National Consumer Law Center

National Community Reinvestment Coalition

NATIONAL CONSUMERS LEAGUE

For confidence and safety in the marketplace since 1899.

August 10, 2022

Governor Lael Brainard, Vice Chair
Governor Michelle Bowman
Board of Governors of the Federal Reserve System
Washington, DC

Re: Preventing fraud and errors in FedNow

Dear Governors Brainard and Bowman,

As the Federal Reserve Board (FRB) continues its work to launch the FedNow Service (FedNow), we urge the Federal Reserve Banks (Reserve Banks) to take additional steps to prevent bad actors from using FedNow to steal funds from members of the public and to address errors. We are disappointed that the Board declined our request to incorporate fraud and error protections into the final Regulation J rule, but 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."[1] Adopting measures to prevent and remedy fraud and errors will not only protect consumers and other users of FedNow, but will be critical to protecting the integrity of and confidence in the system.

NCLC and its partners are very concerned with the devastating harm fraud in Zelle and other faster payment systems wreaks on consumers, including fraudulent inducement to initiate payments to bad actors.[2] If fraud is minimized, consumers will have confidence in utilizing faster payments. Conversely, if consumers lose money to fraud because there is weak monitoring to detect and stop fraud or few remedies for fraud and scams, both the credibility of FedNow and the entire effort to develop and promote faster payments will suffer.

---

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

[2] Herb Weisbaum, Consumer Check, Zelle Scams Spike; Banks Often Refuse to Help (May 20, 2022); Good Morning America, New warning as scammers try to trick Zelle users into sending money (Apr. 5, 2022); Stacy Cowley & Lananh Nguyen, NY Times, Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem. (Mar. 6, 2022); Bob Sullivan, Red Tape Chronicles, Zelle hackers 'improve' their scam, pretending to be fraud investigators; banks often won't help (Nov. 19, 2021).

It is critical for every entity participating in faster payments, such as payment providers, financial institutions, and network providers such as the FRB, 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 Federal Reserve Board still has an opportunity to impose requirements on users of FedNow and to develop tools to assist financial institutions in keeping the system safe so as to prevent, detect, and respond to fraud and errors. The Board has indicated that, beyond Regulation J, Reserve Banks will be issuing operating circulars and other materials to guide financial institutions. We expect that the FRB will also be assessing what more it can do to ensure the safety of FedNow. We offer some suggestions below on how the Reserve Banks and the FRB can build protections into FedNow operations and impose requirements on FedNow users to help detect fraud, prevent it from spreading, and recover money sent due to fraud or error when possible.

1. Actions by Receiving Banks

In our suggestions below, we mirror the UCC'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 the consumer. The "beneficiary" is the individual or entity to be paid and is a customer of the "beneficiary bank."

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

Even when fraud or errors in FedNow payments are not covered by the Electronic Fund Transfer Act's (EFTA) liability protections,[3] it is important for financial institutions to have a mechanism to receive reports of problems and to assist senders in resolving them wherever possible.[4] Despite the irrevocability of a payment, in some instances it may be possible to recover the funds. In addition, it is important to encourage reports of fraud and errors in order 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.

---

[3] We believe that consumer errors are covered by the error resolution requirements of the EFTA, as nothing in the EFTA or Regulation E limits the term "error" or "mistake" to those committed by a financial institution. We also believe that error resolution is required in "me-to-me" scams where the consumer is told to send money to their own mobile number, as the error is on the part of the beneficiary's bank – allowing the scammer to link the wrong token to their account – rather than on the part of the consumer. But even if the EFTA does not apply, as with non-consumer senders, reports of fraud and error should be collected.

[4] Financial institutions may also incorrectly assume that a dispute is not covered by the EFTA. Thus, they should err on the side of accepting and investigating disputes. *See* Andrew Ackerman, Wall Street Journal, CFPB to Push Banks to Cover More Payment-Services Scams (July 19, 2022).

The Reserve Banks should require receiving banks to accept reports of fraud and errors and make it easy for payment originators to make such reports. An operating circular for FedNow should make it a condition of participation in FedNow that each participant who interacts with a payment running over FedNow accept reports of fraud and errors 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, as discussed below.

B. When a payment originator reports that that they have been fraudulently induced into sending money, the receiving bank should initiate a request to return the funds.

While FedNow payments are designed to be irrevocable and there is no mechanism for the originator or receiving bank to unilaterally claw back the funds, the receiving bank does have the ability to request the beneficiary's bank to return the funds. 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 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 urge receiving banks to make an immediate request to return funds on behalf of a consumer when fraud in the inducement has been reported.

C. When a payment originator asserts a mistake in payment, FedNow operating circulars should require receiving banks to initiate a request to return the funds and to assist their customer in correcting the error through the beneficiary's bank.

Consumers may request assistance with transactions that resulted from a mistake. For example, if the consumer initiated a transaction with even one wrong digit in the cell phone number, the wrong person may receive the transfer. That beneficiary is not entitled to the funds, and, unlike in a scam situation, there may be greater prospects for correcting the mistake and retrieving the funds. It is important for financial institutions to assist in recovering the funds rather than merely asking the consumers themselves to ask for the money back. The receiving bank is better positioned than the consumer to interact with the beneficiary bank and sort out what is happening. Additionally, having both the receiving and the beneficiary banks involved can help consumer beneficiaries avoid scams similar to check deposit scams where the consumer is asked to return money but then the original deposit is reversed.

The FedNow operating circulars should direct receiving banks to initiate a request to return the funds and to assist the consumer's efforts to correct those mistakes.

The consumer will likely not know the identity of the beneficiary's bank, and even if they did, the beneficiary's bank would not respond to them. The beneficiary and the beneficiary's bank may be willing to cooperate, but the consumer will need the assistance of the receiving bank to

initiate the process. Further, the mistaken beneficiary needs protection from false requests to return funds via a brand-new payment.

In a real-life example, a consumer accidentally entered a cell phone number incorrectly and sent money to the wrong person. The consumer then called the recipient (unintended beneficiary) and asked him to return the money. The unintended beneficiary knew that he was not entitled to the money and was willing to return it but was reluctant to send it back because he did not know if he was being scammed. Both the consumer and the unintended beneficiary contacted their banks – both large, top-10 banks -- and asked for assistance. Neither bank would cooperate or help the unintended beneficiary to know whether or how he could safely return the money. The unintended beneficiary eventually did return the funds two weeks later in good faith, but with no assistance from the banks.

In this situation, the receiving bank should be required to both send a request to return the funds and to interface with the beneficiary's bank to help correct the mistake.

2. **Actions by Beneficiary Banks**

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

Regardless of which of these categories the beneficiary falls into, the beneficiary's bank has responsibilities under know-your-customer and anti-money laundering laws to ensure that accounts are not opened with fraudulent identities and that accounts are not being used for illegal purposes.[5] For example, banks are required to have red flag programs to detect ID theft under the Fair Credit Reporting Act (FCRA).[6] Under the Bank Secrecy Act, banks are required to verify customer identities using prescribed procedures at the time of account opening.[7] 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.[8]

---

[5] 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

[6] 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).

[7] 31 U.S.C. § 5318; 31 C.F.R. § 1020.220.

[8] *See* 31 CFR 1020.210(a)(2)(v).

Financial institutions that ignore their Bank Secrecy Act, know-your-customer, and due diligence obligations could face regulatory or enforcement actions. Those that overlook warning signs of fraud may also face other legal repercussions if they are found complicit in helping scammers.[9]

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

It is likely that the beneficiary bank will receive notice of the alleged fraud from the receiving bank of the defrauded consumer 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 exercise their right to delay acceptance under Regulation J. More specifically, the beneficiary's bank should notify its Reserve Bank that it needs to delay acceptance of the payment order and not make the funds immediately available to the beneficiary because it has reasonable cause to believe that the beneficiary is not entitled or permitted to receive the payment.[10] These actions are consistent with those outlined in the Federal Reserve Board's commentary.[11] An operating circular could elaborate on this option and encourage banks to exercise it in order to investigate a fraud report based on a claim of fraudulent inducement. Where circumstances warrant, the beneficiary's bank should consider freezing the account.[12] Moreover, even where the payment order is accepted and funds have been made available, if there has been a report of fraudulent inducement, the bank should still investigate to assess whether its customer is engaged in unlawful activity and the account should be closed.

Additionally, until the investigation is complete, the FedNow operating circulars should require suspension of the use of the flagged account and the FedNow tokens linked to it (i.e., cell phone number or email) to receive or send funds through FedNow.[13]

---

[9] *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).

[10] 12 C.F.R. § 210.44(b)(3) ("In circumstances where the beneficiary's bank (other than a Federal Reserve 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.").

[11] "As an additional example, if the beneficiary's bank has reasonable cause to believe that a particular payment order may be related to fraudulent activity, the beneficiary's bank may notify its Federal Reserve Bank that it requires additional time to determine whether to accept the payment order, including to investigate the suspected fraudulent activity." Commentary to Reg. J, Part 210.44(b)(4), available at 87 Fed Reg 34350, 34368 (June 6, 2022).

[12] As discussed in Section 3.B. below, we understand the importance of avoiding overbroad reactions that harm innocent accountholders.

[13] It is important that the Federal Reserve take this action, as the beneficiary's bank will not be able to prevent the beneficiary from linking that cell phone number or email to a different account used to receive FedNow payments.

3. **Fraud Reporting.**

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

Financial institutions utilizing FedNow should be required to report all complaints of fraud and scams asserted by consumers and businesses to a centralized database, even if a Suspicious Activities Report (SAR) is not required. Participants in FedNow, 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. Indeed, FedNow payments may not even reach that size, at least not initially.

The FRB should develop a central database that permits the participants in the chain of a payment to share information to combat fraud, and the FedNow operating circular should require that all entities in the payment chain participate in that database. A scammer who has defrauded one consumer is likely to have defrauded others and to continue to do so until stopped. However, patterns that reveal fraud cannot be detected if information is not reported and collected. Similarly, if one bank closes an account but the scammer just creates a new account, fraud will continue. A centralized fraud reporting system/database will ensure that all financial institutions participating in FedNow 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.

The importance of collecting information about fraud is another reason why receiving banks should be required to send requests for return of payment. 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.

Another reason for creating a fraud database is to ensure that participants have access to information about individuals or entities that have been barred from using the FedNow system because of fraudulent activity. In fact, the Federal Reserve suggested something comparable in its fraud prevention tips to financial institutions utilizing instant payments.[14] NACHA, for example, has a terminated originator list that serves a similar function.

B. Consumers should have procedures to contest actions taken against them based on incorrect reports of fraud.

[14] "Add suspicious accounts and aliases to a watch list to block potentially fraudulent transactions before the funds leave your institution." The Federal Reserve, Fraud and instant payments: The basics.

We recognize that efforts to combat fraud can result in overbroad actions that impact innocent consumers.[15] If a beneficiary raises a dispute about a FedNow payment not properly received or made available, or about an account freeze or a funds freeze or block, the beneficiary's bank must conduct a reasonable investigation and unfreeze improperly frozen accounts.[16] An improper account freeze or block will result in a mistaken hold up of an electronic fund transfer, which should be viewed as an error under the EFTA; thus the procedures and timeline for this investigation should generally be the same as the error resolution procedures under the EFTA if the beneficiary is a consumer.[17] However, there may be exceptions that require funds to be frozen for longer periods of time, as in the case of criminal investigations.

To the extent that a fraud database is governed by the Fair Credit Reporting Act (FCRA), the FCRA's requirements should of course be followed. But even if the FCRA does not technically apply,[18] FedNow operating circulars should require all financial institutions that furnish information to or use information from a fraud database to comply with similar requirements.[19] Thus, if an account is frozen or if a financial institution chooses to deny use of FedNow based upon information reported to a FedNow database, the affected accountholder should receive a notification that includes reliance on the database as the reason for the action. The accountholder should have the right to a disclosure of the information in the database about them and the ability to dispute any inaccuracies.

Moreover, even if the EFTA and FCRA do not apply, using an erroneous fraud report as the basis for denying access to FedNow or freezing funds indefinitely without conducting a reasonable investigation could be an unfair or deceptive practice.[20]

Finally, it is likely that financial institutions that will use FedNow are already familiar with the error resolution procedures under the EFTA and reporting and reinvestigation requirements under the FCRA in other contexts. Thus, undertaking similar investigations should not be burdensome since these same financial institutions must conduct them in other contexts under EFTA and the FCRA.

---

[15] *See, e.g.,* Patrick McGreevy, Los Angeles Times, Bank of America must provide more proof of fraud before freezing EDD accounts, court orders (June 1, 2021); CFPB, Press Release, Federal Regulators Fine Bank of America $225 Million Over Botched Disbursement of State Unemployment Benefits at Height of Pandemic (July 14, 2022).

[16] *Id*.

[17] We believe account freezes are "errors" under the EFTA when they prevent electronic fund transfers.

[18] Courts have found that government agencies are not credit reporting agencies. *See, e.g.,* Ricci v. Key Bancshares of Maine, Inc., 768 F.2d 456 (1st Cir. 1985) (FBI is not a credit reporting agency). If the operator of the fraud database is not a credit reporting agency (CRA), then those who furnish information to that database would not be subject to the FCRA. However, it is not clear if decisions regarding the FBI's status as a CRA would govern in a different setting.

[19] *See* 15 U.S.C. §1681 (k)(B)(iv). An adverse action could include freezing a consumer's account or suspending a consumer's use of FedNow.

[20] *See* Consent Order, *In the Matter of Bank of America, N.A.*, File No. 2022-CFPB-0004 at 16-19 (CFPB July 14, 2022) (finding that Bank of America engaged in unfair and abusive acts or practices by automatically determining, without any further investigation, that no error had occurred regarding purported unauthorized electronic fund transfers flagged on the basis of the bank's fraud filters, and by applying the filter retroactively).

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

FedNow operating circulars should strongly encourage 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.[21] The Fed could identify red flags that are specific to FedNow payments.

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

Additionally, the Fed 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 FedNow. This will help inform regulators, policy makers, and industry and consumer groups about trends and challenges unique to faster payments.

* * *

Thank you for considering these suggestions for making FedNow a safe payment system. We would be happy to discuss these and any other issues with you. For questions, please contact Carla Sanchez-Adams at csanchezadams@nclc.org.

Yours very truly,

National Consumer Law Center (on behalf of its low-income clients)
National Community Reinvestment Coalition
National Consumers League

[21] *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.