Request for Information on Potential Actions to Address Payments Fraud

Comments to the

Office of the Comptroller of the Currency (OCC)
Docket ID OCC-2025-0009

Board of Governors of the Federal Reserve System (Board)
Docket No. OP-1866

Federal Deposit Insurance Corporation (FDIC)
RIN 3064-ZA49

90 FR 26293 (June 20, 2025)

by the

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

Filed on September 15, 2025

Introduction

The National Consumer Law Center ("NCLC"),[1] on behalf of our low-income clients, is pleased to respond to the Office of the Comptroller of the Currency's (OCC), the Board of Governors of the Federal Reserve System's (Board), and the Federal Deposit Insurance Corporation's (FDIC), (collectively "the Agencies") Request for Information on Potential Actions to Address Payments Fraud.[2]

NCLC has previously provided testimony before Congress[3] and to various regulatory agencies[4] on the need to address payment fraud. We reiterate our testimony and suggestions and incorporate them here.

Generally, the Agencies should work with other federal and state regulators to address fraud and protect innocent consumers who are harmed by aggressive fraud reporting. They should:

---

[1] 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 publishes a series of consumer law treatises, including *Consumer Banking and Payments Law* (7th ed. 2024), updated at library.nclc.org. These comments were written by Carla Sanchez-Adams, Lauren Saunders, and Patrick Cotty.

[2] The Notice of Proposed Rulemaking is available at https://www.federalregister.gov/documents/2025/06/20/2025-11280/request-for-information-on-potential-actions-to-address-payments-fraud and published at 90 FR 26293 (Jun. 20, 2025).

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

[4] *See* NCLC Comments regarding the Expansion of Fedwire Funds Service and National Settlement Operating Hours, (Sept. 6, 2024) available at https://www.nclc.org/wp-content/uploads/2024/11/2024.09.06_Comments_NSS-Comments.pdf; NCLC Comments regarding FinCEN's Rulemaking on Anti-Money Laundering and Countering the Financing of Terrorism Programs, (Sept. 3, 2024) available at https://www.nclc.org/wp-content/uploads/2024/09/2024.09.03_Comments_FinCEN-Dept-Treasury-on-AML-Rulemaking.pdf; NCLC *et al*., Comments regarding the FTC Collaboration Act of 2021, (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").

- Enforce and strengthen laws that require financial institutions and other companies to protect consumers from unauthorized and fraudulently induced charges. Giving payment systems responsibility for the fraud on their systems will encourage more efforts to prevent fraud;
- Devote more attention to the responsibilities of institutions that receive fraudulent payments, including stepping up enforcement of Bank Secrecy Act /Anti-Money Laundering obligations;
- Establish interagency collaboration to assist consumers with reporting fraud, collecting data on fraud, and establishing systems for sharing fraud data and findings;
- Provide guidance to financial institutions about the timelines and procedures for consumers to regain access to improperly frozen funds, including providing clarity about what information can and should be given to accountholders regarding account closures and freezes.
- Work with the Federal Communications Commission to address the role that telecommunications providers play in facilitating fraud.

<u>External Collaboration</u> (Response to Questions 1-4)

Increased collaboration among the Agencies, the Federal Communications Commission (FCC), and other stakeholders could help prevent payments fraud resulting from imposter scams. Imposter scams occur when a criminal fraudster pretends to be a government agency, financial institution, or legitimate business. The criminal then contacts a consumer to alert them to a fake and urgent problem and attempts to persuade them to transfer their money under these false pretenses.[5] Imposter scams are a rapidly intensifying problem that disproportionately impacts older adults. Indeed, "combined losses reported by older adults who lost more than $100,000 increased eight-fold, from $55 million in 2020 to $445 million in 2024."[6]

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

A reply to the text will precipitate a call from the (fake) fraud department. Victims say they thought the bank was helping them get their money back. Instead, money was transferred out of their account. This scam's median reported loss was $3,000. The FTC announced that in 2023 these scams accounted for $330 million in reported losses.[7]

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

[6] *Id.*

[7] https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam.

NCLC has previously urged the OCC to address imposter scams and the resulting payments fraud by encouraging or requiring banks to employ safe texting protocols, which allow consumers to easily differentiate between legitimate communications from their financial institutions and dangerous imposter scam texts.[8] Additional collaboration with the FCC to identify and promulgate measures to address the role of scam calls and texts in imposter scams will help to detect and prevent payments fraud.

Additionally, the OCC and the Board should consider collaboration with law enforcement agencies and state attorneys general and regulators to prosecute companies that facilitate and profit from imposter scams and other fraud. For example, the Social Security Administration's (SSA) Office of the Inspector General and the Department of Justice partnered with several law enforcement agencies, the FCC, and the Federal Trade Commission to bring enforcement actions against several communications providers that knowingly transmitted scam calls impersonating the SSA.[9] The OCC and the Board should consider similar partnerships to take action against companies that profit from bank imposter fraud.

<u>Consumer, Business, and Industry Education</u> (Response to Questions 5-8)

Although consumer and business education is important, it alone will not solve the problem of payment fraud. Criminal fraudsters have extraordinary creativity;[10] they are constantly developing ways to steal people's money by setting up increasingly sophisticated schemes to obtain access to accounts or to fraudulently induce consumers into payment transactions.[11]

---

[8] *See* NCLC's letter to the OCC available at: https://www.nclc.org/wp-content/uploads/2024/10/2024.03.29_Letter_OCC-and-Texts.pdf

[9] https://oig.ssa.gov/scam-alerts/2025-07-17-civil-action-to-prevent-social-security-scam-calls-from-reaching-consumers/

[10] *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.

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

SCAM OF THE WEEK:
This Fake App Takes the Cake

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

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

Consumers and businesses should also receive broader education about cybersecurity instead of just scams and fraud. Better education about internet safety, phishing, vishing, ransomware, and

---

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

business email compromise would also reduce the amount of account takeovers and fraud schemes that lead to monetary loss from payments fraud.

With respect to check fraud, we support consumer education about safer ways to make payments.[12] For example, as we described in our comments to the Treasury Department's Request for Information on Modernizing Payments,[13] the goal of reducing the number of paper checks sent by and to the federal government is a worthy one. We support outreach to identify the reasons that people use paper checks, to address those reasons, and to encourage people to send and receive money through safer electronic payments. However, we oppose simply ending all use of checks to and from the federal government on a given date, which will only harm consumers.

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

We also support consumer education about safer ways to pay by check, such as the use of permanent ink and taking mail directly to the post office. AARP has put out materials on that topic.[14] The Agencies and financial institutions can educate consumers on these methods – which will also serve the goal of making people aware of check washing and encourage the use of electronic payments.

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

Regulation and Supervision (Response to Questions 9-15)

The Agencies, in collaboration with other federal and state regulators, should utilize existing laws to more aggressively pursue bad actors who perpetrate payment fraud and/or allow these bad actors to flourish. Additionally, the Agencies and other federal and state regulators should

[12] *See, e.g.*, AARP, Should You Stop Using Paper Checks? (Aug. 14, 2023).
[13] NCLC, Comments to the Department of Treasury's Request for Information on Modernizing Payments (June 30, 2025).
[14] *See* AARP, 6 Ways You Can Thwart Check Washers (Mar. 2, 2023).

amend and update regulations to address any ambiguities in the law caused by emerging technologies.

1. The Bank Secrecy Act

Debanking criminals will help reduce the billions lost in fraud every year, and the Bank Secrecy Act can assist with identifying those criminals.

In an effort to stop money laundering and the flow of money to criminal activities in general, Congress passed a series of laws starting with the Bank Secrecy Act of 1970.[15] The Bank Secrecy Act (BSA) and its implementing regulations are not just about drug cartels and terrorism. They also help to stop an array of criminal activity, including fraud. Fraud profits can also fuel terrorism and other activities by international criminal syndicates. The BSA imposes requirements on financial institutions to have systems to verify the identity of their customers and their businesses, to monitor accounts to ensure they are not being used for illicit purposes, and to report suspicious activity. Vigorous BSA oversight can prevent bad actors from opening accounts or using them to receive funds taken from consumers in unauthorized transactions or through fraud schemes. A lax AML/CFT regime can facilitate criminal activity.

Regulators should take additional steps to address payment fraud under the BSA.

The BSA regime plays an important role in combating fraud, and the Agencies, along with Treasury and FinCEN should take additional steps to address payment fraud. First, the Agencies should urge FinCEN to update the Suspicious Activity Report (SAR) to capture information about accounts that receive fraudulent funds. Second, stricter requirements must be placed on non-bank entities that engage in payment and banking services.

The Agencies should urge FinCEN to update the Suspicious Activity Report (SAR) to capture information about accounts that receive fraudulent funds.

FinCEN can help in the fight against payment fraud by updating the suspicious activity report (SAR) to encompass information about the accounts used to receive ill-gotten funds. The current SAR form only accommodates accounts related to the reporting institution. In fraud cases where the destination account of the perpetrator is known, reporting institutions relegate the destination account to the narrative. This makes identification and aggregation of fraudulent activity more difficult for law enforcement.

When a consumer's financial institution files a SAR following an incident of payment fraud, if the payment was sent through a system that identifies the recipient (such as a wire transfer, ACH,

[15] *See* Fin. Crimes Enf't Network, History of Anti-Money Laundering Laws, *available at* www.fincen.gov.

or P2P system), the SAR should identify the recipient institution and account. Allowing accounts not domiciled at the reporting institution to be reported and designated appropriately would assist FinCEN and law enforcement in identifying, aggregating, and prioritizing fraud investigations to better protect consumers.

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

Stricter BSA requirements must be placed on non-bank entities that engage in payment and banking services.

Although the Consumer Financial Protection Bureau (CFPB) had finalized a rule to enable supervision of the larger nonbank providers of general-use digital payment applications, the rule was overturned by a Congressional Review Act resolution. As such, no federal agency currently supervises non-bank entities that engage in payment and banking services.[16] Therefore, more must be done by other regulators to ensure that these entities are complying with the BSA.

FinCEN should expand the Customer Identification Program (CIP) and customer due diligence (CDD) requirements for entities other than banks that engage in payment and banking services, such as person-to person (P2P) payment apps, payment processors, fintech companies offering banking as a service or offering bank-like services, and crypto-related entities, including crypto exchange platforms.

Person-to-person (P2P) payment apps have become increasingly popular among consumers. Seventy-six percent of households use Venmo or Cash App. In addition to P2P payment services, consumers are also increasingly adopting other forms of technology to make payments. These newer payment apps and technologies are increasingly accepted by retailers, demonstrate a rapid growth trajectory, are situated within platforms with other financial services, and are being structured to work with crypto.

These platforms have become fertile ground for fraudsters and organized crime, posing risks to consumers and law enforcement. According to the FTC, "payment app or service" is the second

[16] For more information about the risks of non-banks and bank-fintech partnerships without adequate supervision, *see* NCLC Comments to the OCC, FRB, and FDIC's Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses, (Oct. 30, 2024) available at https://www.nclc.org/wp-content/uploads/2024/10/2024.10.30_Comments_RFI-Bank-Fintech-Partnership-Deposits-NCLC.pdf.

largest category of payment method specified by fraud victims in terms of number of reports (after credit cards) for all of 2024, and the largest category of payment method specified by fraud victims in terms of number of reports for the first two quarters of 2025.[17] The CFPB has also seen high growth in complaints about fraud in P2P apps and digital wallets.

Without federal supervision, state attorneys general and other state regulators have stepped in to enforce federal law. For example, after Cash App was subject to reports of widespread fraud, the regulators of 48 states obtained a consent order against Block, the operator of Cash App. The consent order required Block to pay $80 million and "undertake corrective action for violations of the Bank Secrecy Act (BSA) and anti-money laundering (AML) laws that safeguard the financial system from illicit use."[18] Similarly, the CFPB ordered Block to pay $175 million and fix its failures after finding that Block failed to take timely, appropriate, and effective measures to prevent, detect, limit, and address fraud on the Cash App platform.[19]

Nonetheless, large multi-state enforcement actions are rare and very difficult, and the CFPB has retreated from most of its enforcement docket. Vigorous federal supervision and enforcement are critical when nonbank actors facilitate and fail to prevent fraud.

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

Crypto companies and platforms should also be subject to strict BSA requirements to prevent an escalation of fraud.

We do not address the safety and soundness issues posed when banks engage with the crypto industry, nor will we comment on whether particular crypto firms should or should not be allowed bank accounts.

---

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

[18] Conference of State Bank Supervisors, "*State Regulators Issue $80 Million Penalty to Block, Inc., Cash App for BSA/AML violations*," (Press Release) (Jan. 15, 2025), available at https://www.csbs.org/newsroom/state-regulators-issue-80-million-penalty-block-inc-cash-app-bsaaml-violations.

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

However, as Congress considers legislation to regulate the market for crypto-assets, it is essential that crypto companies and platforms be required to conduct full BSA compliance. Crypto-assets are one of the top vectors for fraud and other illegal activity, and the growth of the crypto industry will only result in more fraud if strict controls are not built in.

According to the FTC, "cryptocurrency" "is the second largest category of payment method reported by fraud victims in terms of number of dollars lost (after bank transfer or payment) for all of 2024 and the first two quarters of 2025.[20] Crypto platforms are not just prone to fraud by third parties; several crypto firms that suffered losses or became insolvent during the 2022 crash in the crypto markets engaged in practices many believe were unfair, abusive, or deceptive.[21]

Enforcement of BSA requirements is essential to prevent crypto-assets from being used to perpetrate criminal activity. Both federal[22] and state regulators[23] have appropriately brought enforcement actions against crypto players that had lax programs to conduct due diligence on their customers, monitor transactions, and report suspicious activities.

Vigilant BSA oversight of accounts involving crypto-assets is also important as crypto-assets make their way into the U.S. banking and payments system. Several large, well-capitalized crypto firms have made it clear that their business model is focused on making crypto and blockchain-based ledgers a mainstream payment method for American consumers. For example, at least one major payment provider has created a stablecoin expressly intended to facilitate

---

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

[21] Federal Trade Commission, "*FTC Reaches Settlement with Crypto Company Voyager Digital; Charges Former Executive with Falsely Claiming Consumers' Deposits Were Insured by FDIC*," (Oct. 12, 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-reaches-settlement-crypto-company-voyagerdigital-charges-former-executive-falsely-claiming. *See also* Comment Letter by NCRC, NCLC, *et. al.* to the OCC in Opposition to First National Digital Currency Bank Charter Application (Jul. 30, 2025) available at https://www.nclc.org/wp-content/uploads/2025/08/NCRC-et-al.-Comment-Letter-Opposing-Circle-NTB-Charter-Application-Carla-Sanchez-Adams.pdf (discussing history of enforcement actions and litigation against Circle).

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

[23] *See* "Stablecoin Issuer Paxos to Pay Fine to New York for Binance Gaps," Bloomberg Law (Aug. 7, 2025), available at https://news.bloomberglaw.com/crypto/stablecoin-issuer-paxos-to-pay-fine-to-new-york-for-binance-gaps ($48.5 million settlement for lapses in anti-money laundering adherence and other diligence failures in its partnership with Binance); N.Y. Dep't of Fin'l Svcs., Press Release, Superintendent Adrienne A. Harris Announces $100 Million Settlement with Coinbase, Inc. after DFS Investigation Finds Significant Failings in the Company's Compliance Program (Jan. 4, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041

consumers' purchase of household goods and services,[24] while another crypto "native" firm has created a platform where retail merchants are provided crypto wallets that can receive direct crypto payments from customers, without the need to convert crypto assets into fiat currency to settle the transaction.[25] Reports claim that the platform processes payments for thousands of merchants, for "on-chain" payments worth billions of dollars.[26] BSA/AML compliance is essential to ensure that "purchases" using crypto-assets are not used to enable criminals to receive stolen funds or conduct criminal activity.

Consumers also need protection when crypto-assets are used for payments,[27] as discussed below.

2. The Electronic Funds Transfer Act

Fraudulently induced transactions should be subject to the EFTA.

The Electronic Fund Transfer Act (EFTA) and its implementing Regulation E protect consumers when problems with electronic fund transfers (EFTs). The law provides consumers with remedies for EFTs when a payment is unauthorized, such as when a criminal defrauds a person into turning over account credentials and then the criminal initiates the payment to commit 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."[28]

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

[24] PayPal, "Built for stable payments. 1 USD: 1 PYUSD on PayPal," (accessed Sept. 11, 2025), available at https://www.paypal.com/us/webapps/mpp/digital-wallet/manage-money/crypto/pyusd.
[25] Coinbase, "A new standard for onchain payments," (accessed Sept. 11, 2025), available at https://www.coinbase.com/commerce.
[26] Akolkar, Bhushan, "*New Payments Protocol for Coinbase Commerce to Facilitate Instant Crypto Settlements*," CoinGape (blog), (Nov. 17, 2023), available at https://coingape.com/new-payments-protocol-for-coinbasecommerce-to-facilitate-instant-crypto-settlements/.
[27] Any consumer payments made using crypto-assets should come with the full protections given to accounts under the Electronic Fund Transfer Act.
[28] 12 C.F.R. § 1005.2(m) (emphasis added).

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 criminal fraudster any more entitled to the money. Nor does it make the criminal fraudster's bank any less responsible for banking a criminal, or eliminate the role that the consumer's bank can play in preventing the transaction.

The response to payments fraud becomes even more problematic when it involves claims of 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 some financial institutions may reimburse consumers for some fraudulently induced transactions resulting from certain types of imposter scams.[29]

Receiving institutions bear legal responsibility and should bear more liability.

As discussed earlier, payments often involve two institutions: the one that sent the payment (the consumer's institution) 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 criminal fraudsters like the fake IRS caller would be deterred from using the ACH system. The ACH system vets and monitors who is 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 fraudster 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 criminal fraudsters 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 criminal fraudster has no direct liability for enabling the criminal to receive the payment. As a result, that institution has less incentive to prevent the criminal 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.

Financial institutions already have "Know Your Customer" (KYC) and account monitoring obligations under BSA/AML and 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,

[29] 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/.

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.

Recommendations to address payments fraud through the EFTA

The Agencies should also work with the CFPB and Congress to update the EFTA and to encourage financial institutions to use the EFTA framework for all types of electronic payments.

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 payment systems.

We encourage the Agencies to work with the CFPB to address current gaps and ambiguities in the EFTA that leave consumers unprotected. These include:

- Ensuring consumers are protected from liability when they are defrauded into initiating a transfer;
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment;
- Narrowing or eliminating the exemptions for bank wire transfers[30] 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;

[30] The EFTA itself does not directly exempt wire transfers. However, Regulation E exempts any transfer of funds through Fedwire or through a similar wire transfer system that is used primarily for transfers between financial institutions or between businesses. Reg. E, 12 C.F.R. § 1005.3(c)(3). That exemption should be eliminated, and until it is, it should be interpreted narrowly. When the EFTA was written, wire transfers were rarely used by consumers and required an in-person visit to the bank. But wire transfers today are regularly used by consumers and increasingly accessible through online banking and mobile apps. Fraudulent wire transfers can cause consumers to lose their entire life's savings. A court has also held that the wire exemption does not cover the transfer between the consumer and their bank before a service like Fedwire is used to transfer the funds. *See* New York v. Citibank, 763 F.Supp.3d 496 (S.D.N.Y. 2025).

- Clarifying that the error resolution duties under the EFTA apply if a consumer's account is frozen, 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, law enforcement order, or the consumer obtained the funds through unlawful or fraudulent means; and
- Considering whether consumer protections for checks should be included in the EFTA.

3. Challenges with Account Freezes, Closures, and Holds Due to Fraud Leading to Debanking of Consumers

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

The number of consumers who have complained about checking and savings account closures to the CFPB more than doubled since 2017.[31] In 2022, the CFPB ordered Wells Fargo to pay $160 million to over one million people for improperly freezing or closing bank accounts from 2011 to 2016 when it "believed that a fraudulent deposit had been made into a consumer deposit account based largely on an automated fraud detection system."[32]

There have also been stories featured by reporters detailing the devastating impact sudden account closures and freezes can have on consumers, especially when they are deprived access to their funds, are not provided with any information about the reason for the institution's actions, and are not provided an opportunity to address any perceived risk.[33]

---

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

[32] *In re. 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.

[33] 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; Kessler, Carson, "*A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money*," ProPublica (July 6, 2021), available at https://www.propublica.org/article/chime; McGreevy, Patrick, "*Bank of America must provide more proof of fraud before freezing EDD accounts, court orders,*" Los Angeles Times (Jun. 1, 2021), available at

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

Overly broad AML/CFT programs prevent innocent consumers from accessing their bank accounts and funds and understanding why those actions were taken.

Financial institutions have an obligation under the BSA to ensure that they maintain and follow internal ongoing CDD policies. The CDD policies must allow the institution to understand "the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and [c]onducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."[34]

Because of the CDD obligation and the ongoing problem of payment fraud, sometimes the appropriate response by an institution that suspects its customer is engaging in fraudulent or other illicit activity is to freeze a transaction or close an account that is being used to receive fraudulent funds before the funds are gone and more consumers can be defrauded. But sometimes financial institutions get it wrong, especially when automated tools are used. No law requires a financial institution to take these actions; it is up to the risk tolerance of the company and the internal policies set in place by the company. The only required response to potential fraud a company may need to undertake under BSA/AML law is to file a SAR if the transaction is large enough to meet the threshold reporting requirements and update their customer risk profile.[35]

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

---

https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california; KCAL News, "*Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud*," (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/.

[34] 31 C.F.R. § 1020.210(a)(2)(v);(b)(2)(v).

[35] 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/.

report on were likely innocent."[36] As these numbers demonstrate, even activity that leads to the filing of a SAR may ultimately not warrant an account freeze or closure.

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

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

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

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

The EFTA has clear error resolution timelines and procedures, and those should be used when consumers cannot access their funds. When a consumer is unable to make an electronic withdrawal or transfer because of an account closure or freeze based on suspected fraud, that action should be viewed as an error – an incorrect transfer of zero instead of the requested

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

amount – triggering the error resolution rights, duties, timelines, and investigation procedures of the EFTA. The EFTA's error resolution procedures can also be triggered by the consumer's request for information about a failed EFT, which is another enumerated error under the EFTA.[37] However, financial institutions and payment apps seem to believe the EFTA does not apply in this situation.

Recommendations

The Agencies should interpret the EFTA's error resolution procedures to apply to disputes from consumers when EFTs fail because of an account freeze or closure. The Agencies should also provide guidance to financial institutions about the importance of having clear procedures to enable consumers to quickly regain access to their funds when they are frozen due to concerns of suspicious activity, provide guidance as to the timeliness of returning an accountholder's funds after account closure, and specify that failing to have clear procedures and provide timely return of any funds may constitute an unfair, deceptive, or abusive business practice.

The Agencies, along with FinCEN, should 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 an FAQ that, while financial institutions are not allowed to disclose that a SAR was filed, they are allowed to describe the specific activities that raised concerns, giving the consumer an opportunity to respond and appeal a decision that was made in error, or based on false assumptions or false red flags.

The Agencies and FinCEN should also clarify that if a SAR does not lead to criminal prosecution or involvement by law enforcement for suspected money laundering/financing of terrorism activity, then a financial institution should not automatically take derisking measures and close the account based solely on the filing of a SAR, but the institution should instead take a measured, case-by-case, risk-based approach.

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

4. Checks and Regulation CC

Response to Question 13

The disputes between financial institutions about liability for fraudulent checks do not directly impact consumers. However, when the consumer's financial institution (the drawee bank) is

[37] 15 U.S.C. § 1693f(f)(6).

unable to be appropriately compensated by the depository bank, it can make the drawee bank delay in, or sometimes even fail to comply with, its obligations under the Uniform Commercial Code (UCC) to credit the consumer's account for a check that was not properly payable because the payee or amount have been altered or an indorsement has been forged.[38] Thus, we support action by the Agencies to require the depository bank to swiftly compensate the drawee bank. At the same time, the Agencies should be vigilant to ensure that drawee banks fulfill their obligations to their customers even if they have a dispute with the depository bank.

We also note that consumers need to have sufficient time to dispute a check as altered or forged. The UCC only requires that the consumer act with reasonable promptness in examining the bank statement and must promptly notify their bank[39] no later than one year after the statement is made available.[40] But many banks shorten those timelines in the account agreement, sometimes to as short as 30 days. Yet most consumers have never heard of check washing and reasonably do not expect that they should have to examine checks for alterations or forgeries. Moreover, most banks no longer return original checks and instead make check images available, often at a reduced size. Those images can be extremely hard to read. That problem is compounded by the widespread elimination of paper statements, with consumers only getting an email that an online statement is available, and bank websites are generally set up to encourage viewing transactions but not statements. If the amount has not changed, the consumer may have no reason to suspect anything is wrong. Thus, we encourage the Agencies to insist that financial institutions give consumers a reasonable time to identify and report check alterations and forgeries, which may be longer than 30 days.

Response to Question 14

The Board should update the funds availability schedule to eliminate or reduce the extra hold time allowed for several types of deposits. Modern technology and banking practices reduce the need for the extra hold time that was deemed necessary when the Expedited Funds Availability Act was written in 1987 and when Regulation CC was written (with few updates since) in 1987.

Regulation CC provides shorter hold times for checks deposited in person and allows extra hold time for other types of deposits. But banks are eliminating or reducing physical bank locations and encouraging people to deposit checks in other ways, including through ATMs and remote deposit capture (RDC) through mobile devices. These more modern check deposit mechanisms are as fast or faster than handing a paper check in person to an employee. RDC deposits are immediately imaged and can be processed more quickly. Checks deposited at ATMs are also routinely imaged.

[38] UCC § 3-407(b), (c) cmt. 2; § 4-401(d)(1); § 4-401 cmt. 1.
[39] UCC § 4-406(c).
[40] UCC § 4-406(f).

Thus, Regulation CC should be updated:

- To remove the extra day added for checks that otherwise qualify for next-day availability if the check is not deposited in person to an employee of the bank (i.e., eliminate the extra day for checks deposited at a bank's proprietary ATM);[41]
- To reduce the extra time allowed when a check is deposited at a nonproprietary ATM. In 2011, the Board proposed to reduce the maximum hold time for nonproprietary ATM deposits from 5 business days to 4.[42] Given new technology and banking practices, we believe that only one business day should be added for checks deposited at nonproprietary ATMs.
- To clarify the availability schedule for deposits made by remote deposit capture (RDC) through a mobile application. We continue to believe, as we suggested in 2013 and 2015, that mobile applications should be treated as ATMs.[43] Deposits made through the financial institution's own mobile application should be treated like a deposit to a proprietary ATM. Deposits through a nonproprietary RDC application should get one more business day just as we propose above for nonproprietary ATMs. At most, one day should be added to the availability schedule that would otherwise govern ATMs.
- To clarify that prepaid accounts, as defined in Regulation E,[44] are "accounts" within the meaning of Regulation CC[45] and that deposits to those accounts must be made available on the same schedule as deposits to other accounts.[46]
- To remove the extra hold time allowed for deposits made to bank branches in Alaska, Hawaii, Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the U.S. Virgin Islands and drawn on a bank in a different state.[47] With virtually all check processing now being electronic and with the elimination of the distinction between local and nonlocal checks, these geographic differences are no longer warranted.

Consumers need timely access to their funds; giving consumers faster access could help them pay bills on time and better manage their finances. However, funds availability requirements for checks should only be shortened to the extent that they can be done so without unduly exposing consumers to chargebacks in the event of fraud.

---

[41] 12 C.F.R. § 229.10(c)(2).
[42] Availability of Funds and Collection of Checks, Proposed Rule, 76 Fed. Reg. 16862 (Mar. 25, 2011).
[43] *See* NCLC et al., Supplemental Comments, 12 CFR Part 229, Regulation CC: Docket No. R-1409, 76 Fed. Reg. 16862 (Mar. 25, 2011), Remotely Created Items, Funds Availability Schedule for Prepaid Cards and Mobile Deposits at 8 (Sept. 18, 2013) ("NCLC 2013 Reg CC Comments"); Comments of NCLC et al to Federal Reserve Board on Regulatory Review under the Economic Growth and Regulatory Paperwork Reduction Act of 1996 (May 14, 2015) ("NCLC EGRPRA Comments 2015").
[44] Reg. E, 12 C.F.R. § 1005.2(b)(3).
[45] 12 C.F.R. § 229.20(a).
[46] We made this request in comments to the Board 12 years ago. *See* NCLC 2013 Reg CC Comments, *supra.*
[47] 12 C.F.R. § 229.12(e).

Chargebacks occur in situations where funds are made available to the consumer, but the collecting bank fails to receive settlement for the check.[48] A chargeback can result in severe harm to the consumer, who may have already spent the funds that were made available and can be left with a negative or very low balance. The result can be overdraft fees and bounced payments for critical expenses like rent and food.

Many deposit scams rely on funds being made available before a check has finally cleared.[49] Problems are compounded by the fact that bank employees themselves are confused and may tell consumers that a check has cleared when, in fact, the funds have merely been made available. In a typical scam, the consumer is given a check to deposit by the scammer, is subsequently told by the scammer that there was an overpayment, and is finally instructed by the scammer to send part of the payment back. The check appears to have cleared, and the consumer sends the money to the scammer as requested. However, the check then bounces, and the deposit is reversed. The consumer is then left to deal with the aftermath of funds made available too soon without the financial institution first properly verifying the check was properly payable.

As a result, funds should be made available sooner ***but only after*** financial institutions ensure a check has fully cleared. To effectuate this, the Board should shorten hold times to the extent reasonable, given today's faster check clearing and the modern tools available to financial institutions to identify suspected payment fraud. It no longer takes weeks to know whether a check has finally cleared. And, as discussed in the previous section, the Board should eliminate outdated extended hold times that are no longer warranted. But the Board should not otherwise reduce hold times if doing so would expose consumers to a significant risk of chargebacks.

Response to Question 15

- ***Exception for check deposits***

The exception for doubtful collectability should be usable when the depository institution suspects fraud. However, the institution should use it only to freeze the funds availability of the check amount, not to freeze an entire account. It is also important that depository institutions resolve the situation in a reasonable amount of time, such as the 10 days provided by the EFTA for disputes. Depository institutions must also follow the notice requirements in Regulation CC when invoking the exception.[50]

- ***Consider allowing limited exceptions for deposits by electronic fund transfer and wires***

[48] U.C.C. § 4-214(a).
[49] *See* Matt Alderton, AARP, Read This Before Accepting a Stranger's Check (Jan. 17, 2025).
[50] 12 C.F.R. § 229.13(g).

The six exceptions in Regulation CC only apply to check deposits, not to other types of deposits. Some of those exceptions are specific to checks. But other exceptions, such as the new account exception, would also be useful to prevent payments fraud involving wire transfers, FedNow, RTP, and ACH payments.

Most payment fraud is not accomplished by check but rather by different types of electronic transfers. These transfers can steal people's entire life's savings. Yet payment system rules generally require depository institutions to make funds from some types of transfers, such as those made through wire transfer, FedNow, and RTP, available instantly, and Regulation CC requires all electronic transfers to be available the next day.

When a criminal steals money from a consumer, whether through an unauthorized transfer or through a fraudulently induced transfer, that money is transferred somewhere. The depository institution that holds the account where the funds are received has KYC/AML responsibilities and should exercise those responsibilities when receiving suspicious transfers.

The Board should extend the new account exception to all types of transfers. New accounts are especially likely to be involved in fraud. Criminals open accounts using synthetic or stolen identities and then use those accounts to receive and launder stolen funds. By the time the depository receives disputes about the transfers or otherwise suspects that the account is being used for fraudulent purposes, the funds are likely gone. Even a short delay of a day or two in funds availability could help depository institutions freeze funds before they disappear.

The Board should also consider a new exception for suspected fraud, which would be similar to doubtful collectability for checks. For example, while Regulation J generally requires that funds sent by FedNow be made immediately available, if the beneficiary's bank has reasonable cause to believe that the beneficiary is not entitled or permitted to receive payment, the beneficiary's bank may notify its Federal Reserve Bank that it requires additional time to determine whether to accept the payment order.[51] A fraud exception to funds availability should be allowed even if the bank has formally accepted the payment order. The exception should encompass not only unauthorized transfers but also situations where the bank has reasonable cause to believe that a transfer initiated by the consumer was fraudulently induced.

<u>Payments fraud data collection and information sharing</u> (Response to Questions 16-20)

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,[52] as well

[51] Reg. J, 12 C.F.R. § 210.44(b)(3).

[52] 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

as the extent to which the activities[53] undertaken by an institution are covered by existing law. As a result, no centralized federal agency receives or collects all data about payment fraud.[54] Additionally, defrauded consumers may report fraud to the Federal Trade Commission, the FBI's internet crimes division, and/or the CFPB, 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. [55]

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 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.[56] 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.[57]

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.[58] The Clearing House also collects fraud reports for RTP® (their real time payments platform) and Early Warning Systems (EWS), owner

---

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.

[53] 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.

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

[55] 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.

[56] "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.

[57] *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).

[58] *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.

of Zelle, collects reports of fraud occurring on Zelle, though it is unclear if this information is shared widely among users.[59] Even initiatives such as SardineX[60] and Beacon[61] 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.[62]

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.

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

- **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.

---

[59] *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.

[60] *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.

[61] 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.

[62] 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.

Indeed, NCLC provided many of the recommendations that follow in comments to the FTC Collaboration Act of 2021.[63] 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.

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, 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 legislation[64] that encourages partnerships among various stakeholders, including regulators, industry representatives, consumer groups, and victim support groups. These kinds of task forces will not solve the problem of payment fraud, but will be an important first step to broaden information sharing.

- **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.

---

[63] *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.

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

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 reports from institutions utilizing Fedwire, though we have provided recommendations in the response to Questions 21-22 below. We do not know what fraud information is collected on other wire transfer services, such as The Clearing House's CHIPS system.

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.

- **Ensure consumers are protected from false positives.**

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

At the same time, if current legal regimes are interpreted or amended to allow for this type of information sharing (including changes to the BSA or the Gramm-Leach-Bliley Act), [65] then innocent consumers who are negatively impacted by the sharing of this information need adequate protection. Consumers who experience an account closure, account freeze, or the inability to open a new bank account after a closure due to suspected fraud (an adverse action) based on the shared information should have protections like those already provided under the Fair Credit Reporting Act. These protections should ensure, at a minimum, that:

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

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

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

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

The Agencies should also ensure impacted consumers have an avenue for disputing account closures and freezes through the EFTA's error resolution procedures, as described in more detail above.

Reserve Banks' Operator Tools and Services (Response to Questions 21-22)

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."[66]

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:

- 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 Board has an opportunity to impose requirements on users of its payments systems and to develop tools to assist financial institutions in keeping the systems 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 Board can build protections into Fedwire operations and impose requirements on Fedwire users to help detect fraud, prevent it from spreading, and recover money sent due to fraud or error when possible.

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.

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

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 criminal 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 Board 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 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 Board 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 criminal fraudster 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 criminal fraudster 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 database 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.

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."

Actions that receiving banks should be required to take.

- **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.[67] 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.

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.

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

[67] 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.

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 criminal fraudster posing as the agent to send it to another account.[68]

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.

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.

Millions of consumers and small businesses are hurt by criminal fraudsters who fraudulently induce them to send payments to beneficiaries who are not entitled to those payments. The beneficiary could be the actual fraudster; 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 fraudster.

---

[68] 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.

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.[69] Under the BSA, banks are required to verify customer identities using prescribed procedures at the time of account opening.[70] 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.[71] Banks are also required to have red flag programs to detect ID theft under the FCRA.[72]

Financial institutions that ignore their BSA, KYC, 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 a criminal fraudster.[73]

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 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,

---

[69] 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
[70] 31 U.S.C. § 5318; 31 C.F.R. § 1020.220.
[71] *See* 31 CFR 1020.210(a)(2)(v).
[72] 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).
[73] *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).

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.

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.[74] The Board 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 Board 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.

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, the Agencies 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.

[74] *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.

We appreciate the Agencies' willingness to undertake this effort and are happy to answer questions. If you have any questions, please contact Carla Sanchez-Adams at csanchezadams@nclc.org.

Respectfully submitted,

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