legislative efforts to address gaps that leave consumers who have been victimized by unauthorized and fraudulently induced wire transfers unprotected. As a result, we support HB 1156 / SB 930, which will extend the core EFTA protections to wire transfers and provide remedies for fraudulently induced wire transfers sent to criminals.

Thank you for the opportunity to provide this testimony. With any questions, please contact me at csanchezadams@nclc.org.

---

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.

[20] *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.