September 9, 2021

By email to regs.comments@federalreserve.gov
Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750, RIN 7100-AG16, 86 Fed. Reg. 31376 (June 11, 2021)

The National Consumer Law Center (NCLC) (on behalf of its low-income clients), the National Community Reinvestment Coalition (NCRC) and the National Consumers League (NCL) appreciate the opportunity to submit comments to the Federal Reserve Board (FRB) on its proposed rules for implementing the FedNow faster payment system.

We have significant concerns that FedNow, under the proposed Regulation J ("Reg J"), will not be safe for consumers and other small users. We urge the FRB not to launch the FedNow service until it is safe for small users, including protection against fraud in the inducement and sender mistakes. We also urge the FRB to address specific parts of the proposed Reg J that are inappropriate for consumers and will cause confusion, that will impede financial institutions from preventing and remedying fraud and errors, that conflict with Regulation E, and that leave consumers and other users without a reliable right to the speed that the system promises.

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, and has been involved with the FRB's faster payments efforts since their inception.

The National Community Reinvestment Coalition (NCRC) is an association of more than 600 community-based organizations that work to promote access to basic banking services including credit and savings. Our members, including community reinvestment organizations, community development corporations, local and state government agencies, faith-based institutions, community organizing and civil rights groups, and minority and women-owned business associations help create

and sustain affordable housing, job development and vibrant communities for America's working families.

The National Consumers League is America's pioneering consumer advocacy organization, representing consumers and workers on marketplace and workplace issues since our founding in 1899. Headquartered in Washington, DC, today NCL provides government, businesses, and other organizations with the consumer's perspective on concerns including fraud prevention, child labor, privacy, food safety, and medication information. NCL operates Fraud.org, which provides and collects information about consumer fraud.

NCLC, NCRC and NCL are all members of the Faster Payments Council, but these comments are submitted solely on behalf of our own organizations.

Our comments follow. Thank you for considering our views.

Yours very truly,

Lauren Saunders, Associate Director
Margot Saunders, Senior Counsel
National Consumer Law Center (on behalf of its low-income clients)

Adam Rust, Senior Policy Advisor
National Community Reinvestment Coalition

John Breyault, Vice President of Public Policy, Telecommunications and Fraud
National Consumers League

Table of Contents

I. Introduction and Summary

We appreciate the efforts of the Federal Reserve Board (FRB) to articulate rules for the anticipated FedNow faster payments system. While individuals are increasingly using the person-to-person (P2P) processes currently available to make and receive fast payments, a more secure, transparent, reliable and ubiquitous payments system is very much needed. There is much room for improvement in faster payment services, as those currently operating too often facilitate fraud at higher rates than traditional payment systems, while failing to protect individuals from common errors.

However, as detailed below, the current formulation for the FedNow program will not provide the secure and reliable process needed for consumers and small business users to be safe. The proposed Regulation J[1] ("Reg J") may work well for the bank participants in the process, and for large corporate entities that are able to evaluate and negotiate the benefits and risks of using FedNow. But the proposed rules replicate the problems in existing P2P systems that subject the "small users"[2] – individuals who are either consumers or those engaged in small business enterprises – to a heightened risk of harm from fraud and mistakes.

Section II of these comments focuses on the need to protect small users of FedNow, especially in cases of fraud and mistakes. We provide illustrations of the financial hazards that are currently faced by individuals using the faster payment systems in the existing marketplace. Indeed, if finalized as proposed, FedNow would likely join the list of payment operating platforms that enable scams. And the individual victims of these scams would continue to be without effective protection or redress from the financial institutions that allow scammers into the system and facilitate the transfers of funds.

The FRP cannot rely solely on Regulation E to provide protections for consumers because, in its current form and as interpreted by financial institutions, Regulation E does not adequately protect consumers against fraud in the inducement and sender errors. Regulation E also provides no protection to small businesses at all.

We strongly urge the FRB to move forward with the launch of a FedNow service *only* when the new system can provide reasonable assurances that individuals will be protected from fraud and errors. The United Kingdom (UK) has taken steps to protect consumers from errors and fraud in the inducement,[3] illustrating that financial institutions can provide these protections in a competitive marketplace. The FRB should learn from and improve on the UK experience.

---

[1] Federal Reserve Sys., Proposed Rules, Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, 86 Fed. Reg. 31,376 (June 11, 2021) [hereinafter Proposed Rules].

[2] For this discussion, we include both individual consumers as defined by the EFTA and small businesses as "small users," because they all would suffer from similar risks from the transfers in the proposed Reg J.

[3] UK Finance. "Fraud - The Facts 2021: The Definitive Overview of Payment Industry Fraud," 2021. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf.

Protecting users will also incent the financial institutions and their service providers that facilitate FedNow payments to create their own guardrails to prevent losses from fraud and errors in the first place. The system can bear and spread the cost of minor amounts of fraud and errors, but even a single loss can be devastating to a consumer or small business. If overall losses are significant, then the system is not safe to use.

The FedNow system must also include a mechanism, such as a reverse entry, that allows the sending institution to quickly reverse a payment to correct errors or fraudulently induced payments, without waiting for the receiving institution to act or return the funds. Payments can still be final immediately, but error resolution will be faster. Time is of the essence when correcting errors to protect all participants from problems before funds are gone.

The FedNow system also needs better information sharing to prevent fraud and mistakes. The FRB should develop a FedNow directory to ensure that funds are being sent to the right person. The directory should be governed by rules and procedures to ensure that the directory information is and remains accurate and that users' private information is not accessed inappropriately without their consent. End-users should be able to review and correct their information and to set permissions on its usage. FedNow should also permit the players in the chain of a payment to share information when it can help to combat fraud.

The FRB should work closely with the Consumer Financial Protection Bureau (CFPB) to develop a comprehensive set of proposed regulations that both facilitates the faster payments contemplated and protects all the users of the system, particularly including consumers and small businesses.

Section III of these comments addresses concerns about other specific aspects of the proposed rules, including:

A. **Reg J should not apply Uniform Commercial Code (UCC) Article 4A to consumer transactions at all, even in the absence of a conflict.** Article 4A was designed for transactions between large, sophisticated parties with equal bargaining power. Article 4A was not designed with protections for small users of bank transfers in mind. It includes provisions that are inappropriate for consumers and permits adhesion contracts that could abrogate those protections it does provide. Conflicts between Regulation E and 4A may also not always be apparent, and combining two regulatory regimes that were designed to be separate will add confusion.

B. **Payments should not be processed if the recipient identified by the sender does not match the name on the account.** The proposed Reg J would explicitly permit the non-refundable payment of funds to mistaken recipients. Rather than require that the banks implementing these instantaneous payments employ systems designed to screen for, detect, and rigorously guard against mistakes, the proposed Reg J would allow the non-recoverable transfer of funds into accounts that do not even match all the information provided by the sender. This maintains and validates a system that prioritizes speed and ease of use ahead of safety. The UK, by contrast, requires a consortia of the UK's nine largest banks to make a "confirmation of payee" before they send funds through the UK's Faster Payments system.

C. **Receiving institutions should have more leeway to delay accepting payments or making funds available in order to prevent identifiable problems before they occur.** The proposed Reg J would allow the recipient's bank to delay acceptance of the payment order or funds availability only in limited circumstance, such as potential violations of sanctions rules. Instead, banks should have more latitude to delay acceptance in case of red flags, which may indicate mistaken transfers or transfers that are the result of frauds on the senders. Financial institutions have a duty to know their customers and to ensure that their customers are not using their accounts for illegal purposes. The FedNow system must allow a bank to stop or slow down a transfer when there are indicia of fraud or mistakes.

D. **Absent indicia of fraud or mistake, Reg J should provide an enforceable right that the funds be made available to the recipient within the promised timeframe.** FedNow generally contemplates and require transfers and funds availability "in a matter of seconds."[4] Yet neither recipients nor senders could enforce these promises. Instead, the only enforceable right to the availability of the funds would depend on the application of Regulation CC, which would allow delays of multiple days in some instances.

E. **If used for international transfers, the proposed Reg J would appear to set up a conflict with the Electronic Fund Transfer Act's (EFTA) rules for remittance transfers.** The potential application of these rules to international transfers is unclear. Without further protections, international use could pose a significant risk to senders of remittances. The error resolution procedures in Reg J directly conflict with those applicable to remittances, and Reg J would conflict with the EFTA requirement for a 30-minute right to cancel in a way that would effectively eradicate the right to cancel. While international use may not be presently contemplated, the rules should either bar international use or require compliance with the EFTA in the event of a conflict with Reg J rules.

II. The FRB Should Not Launch the FedNow Service nor Finalize the Proposed Rules Until the System is Safe for Small Users

A. Scams and Mistakes Enabled by P2P Payment Systems Create Expensive Problems for Consumers and Small Businesses

In 2020, the FTC received 62,371 complaints of fraud in which the scammers had used a payment app, resulting in consumers' total loss of $87.4 million.[5] This is an increase of 192% over the previous years.[6] A new FedNow system adopted without sufficient protections will only exacerbate the rate and amount of these losses.

---

[4] Proposed Rules at 31,378.

[5] FTC Consumer Sentinel Network, Fraud Reports by Payment Method 2020 (July 28, 2021), *available at* https://public.tableau.com/app/profile/federal.trade.commission/viz/shared/PNHPRMN39.

[6] *Id.,* FTC Consumer Sentinel Network, Fraud Reports by Payment Method 2019 (July 28, 2021), *available at* https://public.tableau.com/app/profile/federal.trade.commission/viz/shared/PNHPRMN39.

Many of these losses are directly linked to the rapid growth of peer-to-peer ("P2P") payment platforms such as PayPal's Friends & Family and Venmo services, Square's Cash App, and Zelle. These P2P services are used by tens millions of people by allowing for free or very low-cost payments to be sent between consumers or from consumers to businesses.[7] An astounding 79% of Americans use mobile payment apps.[8]

As the usage has climbed in recent years, so have the complaints: in the past four years, there have been almost 10,000 complaints to the CFPB about payment apps, more than half of which were in the year preceding April 2021.[9] So while the convenience of the immediate payment systems has taken off throughout the U.S., the problems created for consumers have also skyrocketed—the yearly number of complaints doubling in the last year.[10]

Approximately one quarter of the payment app complaints to the CFPB related to scams, with about the same number tied to unauthorized transactions or other transaction problems. These problems are escalating because there are no requirements in the current payment app systems that require the system operators to protect consumers against fraud and common errors. Given what we know about how scammers target opportunities with the least resistance, it stands to reason that fraud and errors will continue to plague faster payments if financial institutions are allowed to operate under the assumption that they are not liable for fraud in the inducement or sender errors.

According to recent testimony submitted to Congress by the National Consumers League,[11] which tracks losses due to frauds and scams, the median loss reported by victims of these scams was $374, though many victims lost far more.[12] One consumer who contacted NCL's Fraud.org campaign recently reported losing $15,000 to a scammer.

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

A. A South Carolina woman loaned her phone to a man who knocked at her door claiming to be locked out of his car. While pretending to text a family member, he transferred more than $1,000 to himself through her Venmo account. She filed a police report and notified Venmo

---

[7] Alexander Kunst, Statista Global Consumer Survey (Nov. 19, 2020), *available at* https://www.statista.com/forecasts/997123/peer-to-peer-payments-in-the-us.

[8] U.S. PIRG Educ. Fund, Virtual Wallets, Real Complaints 2 (June 2021), *available at* https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

[9] *Id.*

[10] *Id.*

[11] Hearing Before the U.S. Sen. Comm. on Banking, Housing, & Urban Affairs Subcomm. on Financial Institutions & Consumer Protection, 117th Cong., 1st Sess. (Aug. 3, 2021) (testimony of John Breyault, Vice President of Public Policy, Telecommunications, & Fraud, National Consumers League).

[12] *Id.* at 2.

but has received no relief.[13]

B. Luke Krafka, a professional musician in Long Island, lost almost one thousand dollars through Zelle when a fake client "hired" him to play at a wedding. The man sent him a large check and asked him to pay part of the money back through Zelle. The check bounced after Krafka had already sent the money. Zelle refused to refund his payment.[14]

C. Mary Jones of Kansas City paid $1,700 through Venmo in "rent" to a man who claimed to own the house she wanted to move into. He even gave them access to tour the house before she signed the lease. After she saw a For Lease sign in the front yard, she called the rental company and discovered that she had paid a scammer. She filed a police report but has not been able to retrieve her money.[15]

D. Brinda Gupta, a Chicago business owner, received a text that her Zelle account had been compromised. She spoke on the phone to a man claiming to represent Bank of America. He gleaned enough information about her account that he was able to steal its details and transfer more than $6,000 to himself. Bank of America at first refused to refund her, and only did so after a journalist from the *Chicago Sun Times* reached out to them.[16]

E. Arthur Walzer of New York City tried to send his granddaughter $100 through Venmo as a birthday present, but instead sent it to a woman with the same first and last name. When he discovered the error, he told his bank to refuse payment of the $100, and in response Venmo froze his account and demanded that he pay them. Venmo eventually refunded him, but only after a journalist contacted the company on his behalf. It was the first time he had ever used Venmo – he set up an account specifically to give his granddaughter the gift.[17]

---

[13] *See* Briana Harper, *'This could happen to you': Charlotte woman falls victim to Venmo scam*, WCNC Charlotte (Feb. 4, 2021), *available at* https://www.wcnc.com/article/news/crime/charlotte-woman-shares-warning-about-falling-victim-to-venmo-scam/275-61c3fd40-d040-4604-ae18-bf1bfb863a61.

[14] *See* CBS This Morning, *Complaints against mobile payment apps like Zelle, Venmo surge 300% as consumers fall victim to more money scams*, CBS News (June 23, 2021), *available at* https://www.cbsnews.com/news/venmo-payal-zelle-cashapp-scams-mobile-payment-apps/.

[15] Tia Johnson, *Kansas City woman warns others after losing nearly $2,000 in rental home scam*, Fox4 (May 3, 2021), *available at* https://fox4kc.com/news/kansas-city-woman-warns-others-after-losing-nearly-2000-in-rental-home-scam/.

[16] *See* Stephanie Zimmerman, *'Painful lesson' on payment apps: It was a lot easier to be scammed than Chicago business owner realized*, Chicago Sun Times (July 2, 2021), *available at* https://chicago.suntimes.com/2021/7/2/22559464/payment-app-p2p-zelle-venmo-square-brinda-gupta-boa-bank-america-pirg-bbb-scam-fraud-consumer-money.

[17] *See* Christopher Elliott, *A Venmo user sent $100 to the wrong person. Then the payment service froze his account*, Seattle Times (Nov. 2, 2020), *available at* https://www.seattletimes.com/life/travel/a-venmo-user-sent-100-to-the-wrong-person-then-the-payment-service-froze-his-account-travel-troubleshooter/.

F. An employee of NCLC unexpectedly saw $1,000 arrive in his bank account through Zelle. A few minutes later, he received a frantic phone call from a man telling him that he had put in the wrong cell phone number and asking for the money back. The NCLC employee wanted to return the money but asked his bank for assurances that it was not a scam. The man also called his bank. Both banks (both large top-10 institutions) refused to help correct the error. After weeks of getting nowhere, the NCLC employee returned the funds on faith.

In some of the instances above, consumers may be protected by Regulation E and the financial institution may have violated Regulation E by failing to resolve the error. But if the consumer initiated the transfer, caused the error, or is viewed as having furnished the access device to the scammer, financial institutions are likely to dispute their liability and even their responsibility for trying to resolve the error.[18]

Scammers have extraordinary creativity. They are constantly developing creative ways to steal people's money. The Federal Communication Commission's website includes a Scam Glossary detailing dozens of different ways individuals and small businesses have lost money to scams.[19] And P2P payments are specifically identified as a primary means for executing these scams.[20] Clearly the warnings provided by the payment apps themselves to beware of scams is not adequate to protect consumers from the losses.

US PIRG noted in its recent report: "As consumers grow increasingly reliant on payment apps, more and more consumers are running into problems that cost them money and time. This is clearly evidenced by the explosion of digital wallet consumer complaints in the CFPB's Consumer Complaint Database over the past year."[21]

Regulators in the United Kingdom have acknowledged that faster payments have become the preferred tool for "faster fraud." A recent study by the UK Finance Authority of fraud in 2019 and 2020 reported that faster payments were used in 96 percent of the push payment fraud cases.[22] Losses due to authorized push payment scams were £479 million in 2020 ($662),[23] a five percent rise from the previous year.[24] This was split between personal (£387.8 million) and nonpersonal or

[18] The inadequacies of Regulation E are discussed in the next section.

[19] Federal Commc'ns Comm'n, Scam Glossary, *available at* https://www.fcc.gov/scam-glossary.

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

[21] U.S. PIRG Educ. Fund, Virtual Wallets, Real Complaints 9 (June 2021), *available at* https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

[22] UK Finance. "Fraud - The Facts 2021: The Definitive Overview of Payment Industry Fraud" at 75 (2021), https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf.

[23] *Id.* at 52.

[24] *See* UK Finance, Press Release, "Criminals exploit Covid-19 pandemic with rise in scams targeting victims online" (March 25, 2021), https://www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-pandemic-rise-scams-targeting-victims-online.

business (£91.3 million). In total there were 149,946 cases. Of this total, 143,259 cases were on personal accounts and 6,687 cases were on non-personal accounts.

The FRB should learn from the experience of existing P2P payment systems and build protections in at the beginning.

B. Regulation E currently provides inadequate protections for consumers in P2P systems and none for small businesses

1. Regulation E does not provide adequate protections to consumers for modern-day electronic fund transfers.

The proposed rules rely on the EFTA, which is implemented by Regulation E, to provide protection against unauthorized transfers and error resolution for consumers. But Regulation E, in its current form and as interpreted and implemented by financial institutions, does not provide adequate protections to consumers in P2P push-payment systems like those on the market today or FedNow.

The EFTA was enacted 43 years ago and does not directly address many of the most important issues in the current consumer payment ecosystem. While Regulation E has been updated over the years (most recently in 2019 to incorporate prepaid accounts), neither the statute nor the regulation directly addresses authorization procedures for most payments, fraudulently induced payments, or mistakes by consumers in new payment systems that were not contemplated in 1978. The statute was initially adopted at a time when consumers were conducting business with their own financial institutions and were using payment systems that did not lead to the same types of problems that plague today's P2P systems.

Regulation E gives consumers protection from unauthorized transfers, but the definition of "unauthorized transfer" 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." 12 C.F.R. § 1005.2(m) (emphasis added). Since FedNow will be a push-payment system, with the payment initiated by the consumer, that means that Regulation E's protection against unauthorized transfers will likely not apply when the consumer is fraudulently induced to make a payment, even if that payment is arguably unauthorized.

Whether a fraudulently induced payment is "incorrect" and thus can be considered an error under Regulation E is unclear. While the CFPB has authority to identify types of errors by regulation,[25] it has not yet done so. That omission is the reason that fraud in the current P2P systems leaves people exposed to the serious problems described in the previous section.

There is little difference between these 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.*

[25] *See* 15 U.S.C. §1693f(f)(7).

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.

The only difference between these two scenarios is that in the second Laurie was the person that took the first step in the payment system to initiate the payment. That difference does not make the scammer any more entitled to the money or make the scammer's bank any less responsible for banking a scammer. Yet in the first scenario, Regulation E protects Laurie, and she could contest the debit as unauthorized, whereas in the second, financial institutions take the position that she is unprotected because she initiated the payment.[26]

Indeed, the first scenario is unlikely, because scammers like the fake IRS caller would likely not use 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 scammer from having an account or having access to the ACH system.

But under the proposed Reg J, the FedNow system would be more attractive to scammers than the ACH system. It will be easier for scammers to sign up for the FedNow service – potentially using stolen identities – and to receive FedNow payments (directly or through money mules). Using FedNow, the scammer's or money mule's bank would not need to make a warranty to the consumer's bank about the payment, leaving Laurie unprotected. This process would mean the receiving bank would have no liability for enabling the scammer to receive the payment, giving the bank less incentive to prevent the scammer from having an account, to put a hold on access to suspicious payments, or to shut down the account quickly.

A second problem with Regulation E is the lack of clarity around protections involving errors that are made by consumers. While Regulation E gives consumers a right to ask their bank to resolve errors, and imposes error resolution duties on financial institutions, many banks take the position that they have no duty if the error was committed by the consumer.

It is disputable whether this narrow view of the errors covered by Regulation E is correct: nothing in the EFTA excludes consumer errors, and Regulation E should be interpreted to cover them. When a payment is sent to the wrong person or in the wrong amount, the person receiving the payment is no more entitled to the payment even when the error was caused by the sender. But today, most consumers are out of luck in this situation unless their bank decides to help them and the receiving bank or payee is cooperative.

[26] In the ACH system, the scammer's bank that originated the ACH debit entry gives the consumer's bank a warranty that the entry is authorized. That warranty, along with the receiving's bank ability to initiate a return entry to recredit the funds, creates a mechanism to protect Laurie. There is no reason that those warranties and mechanisms could not be built into the FedNow system even though it is a push payment system. Those who enroll in the FedNow system and use it to receive payments could warrant that they will not fraudulently induce people to send payments to which they are not entitled.

As illustrated with the examples in the previous section, errors are easy to make in today's P2P systems. For example, today consumers can send money through P2P systems using nothing more than a cell phone number to identify the recipient. It is simple to accidentally type in the wrong cell phone number. The intended recipient also may have provided the wrong number (in which case it really was not the consumer who made the error). Or, a scammer may have claimed that they were someone other than who they are, and the cell phone number will not reveal who the money is really going to. Even if it is the right number and the right person, there can be problems. A consumer may have a cell phone number that is linked to numerous accounts at more than one financial institution:

- Both a joint check and savings account with her husband
- A joint account with her older son, now an adult, which he controls
- A joint account with her younger son, now an adult, which he controls
- A joint account with her uncle, whose finances she helps to manage
- A savings account in her own name.

How is someone to know which account it will go to – or whether the money will be withdrawn by someone else if it goes to the wrong account?

Errors can be devasting to consumers.

> ***Picture Mary****, a consumer whose rent is due on August 1. Mary has an account with a nonbank entity (sometimes inaccurately called a challenger bank or neo bank) and the funds are held at a bank that does not interact with Mary. Mary plans to use FedNow to pay the rent in the afternoon once she has deposited sufficient funds. She is behind in her rent and her landlord has threatened to evict her if she is late paying her August rent. If she is evicted, she and her 2 children will be homeless.*
>
> *Mary's uses FedNow to transfer money to the landlord, but a mistake at some point in the transaction occurs, and although the funds are withdrawn from her account, they are not deposited into the landlord's account. The result is that the landlord considers the rent as not paid on time, and Mary does not have any more the funds to pay her rent.*

In this scenario, neither Mary nor the landlord may know the actual cause of the failure of the funds to appear in the landlord's account. Was there a mistake in the transmission? Whose mistake was it, one of the banks involved, or one of the parties (and which party)? If the bank takes the position that this was a consumer error and it has no responsibility under Regulation E, Mary can do nothing.

Another inadequacy of Regulation E is that it provides that the financial institution reviewing an error claim will only have the obligation to do a "review of its own records regarding an alleged error . . . if (i)[t]he alleged error concerns a transfer to or from a third party; and (ii) [t]here is no agreement between the institution and the third party for the type of electronic fund transfer involved."[27] The proposed FedNow system involves transfers through Federal Reserve Banks, and Reg J applies a superstructure governing these transfers between independent parties that interact with those banks, making it less likely that there will also be agreement between the end-users'

[27] 12 C.F.R. § 1005.11(c)(4) (emphasis added).

institutions themselves. As a result, if the error was caused by or revealed only in the records of a party other than the financial institution[28] with which the consumer deals, Mary has no effective remedy to deal with the lost money.

Adding one fact to *Mary's* plight, further illustrates the problems with relying solely on the EFTA to protect consumers like Mary.

> *Let's assume that the landlord's last name is Smithe (with an "e"), and when Mary initiated the transfer on her smartphone, and typed the name in the payment app, the app autocorrected the spelling to be "Smith" (without the "e").*
>
> *And assume further that at the large national bank which holds the landlord's account, another person with same first name as the landlord, and the last name of Smith (spelled without an "e") also has an account.*
>
> *Mary's money was deposited within seconds into the wrong Smith's bank account. And that Smith immediately withdrew the funds.*

If the bank or app provider views this as an error by Mary, it is unlikely to resolve the error, as discussed above – even though the app designer enabled the error. So again, Mary would be out of luck, and would be subjected to eviction because the payment system did not protect her from a series of errors that were made by machines.

Before it launches a system that can create such problems for consumers, the FRB, potentially working with the CFPB, must fill the gaps in Regulation E's protections.

2. The EFTA does not apply at all to small users that are not defined as consumers, such as small businesses.

Despite its inadequacies, Regulation E does provide consumers many protections. It protects consumers from unauthorized transfers and different types of errors, puts the burden on the financial institution to show that a contested transfer was authorized, protects consumers even if their negligence led to an unauthorized transfer, limits liability (if losses or errors are timely reported) to $50 or nothing at all, has a detailed error resolution regime with time limits, allows for a provisional credit when an error is being investigated, and allows for private enforcement with penalties and attorneys' fees, among other protections. Many of these protections are absent or less robust in the Article 4A provisions that govern electronic payments by businesses.

The protections of the EFTA only apply to a "consumer," defined as a "natural person."[29] But it also only protects transfers from "accounts" that are "established primarily for personal, family, or household purposes, ..."[30] As a result, accounts established in the name of sole proprietorships,

---

[28] Under Regulation E, the term financial institution encompasses nonbank entities like prepaid or debit card account providers that hold accounts or issue access devices and provide electronic fund transfer services.

[29] 15 U.S.C. § 1693a(6).

[30] 15 U.S.C. § 1693a(2).

partnerships, family businesses, Subchapter S corporations, and ordinary corporations have none of the protections of the EFTA.

Yet, small, relatively unsophisticated, users make up the majority of businesses in the United States. Ninety-nine percent of all businesses, or over 30 million, are considered small businesses.[31] The majority of these small businesses have fewer than five employees.[32] Even solo, independent contractors running an Uber service, or providing an in-home day care center – much closer to a consumer than a business – may have a bank account just for their business, or may use their personal account for purposes that are arguably business-related.

Small businesses are subject to the same scams and errors as are consumers. As with consumers, the loss of only one large payment by a small business as the result of an error or fraud could be devastating. It might even cause the failure of the business. The FRB must address this gap in protection for small businesses in the FedNow system.

C. The FRB must protect users from fraud and errors to fulfill its responsibility to ensure that its faster payments system is safe, especially for vulnerable consumers and small businesses.

The FRB should not launch the FedNow service or finalize the Reg J rules until two critical regulatory gaps are filled: protection against fraud in the inducement and against sender errors. Reg J should define fraud in the inducement and sender errors as errors in the FedNow system and require them to be resolved under error resolution procedures. The FRB is creating this system and it has the authority to write the rules for the system regardless of any ambiguities or gaps in Regulation E. The CFPB should separately also clarify that Regulation E applies to these situations.[33]

When losses from fraud or errors are reported, if validated, small users should be reimbursed in the first instance from their bank (the sending bank). If the sender has a valid claim that the payment was fraudulently induced, it should be reversed and the beneficiary or receiving institution should ultimately bear the loss.[34] In the event of a sender error, the sending bank and receiving bank and any other participants in the payment chain should be required to follow the error resolution process and to cooperate to attempt to correct the error. If there is an error found after an investigation, and the beneficiary is not entitled to the payment, then the beneficiary's account should be debited and the funds returned to the sender.

---

[31] *See* Andrew W. Hait, United States Census Bureau, *The Majority of U.S. Businesses Have Fewer Than Five Employees* (Jan. 19, 2021), *available at* https://www.census.gov/library/stories/2021/01/what-is-a-small-business.html.

[32] *See id.*

[33] The CFPB has the authority to define additional errors that are covered by the EFTA's error resolution procedures. *See* 15 U.S.C. §1693f(f)(7).

[34] But, as discussed below, the sender's bank should have the initial obligation to resolve the error and then to recover repayment from the receiving bank. The sender should not be required to deal with the receiving bank. The receiving bank may also be able to pass the loss down the line if funds were transferred a second time.

If the beneficiary that received the funds is a money mule[35] intermediary who was also a fraud victim and transferred funds to the scammer's account at a third institution, the liability should be passed down the chain. The money mule may have transferred the funds to the scammer through a method other than FedNow (cash withdrawals, gift card purchases, etc.), making it impossible to reach the ultimate scammer. But the money mule will be liable to the receiving bank in the first instance, and imposing liability on the receiving institution will create the incentive set up systems that detect and ideally prevent suspicious transactions, such as large and unusual FedNow transfers immediately followed by large cash withdrawals. For example, in the UK, financial institutions are working to implement the Mules Insights Tactical Solution (MITS), a new technology that helps to track suspicious payments and identify money mule accounts.[36]

Some argue that the sender is at fault in both fraud and error situations and as a result, the sender should bear the loss. Yet, for several reasons it would be better policy for financial institutions to bear these losses just as they do with other types of unauthorized transfers and errors.

Making those who design and operate the payment system responsible will provide incentives to innovate and prevent fraud and errors in the first place. The payments industry has the ability to make decisions about how much safety to build into the system and must take responsibility for those decisions. In today's P2P systems, the fraud and error protection that exists in payment systems like the ACH system has been sacrificed in the name of speed (instant v. one business day, with little fraud monitoring), convenience (just a cell phone number or email needed rather than a bank account and routing number or confirmation of small deposits) and ubiquity (anyone can send money to anyone). But those three elements put together add up to a dangerous system for users. Speed, convenience and ubiquity can coexist with safety only if consumers and other small users are protected.

Protecting senders puts more responsibility for fraudulent payments on the receiving bank, whose customer fraudulently received the funds and was not entitled to them. Imposing liability on the receiving institution – even if it cannot recover from its customer – is consistent with their obligations under existing know-your-customer and anti-money laundering obligations to ensure that accounts are not opened with fraudulent identities and that an institution's customers are not using an account for illegal purposes.[37]

---

[35] *See* Lisa Weintraub Schifferle, Federal Trade Comm'n, What's a money mule scam? (Mar. 4, 2020), https://www.consumer.ftc.gov/blog/2020/03/whats-money-mule-scam.

[36] *See* UK Finance, Fraud-the Fact 2021, *supra,* at 55.

[37] *See* Federal Fin. Inst. Examinations Council, Authentication and Access to Financial Institution Services and Systems (Aug. 11, 2021), *available at* [https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf. This and other guidances noted point to a myriad of methods that institutions should be monitoring, and protecting themselves from "high risk users" and potential threats to security, as well as related challenges that can trigger losses.

Financial institutions are in a much better position to bear the losses than are consumers and other small users. If losses from fraud and errors in the FedNow system are within reasonable levels, financial institutions and the payment system can afford to bear and spread the costs. But even a single instance of fraud can be ruinous to a consumer.

While financial institutions are making some efforts to address fraud and errors in P2P services, those efforts tend to fall into one of two buckets: (1) efforts to prevent and identify unauthorized transfers not initiated by the consumer – that is, situations where the institution is liable, and (2) warnings to consumers about the risk of fraud or about the finality of P2P payments, without providing measures to remedy the frauds that do occur. Yet, as is evident from the extensive complaints and individual reports of losses detailed in Section II, disclosures and warnings to consumers are an ineffective method of consumer protection, especially for combatting fraud, since fraudsters deliberately create trust and then abuse that trust.

Rather than hope that vulnerable consumers will protect themselves, a much more effective way to build safe payment systems is to protect consumers and thereby give those designing the system the incentive to use all available tools to make the system safe. In this modern era of big data, artificial intelligence, and machine learning, we know that institutions that bear the cost of losses from fraud or errors are capable of developing sophisticated, ever-improving methods of detecting and limiting those losses. For example, in the UK, one company has developed a system to use behavioral biometrics and to associate lengthy scammer calls with payment activity to counteract push payment fraud.[38] And these loss-prevention systems are far more effective in limiting those losses than simple warnings to consumers.

These changes will benefit everyone in the faster payments ecosystem as they will make the system safer and instill confidence. It is for that reason that in the UK, the largest banks and building societies joined together in a Contingent Reimbursement Model Code (the CRM Code) to protect consumers from fraud in the inducement.[39] Signatory firms commit to:

- protecting their customers with procedures to detect, prevent and respond to APP scams, providing a greater level of protection for customers considered to be vulnerable to this type of fraud;
- greater prevention of accounts being used to launder the proceeds of APP scams, including procedures to prevent, detect and respond to the receipt of funds from this type of fraud; and
- reimbursing customers who are not to blame for the success of a scam.[40]

---

[38] *See, e.g.,* Prove, "Fighting Authorized Push Payment Fraud in the UK" (Aug. 27, 2021), https://www.prove.com/blog/fighting-authorized-push-payment-fraud-in-the-uk.

[39] *See* UK Finance, UK Finance responds to the launch of the Authorised Push Payments Scams Voluntary Code (May 28, 2019), https://www.ukfinance.org.uk/press/press-releases/uk-finance-responds-launch-authorised-push-payments-scams-voluntary-code.

[40] The Contingent Reimbursement Model Code (CRM) Code), https://www.lendingstandardsboard.org.uk/crm-code/.

> Banks and other providers returned to consumers and businesses £206.9 million of the £479 million losses in push payment fraud in 2020.[41] The reimbursements have been funded through an interim compensation fund from the banks, pending a more permanent arrangement.[42]

While helpful, the voluntary nature of the CRM Code may be a reason for the problems that exist with consistent implementation.[43] One recent report describes consumers having trouble getting attention or reimbursements, with decisions being made on an ad-hoc basis.[44] In response, UK Finance, the banks' trade association, recently stated: "we agree that more needs to be done and we firmly believe that a regulated code, backed by legislation, is the most effective answer so that consumer protections apply consistently across the banking industry."[45]

The UK has also designed a method to protect senders when there is error such as discrepancies in the name and/or account number:

> Banks have quietly launched a vital security crackdown to prevent fraudsters intercepting payments. Online bank transfer payments will now be blocked if the recipient's name and account number do not match.
> A box will pop up asking you to check the payee's details for errors—and alerting you to potential fraud. This will happen even if you only enter one wrong letter or use someone's nickname.
> Previously, banks did not check whether the name was correct on a bank transfer. It meant you could put down "Bugs Bunny" and, as long as the right sort code and account number were entered, your payment would go through.
> But that made it too easy to get a digit wrong and send money to a stranger's account. Some customers have struggled to get their money back again after these so-called fat-finger errors.
> Fraudsters also found ways to exploit the loophole, masquerading as Revenue & Customs or a victim's builder or estate agent while giving out their own bank sort code and account number for payment. [46]

---

[41] *See* UK Finance, "Criminals exploit Covid-19 pandemic with rise in scams targeting victims online," *supra.*

[42] *See* UK Finance, Press Release, "Interim funding for APP scam victim compensation to continue to 30 June 2021" (Dec. 9, 2020), https://www.ukfinance.org.uk/press/press-releases/interim-funding-for-app-scam-victim-compensation.

[43] *See* Lending Standards Board, LSB issues warning to CRM Code signatories over Authorised Push Payment (APP) scams (June 16, 2021), https://www.lendingstandardsboard.org.uk/lsb-issues-warning-to-crm-code-signatories-over-authorised-push-payment-app-scams/; Lending Standards Board, "Protecting customers from APP scams: what are the next steps for the CRM Code?" (Aug. 5, 2021), https://www.lendingstandardsboard.org.uk/protecting-customers-from-app-scams-what-are-the-next-steps-for-the-crm-code/

[44] Miles Brignall, The Guardian, Banks failing to properly help victims of fraud, says Which? (Aug. 3, 2021), https://www.theguardian.com/money/2021/aug/03/banks-failing-to-properly-help-victims-of-says-which

[45] *See id.*

[46] Toby Walne, This is Money, *Paying online? Now you'll have to tap in names EXACTLY right…New system to fight fraud means account name must sort code and number* (June 27, 2020), *available at*

The existence of a profitable and competitive credit card marketplace in the United States shows that systems can be developed that protect small users from losses, while still providing ample profit for the providers.[47] With the simple directive to protect consumers against a broad array of unauthorized charges, fraud, and errors – much broader than under Regulation E -- the credit card providers have built a robust system that minimizes losses. That system includes numerous – and constantly improving – mechanisms for the banks involved to spot and catch fraudulent charges. The financial institutions have the ultimate incentive to detect and deter losses: the law requires that they suffer the lion's share of the losses. The exact methods of avoiding the losses are left to the cleverness of the providers. The Fair Credit Billing Act does not explicitly tell institutions providing credit cards exactly how to prevent frauds and other losses; by simply protecting consumers from those losses in most situations, institutions are incented to constantly improve their fraud prevention and monitoring tools.

The FRB, as a public agency, has a public responsibility to ensure that its system is safe, especially for those users for whom fraud or errors can be devastating. The FRB should provide the model for other P2P systems developed by private companies that do not have the same public accountability.

---

https://www.thisismoney.co.uk/money/bills/article-8465903/Paying-online-youll-tap-names-EXACTLY-right.html.

[47] *See* Maya Dollarhide, Investopedia, *Who is Liable for Credit Card Fraud?* (updated July 12, 2021), *available at* https://www.investopedia.com/ask/answers/09/stolen-credit-card.asp. *See also* Federal Trade Comm'n, Lost or Stolen Credit, ATM, and Debit Cards, *available at* https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

D. The FedNow System Should Have a Mechanism for Sending Institutions to Reverse Payments Sent in Error or Due to Fraud.

Beyond legal protection and the right to dispute payments sent due to fraud in the inducement or errors, the FedNow system also needs a mechanism to enable those types of errors to be correctly quickly. The sending institution should have the ability to reverse a payment within a certain period of time without waiting for the receiving institution to respond, agree there is an error, or send the funds back. Payments can still be final in second, but error resolution can be faster too.

When fraud or an error is detected, it is in the interests of all parties for it to be corrected as soon as possible. The more time that goes by, the more likely it is that the beneficiary will have withdrawn or spent the funds. In fraud situations, the receiving institution can avoid liability if the payment is reversed before the scammer disappears. Even in the case of erroneous payments, a beneficiary may innocently spend the funds and have difficulty returning them. Yet waiting for the receiving institution to agree that a payment was in error or due to fraud, and to act on a request to return the funds, will take time. Thus, having a mechanism for the sending institution to correct errors and fraud as soon as possible will minimize the chance that any party will bear a loss.

In the ACH system, for example, in the case of a debit entry sent by an originating depository financial institution (ODFI) to debit an account at a receiving depository financial institution (RDFI), if the RDFI's consumer customer contests the debit as unauthorized, the RDFI may send a return entry (reversing the payment) within 60 days, without agreement by the ODFI.[48] In the case of an erroneous direct deposit or other credit entry sent by an ODFI, the ODFI may send a reverse entry within five days without the RDFI's consent.[49] After five days, the ODFI may send a request for return.[50]

E. The FRB Should Create a Directory and Take Other Steps to Prevent Mistakes and Fraud While Protecting Privacy

While separate from Regulation J, the FedNow system must incorporate methods for financial institutions to access and share information in order to authenticate users, prevent mistakes, and deter fraud.

The FRB should create a central directory to check the consistency of the information provided, such as ensuring that the account number and name match. This will ensure that users are sending funds to the correct person, and that everyone has access to information about an email, cell phone, or account linked to the wrong account or an imposter account.

As the Faster Payment Council has noted—

---

[48] *See* NACHA Operating Rules Section 3.8; NACHA Operating Guidelines Ch. 26, Returns of Unauthorized/Improper/Incomplete Consumer Debit Entries.

[49] *See* NACHA Operating Rules Sections 2.8, 2.9.

[50] *See* NACHA Operating Guidelines Ch. 12, ODFI Requests for Return.

> Both senders and receivers of payments benefit from having a directory pre-validate the routing information for a payment:
>
> - For receivers, this ensures the funds are applied to the correct account.
> - For senders, it provides a level of safety by ensuring funds are being sent to a properly validated account.
> - Both parties benefit as this reduces the need for validation each time a transaction or payment is initiated.
>
> Pre-validating the routing information also benefits financial institutions (FIs) by reducing the number of exception items due to misapplied or unapplied payments.[51]

The Council further stated:

> To encourage real-time payment adoption across the ecosystem, safety and surety are paramount. Validating routing information will help create the confidence necessary to help grow widespread adoption. Both senders and receivers can be confident that funds are being properly routed and applied to the intended account.[52]

As discussed in Section III.B below, the UK confirmation of payee (CoP) model checks information the consumer enters to ensure that payment information is accurate.[53]

Yet a directory and other forms of information sharing also must be set up to protect users' privacy. Access to consumer data should only be permissible to the extent needed for each real time payment transaction, and participants should not be able to use a directory or other shared information for debt collection, marketing or other purposes. The system should subscribe to a "minimum data necessary" principle where solution providers can only request the minimum amount of data they need to perform a requested function.

As a condition of gaining access to the FedNow directory, financial institutions, solution providers (third parties who handle or facilitate payments), and other industry participants should commit to meeting rules establishing a standard set of information sharing. The solution providers and financial institutions involved should provide senders and receivers with effective tools for controlling permission for the content about themselves kept in the directory. Conditions for usage should include providing senders and receivers with the ability to review their information, to make changes

---

[51] *See* Faster Payments Council, Beneficial Characteristics Desirable in a Directory Service at 5 (May 2021) (emphasis added), *available at* https://fasterpaymentscouncil.org/userfiles/2080/files/DMWG%20Beneficial%20Characteristics%20Desirable%20in%20a%20Directory%20Service_05-24-2021%20Final.pdf.

[52] *Id.*

[53] Royal Bank of Scotland. "What Is Confirmation of Payee (CoP) and How Does It Work?" Ask a Question, n.d. https://www.supportcentre-rbs.co.uk/Searchable/1419877212/What-is-Confirmation-of-Payee-CoP-and-how-does-it-work.htm.

(additions, corrections, and redactions), to indicate which account is used to make each individual payment, and to remove any or all of their information from the directory.

The FRB should provide guidance on how banks and third-party solution-providers should design the user experience of information-sharing controls. A consumer should be able to see which accounts are connected to a payment service. End-users should have the ability to make edits to their data from inside their bank account app. If the solution is managed by a third-party intermediary, such as Zelle, then the provider should consider offering a portal or other means for an end-user to review and edit their information and to remove it from the directory. (Though any portal must be designed in a way that it prevents scammers from accessing it, *i.e.,* to redirect payments to a different account.) The portal should give consumers the right to see where their payment details are being shared, set time limits on the duration of the sharing privileges, and revoke permission. For example, if a third-party solution provider connected a real-time payments service to a credit-building tool, then the portal would give the consumer the ability to limit the duration of the sharing to the period of time when the consumer intended to use the credit building service.

Relatedly, the FRB should routinely take the proactive step to verify the accuracy of consumer information held within the directory.

F. The FedNow System Should Require Reporting of Fraud to a Central Database and Permit Sharing of Information to Combat Fraud.

FedNow rules should also require participants to report fraud and should permit the players in the chain of a payment to share information when it can help to combat fraud. A scammer who has defrauded one consumer is likely to have defrauded others. But 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.

Fraud reports should be made not just through suspicious activity reports (SARs). Participants in the payment system, 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 reports.[54] Indeed, FedNow payments may not even reach that size, at least not initially.

The importance of collecting information about fraud is another reason why small users must be protected against fraud in the inducement. If the bank's response to a consumer who calls 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 receiving institution or to others who may be sending money to the same scammer or money mule. It is essential to collect and share as much information as possible about fraudulent actors to keep the system safe.

In its 2019-2022 Economic Crime Plan, the UK Finance Authority called for better information sharing among financial institutions, based on the view that cross-system analysis of intelligence can be more effective at combatting fraud. The UK's Criminal Finances Act of 2017 and the Data

[54] *See* 12 C.F.R. § 21.11(c)(2), (4).

Protection Act of 2018 permitted the processing of personal data to prevent crime.[55] The UK has been developing a secure mechanism to enable firms to share information about confirmed push-payment frauds with a view to enhancing the industry's ability to freeze and repatriate funds.[56]

The FRB should also ensure that participants have access to information about individuals or entities that have been barred for fraud reasons from using the FedNow system. NACHA, for example, has a terminated originator[57] list. Any database, however, must comply with the Fair Credit Reporting Act (FCRA) to the extent that it collects information on consumers that is used, is expected to be used, or is collected in whole or in part for an FCRA-covered purpose.

III. Other Aspects of the Proposed Rules are Problematic

Beyond the lack of sufficient protections against errors and fraud, some of the other specific aspects of proposed Reg J are problematic.

A. Applying UCC 4A to any aspect of FedNow transfers for consumers creates substantial problems.

The proposal applies UCC 4A to 1) all non-consumer transactions to which the EFTA does not apply, and 2) consumer transactions except to the extent of a conflict between 4A and the EFTA. The FRB believes that it is necessary to incorporate UCC 4A in Reg J, even as to consumer transactions, to avoid the lack of "clear and consistent rules":

> "[b]y its terms, UCC Article 4A would not apply to a funds transfer any part of which is governed by the EFTA. Therefore, absent this proposed section in subpart C, a number of important legal aspects with respect to these consumer transfers over the FedNow Service could potentially lack clear and consistent rules." [58]

The FRB does not explain which legal aspects of consumer transfers need clear rules that UCC 4A supplies, which itself leads to confusion. Also as discussed below, to the extent that 4A does supply rules, often they act to the disadvantage of consumers.

Making UCC 4A applicable to consumer transfers will not achieve the goal of applying clear and consistent rules to all FedNow transactions. In many situations, the interplay between Regulation E and 4A will be unclear and confusing. Moreover, because UCC 4A allows changes in the obligations between the parties based on contract, the contracts entered into by consumers will no doubt be adhesion contracts, with different rules imposed by different institutions. These differences will mean not only inadequate protections, but also that the applicable protections will vary between

---

[55] HM Government and UK Finance. July 2019. Economic Crime Plan 2019-2022. Accessed at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf

[56] UK Finance, Fraud-The Facts 2021, *supra*, at 55.

[57] https://www.nacha.org/content/risk-management-portal.

[58] Proposed Rules at 31,378 (Commentary, § 210.40) (emphasis added).

providers. As a result, consumers will not be able to rely on the consistent protections of Regulation J, and, there *will* be a complete dearth of clear and consistent rules.

Beyond inconsistencies, the much more serious problem is the inappropriateness of applying UCC 4A wholesale to consumers without ensuring through a section by section basis that the rules will not disadvantage consumers, lead to confusion, or weaken Regulation E rights. Article 4A was designed for transactions between large, sophisticated parties with equal bargaining power. It was not drafted with consumers in mind, and thus many of its provisions will leave consumers at a disadvantage. Conflicts between Regulation E and 4A may also not always be apparent, and combining two regulatory regimes that were designed to be separate will add confusion. Provisions of 4A may be applied when they should not be, interfering with Regulation E rights.

For example, as noted above, UCC 4A permits the parties to adjust the 4A obligations by contract. Yet consumers who must accept adhesion contracts will have no ability to protect themselves. Thus, they could even lose the few rights they receive under 4A. The EFTA, on the other hand, prohibits its provisions from being waived.

UCC 4A has a provision that allows an unauthorized payment order to be effective (and thus deemed authorized) if the bank and its customer have agreed on a security procedure to authenticate the customer and that procedure is either commercially reasonable or a procedure which is commercially reasonable is offered and declined.[59] That provision conflicts with the absolute Regulation E protection against unauthorized transfers, which is nonwaivable and applies even if the consumer is negligent.[60] As a result, this provision should never be applicable to consumers.

But some may deny that there is a conflict with Regulation E if a bank disclaims responsibility for a payment that could have been prevented had the consumer followed an offered security feature. While allowing the parties to agree to a security procedure that is not commercially reasonable may makes sense for large players who are able to understand the risks involved, and who choose how much security risk to take for themselves across all their own transactions, it is not appropriate for consumers and small users. For example, if an institution wants to avoid the obligation to use a particular security procedure, could it include fine print stating that it was offered and declined? More fundamentally, giving consumers any responsibility for losses due to inadequate security procedures is wholly inappropriate:

- First, consumers cannot spread losses over a broad set of transactions.
- Second, "commercially reasonable" is vague and subject to a case-by-case determination—an expensive process for anyone who wishes to challenge a security procedure. Plus, any caselaw on what is commercially reasonable will be likely to develop only through actions of those parties whose transactions are large enough to be worth litigating—transactions quite different from those of consumers and small users.

---

[59] U.C.C. § 4A-202(b), (c). *See* Stephen C. Veltri & Greg Cavanagh, Survey-Uniform Commercial Code, Payments, 69 Bus. Law. 1181, 100 (Aug. 2014) ("[I]f a bank offers, and its customer refuses, a security procedure that is commercially reasonable for that customer, then the less-secure procedure the customer chooses to follow is treated as 'commercially reasonable.'").

[60] *See* Official Interpretations of Regulation E § 1005.6(b)-2

- Third, Article 4A allows even these standards to be abrogated in the adhesion contracts signed between banks and small users.

In other words, using UCC Article 4A for gap filling would apply an inadequate standard that could not develop further under general principles of law and equity. Other rules providing consumer protections—such as the EFTA[61] or those provided through the Fair Credit Reporting Act[62]—do not permit waiver. To allow waiver for an issue so important as security standards would be completely inconsistent with the basic consumer financial services protections Congress has adopted across a variety of platforms.

Another example of a 4A provision that is inappropriate to apply to consumers, and could cause confusion as to whether it is superseded by Regulation E, is the rule making an originator responsible for the mistakes of third-party communication systems that it uses.[63] That rule may make sense for large, sophisticated parties selecting and vetting their communication systems. But it is unfair to consumers, and it is unclear how that rule might even apply in the modern consumer context – such as a smartphone designed by one party, an app by another, and a financial institution or payment solution that actually transfers the funds. For example, as illustrated in the example about the problems of the fictional Mary in Section II.B.1, *supra*, because of the application of § 4A-206(a) to a bank app's accidental change in the spelling of her last name, would Mary be deprived of a remedy when her funds are deposited in another Mary Smith's account because she chose which smartphone to buy? Would holding Mary responsible for the app's error be allowed because Regulation E is not specific as to communications services, or be viewed as an impermissible waiver of her Regulation E error resolution rights?[64] Would the 4A provision governing communication services even apply to smartphones and apps?

Another place of potential conflict or confusion between Regulation E and UCC 4A – and proposed Regulation J – involves the time frame for resolving errors. UCC 4A has provisions governing unauthorized charges and errors and the duty to restore lost interest due to errors. 4A requires the bank receiving a payment order to credit any interest that would have been due on an amount erroneously withdrawn. However, it need not do so if the customer fails to notify the bank of the relevant facts in a reasonable time, and the parties may specify what is a reasonable time.[65] The FRB has proposed to fix 60 days as a reasonable time.[66] But in some cases, the EFTA gives consumers

---

[61] 15 U.S.C. § 1693*l*.

[62] 15 U.S.C. § 1681b(b)(2)(A); Syed v. M-I, LLC, 853 F.3d 492, 496 (9th Cir. 2017) (FCRA disclosure that included a waiver of liability violated FCRA).

[63] *See* U.C.C. § 4A-206(a).

[64] *See* 15 U.S.C. § 1693*l* (prohibiting waivers).

[65] UCC § 4A-204(a), (b); *id.* § 4A-304.

[66] *See* Proposed Rules at 31,389 (§ 210.43(c): "Review of payment orders. A sender, by sending a payment order to a Federal Reserve Bank, agrees that for the purposes of sections 4A–204(a) and 4A–304 of Article 4A, a reasonable time to notify a Federal Reserve Bank of the relevant facts concerning an unauthorized or erroneously executed payment order is within 60 calendar days after the sender receives notice that the payment order was accepted or that the sender's settlement account was debited with respect to the payment order.").

longer than 60 days to contest errors. In general, in order to invoke the EFTA's error resolution procedures, the consumer has 60 days from the date that the institution sends the periodic statement in which to notify the institution of an error.[67] Even that 60 days from the statement may be different than the 60 days proposed by the FRB, which is 60 days from notice of acceptance of a payment order or of debiting an account. But in the case of prepaid accounts and government benefit accounts, the consumer may have 120 days.[68]

This highlights the problem of applying both 4A and the EFTA, when those rules were designed to be completely separate. Regulation E excludes "[a]ny transfer of funds through Fedwire or similar a similar wire transfer system that is used primarily for transfers between financial institutions or between businesses."[69] Conversely, UCC 4A excludes any fund transfer covered by the EFTA.[70] The two sets of rules were not designed to work together, and no consideration has been given to how or whether they fit together. Doing so will both harm consumers and create confusion for financial institutions.

The Clearing House, which operates the Real Time Payments (RTP) faster payment system, has taken a different approach, not attempting to apply UCC 4A to consumer transfers: "4A will apply to funds transfers made through RTP that do not involve credits or debits to consumer asset accounts as defined in Regulation E. As a general rule, this means that an RTP funds transfer must have both a commercial Sender and a commercial Receiver in order for 4A to apply to the transfer."[71]

That is the better approach. The FRB simply should not take the shortcut of applying UCC 4A to consumers who have very different levels of knowledge, bargaining power, and tolerance for losses than those for whom 4A was designed. Even if such a system works for the FedWire program, that program is for large players, who all have relatively equal ability to negotiate risks.

B. Reg J appears to explicitly anticipate the non-refundable payment of funds to mistaken recipients.

The key features of the FedNow program are both the immediacy and the finality of the payments. As noted in proposed § 210.46, once the participant bank receives the conforming payment, the payment is "final and irrevocable when made." Although, the footnote to this statement allows FedNow participants to implement "procedures to resolve erroneous payment" or attempt to retrieve funds from the beneficiary,[72] as discussed in Section II.B.1, *infra,* financial institutions

---

[67] 12 C.F.R. § 1005.6(b)(3).

[68] *See* 12 C.F.R. § 1005.15(e)(3)(ii), 1005.18(e)(1)(ii).

[69] 12 C.F.R. § 1693a(7)(B).

[70] U.C.C. § 4A-108 cmt. 1.

[71] The Clearing House, Application of Key UCC 4A Concepts and Terms to the Real-Time Payment System, https://www.theclearinghouse.org/payment-systems/rtp/-/media/4b7848d96b6140488ba25360ad94bd06.ashx

[72] Proposed Rules at 31,381 n.5 (Commentary, § 210.46).

generally do not allow consumers to correct their own errors, and in most situations the effort to recover funds is likely to be unsuccessful. Even if the receiving institution is willing to reverse a mistaken transfer, retrieving money from the recipient requires that the money still be in their account.

However, even while establishing a system for immediate and – essentially – final payments, the proposal would turn a blind eye to the payment of the funds into accounts to which they do not belong. This is fundamentally wrong, as it causes the greatest potential for loss to fall on the users of the systems who have the least control over the system.

Proposed section 210.42(a), in reliance on UCC 4A-208, allows a Federal Reserve Bank that receives a payment order from a sender to rely on the number in the order "even if the payment order identifies another bank by name, provided that the receiving bank does not know of the inconsistency."[73] Proposed section 210.42(b), in reliance on UCC 4A-207, allows the Federal Reserve Bank, acting as a beneficiary's bank, to rely on a number in a payment order "even if the payment order identifies another beneficiary by name, provided that the beneficiary's bank does not know of the inconsistency."[74]

So, rather than develop a system that looks for and spots inconsistencies in payment orders to rigorously guard against mistakes and fraud, the proposed regulation would allow the non-recoverable transfer of funds into accounts that do not even match all of the information provided by the sender. This mechanism not only fails to provide the banks with incentives to protect small users from fraud, but it also affirmatively *reduces incentives* that would otherwise exist within the system for participating banks to develop and maintain procedures to detect and protect users against risk of loss from mistake, security breaches, and outright fraud. After all, if a financial institution is not responsible for fixing a problem if it is not discovered, there is no reason to design a system that will catch these inconsistencies in the first place.

The directory discussed in Section II.E above is one method of preventing these inconsistencies. Similarly, if receiving institutions are made responsible for fraudulent payments that they receive, they are more likely to design systems that catch inconsistencies in beneficiary names, which may be a sign of fraud.

Again, the FRB should look to the UK model, which requires a consortium of the largest banks to make a "confirmation of payee" (CoP) before they send funds.[75] The banks recently emphasized that

[73] Proposed Rules at 31,392 (Commentary, § 210.42(a) (emphasis added)).

[74] Proposed Rules at 31,392 (Commentary, § 210.42(b) (emphasis added)).

[75] Payment Systems Regulator, "PSR confirms widespread implementation of name-checking system, Confirmation of Payee" (Jan. 7, 2020), https://www.psr.org.uk/news-updates/latest-news/announcements/psr-confirms-widespread-implementation-of-name-checking-system-confirmation-of-payee/

the CoP system "has improved security, reduced errors and strengthened customer confidence when making a payment to a new payee."[76]

In the CoP system, the consumer enters the bank's sort code, the name of the account holder, the account type, and the account number. Four outcomes can be returned to the sender: the information matches, it is a close match to the actual name, the name does not match, or it is impossible to check the name.[77] CoP has been recognized as a tool that thwarts fraud and mistakes.[78] Additionally, CoP protects the reputation of participating financial institutions. For these reasons, FedNow should have a CoP function. Additionally, consumers should see a consistent interface across all solution providers.

While this system is not as convenient as simply being able to send funds with a mobile number or an email, safety is more important than convenience. The FRB should not allow payments to be deposited into—and potentially unrecoverable from—the wrong account.

C. Proposed Reg J provides inadequate ability to delay acceptance or funds availability for suspicious payments.

As explained in earlier sections, fraud and errors are likely to be a problem in the FedNow system, as they are in other P2P systems, yet neither the proposed rules nor Regulation E provide adequate means of resolving those issues. The unauthorized payments that bedevil traditional payment systems will also be more dangerous due to the speed of FedNow. That makes it all the more critical to prevent payments from being finalized when there are significant red flags of problems.

Yet the proposed rules require the beneficiary's bank to immediately credit the beneficiary's account after acceptance of the payment order, and allow only limited grounds for taking additional time to determine whether to accept the order. The only authorization in the proposed rule for the recipient's bank to delay accepting the payment is if the "has reasonable cause to believe that the beneficiary is not entitled or permitted to receive payment."[79] While the scope of "not entitled or permitted to receive" is not clear, the example given in the commentary is if sanction rules would be violated,[80] a rare and narrow issue. It is not clear if this provision would allow the receiving bank to

---

[76] *See* Letter from Bank of Scotland et al. to Chris Hemsley, Payment Systems Regulator (June 25, 2021), https://www.ukfinance.org.uk/system/files/25June2021%20-%20Letter%20to%20PSR%20on%20behalf%20of%20SD10%20firms.pdf.

[77] UK Finance, Confirmation of Payee (Feb. 21, 2021), https://www.ukfinance.org.uk/confirmation-of-payee.

[78] However, in implementing a confirmation of payee system, the FRB should weigh the benefits against the potential risks for revealing the specific name of the recipient to the sender, which could become a tool for criminals. *See* FICO. "Confirmation of Payee Might Not Stop Push Payment Fraud: Confirmation of Payee Has Some Benefits in Fighting Authorised Push Payment Fraud, but It Also Has Drawbacks. Here Are Six." *FICO/Blog* (blog), October 24, 2018. https://www.fico.com/blogs/confirmation-payee-might-not-stop-push-payment-fraud.

[79] *See* Proposed § 210.44(b)(3).

[80] *See* Proposed Rules at 31,393 (Commentary, § 210.44-(b)(4)).

delay – for an investigation –acceptance of the payment order or to accept the order but delay funds availability in cases of suspected fraud or mistake.

We appreciate the fact that the FRB has requested comment[81] on whether delays should be permitted in other circumstances, and we urge that fraud and errors be added to the list. Without such clear latitude, banks may authorize the settlement of a payment when they have strong grounds to suspect fraudulent activity or other problems. Given the likelihood of problems with a faster payment system, banks must be able – and even required -- to perform various checks to monitor transaction trends for suspicious and out of pattern activity that can be indicia of fraud or errors.

Payment system participants must be permitted to delay funds availability, for reasons going beyond having "reasonable cause to believe that the beneficiary is not entitled or permitted to receive the payment."[82] "Reasonable cause" may also be too high a standard. We suggest that the FRB change "reasonable cause" to "a reasonable suspicion" and add "or that the payment is in error or is the result of fraud" to the list of grounds for delaying acceptance or funds availability.

In addition to a broader standard, the FRB should provide examples in the commentary of situations that would be permissible. For example, permissible examples occasioning a delay in accepting payment could be:

- An account was recently opened online. The account immediately begins receiving a large volume of FedNow payments which are immediately withdrawn at ATMs or through gift card purchases.
- A previous FedNow payment to the account was disputed and found to be unauthorized or in error.
- The account has an unusual pattern of withdrawals, such as simultaneous withdrawals in different states.

These examples, of course, cannot be exhaustive. Financial institutions will develop ever more sophisticated ways of detective fraud and errors, including patterns that may not be apparent today.

We anticipate that this broader discretion to delay payment acceptance will only be used rarely. The vast majority of nonproblematic payments will be processed immediately as envisioned. Even if some payments are slowed down, speed is not necessarily the most important element of a P2P system. If it is successful, FedNow will be a broad, ubiquitous person-to-person payment system that permits almost anyone to pay almost anyone else in ways that cannot be done directly through the card networks or ACH system. But permitting delay when there are concerns is critical to the safety and success of the system.

D. The Proposed Reg J would allow funds to be withdrawn from the sender's account without giving the receiver an enforceable right to funds availability within the promised timeframe.

[81] *See* Proposed Rules at 31,381.

[82] Proposed Rule, 12 C.F.R. § 210.44(3).

The proposed system would allow transfers "in a matter of seconds."[83] As such, FedNow's promises for speedy transfers would raise the expectation for both senders and recipients that the money also would be available to spend or to pay debits in the recipient's account "in a matter of seconds."

However, under the terms of the proposal, neither recipients nor senders could actually enforce the promises of funds availability in seconds. While the rules require the funds to be credited to the beneficiary's account and made available immediately,[84] neither consumers nor other users can depend on or enforce that obligation. Instead, the proposed rules governing immediate payment to the beneficiary state that the rules and related circulars do not create any rights that the beneficiary or any other party may assert against the beneficiary's bank.[85] The rules and commentary make clear that the only enforceable right to available funds would depend on the application of the Expedited Funds Availability Act and Regulation CC.[86]

Reg CC allows electronic payments to be held until the next business day.[87] In some circumstances, such as a transfer at the start of a holiday weekend, rather than the funds appearing in the recipient's bank account within seconds, Reg CC would allow the money to be held up for the balance of the day of the transfer, plus the two-day weekend, and the holiday. For example, a transfer at 9 am on the Friday morning before the Labor Day holiday, could be held until the following Tuesday morning.

Limiting consumers' rights to speedy transfers in FedNow only to the times required by Reg CC deprives consumers of the primary allure and promise of faster payments. Seconds could become four days and the consumer could do nothing about it. This is not immediate. Indeed, it would be false advertising, which would likely lead to significant financial difficulties faced by the parties to the transfers. The funds would be removed from the sender's bank account immediately. The sender would have no ability to unwind the FedNow transaction and send the money through a channel that would actually be immediate.

---

[83] *See* Proposed Rules at 31,380 ("The proposed section also includes a requirement for a FedNow participant that is the beneficiary's bank to make funds available to the beneficiary immediately after its acceptance of the payment order over the service. As noted above, this requirement reflects the fact that an end-to-end transfer over the FedNow Service is intended to be completed in a matter of seconds. Under the proposed section, if a FedNow participant accepts a payment order over the service, it must pay the beneficiary by crediting the beneficiary's account, and it must do so immediately after its acceptance of the payment order.").

[84] *See* Proposed 12 C.F.R.§ 210.44(b).

[85] Proposed 12 C.F.R. § 210.45(b)(2).

[86] Proposed 12 C.F.R. § 210.45(b)(1) (specifying that the EFAA and Regulation CC also govern); Proposed Rules at 31393, Commentary to Section 210-44-(b)(3) (providing an example showing that the beneficiary would not have a claim against a bank if the beneficiary bank accepts an order at 10:00 am but does not make funds available until 5:00 pm, even though the bank failed to satisfy its obligations under the rules).

[87] 12 C.F.R. § 229.10(b).

Consumers and other small users cannot depend solely on enforcement by the bank regulators to protect their rights. Even enforceable rights like those under Regulation E are violated repeatedly. If the immediacy promised by FedNow is not backed up by enforceable rights, it will not be dependable and will not give consumers confidence. The combination of the *promise* to make the funds available to the recipient *immediately* with the *lack of right to depend on that commitment* could make FedNow a risky payment method for people who use it depending upon that promise. If consumers find that FedNow payments leave their accounts immediately, but the payments coming in are still subject to next business day availability, they are likely to feel cheated of the touted benefits of faster payments, undermining confidence in FedNow. Even occasional problems that receive media attention could have repercussions for confidence in FedNow.

There is a simple fix here – the regulation should require that, as a condition of using FedNow, all participating financial institutions should, by contract, promise funds availability of incoming FedNow processed payments at the same time that these rules require the funds to be credited to the account. That will give consumers a contractual right to depend on what they are being promised (subject to the ability to delay funds availability in limited situations as discussed in the previous section).

The FRB and CFPB should also consider whether they have the authority to amend Regulation CC to impose more immediate funds availability rules for FedNow.

E. If international use is contemplated, the rules must conform to the Regulation E right to cancel.

The potential application of these rules to international transfers is unclear. However, if international use is permitted or contemplated, the rules must be revised to allow consumer senders to exercise the right to cancel provided under Regulation E's international remittance rules.

Congress amended the EFTA[88] requiring consumer protections for remittances in a deliberate attempt to provide more protections to all remittance senders. Many remittance senders are immigrants sending money to family members or others in their countries of origin or those of their families. These senders and their families often have low incomes, and protection against errors is especially important to them.

The Regulation E remittance rules add requirements for enforceable disclosures, rights to cancel previously sent remittances, and robust error resolution procedures.[89] As they are part of EFTA, these requirements would apply under the proposed regulation. Under Regulation E, a consumer has 30 minutes to cancel a transfer so long as the transferred funds have not been picked up by the designated recipient or deposited into an account of the designated recipient.[90]

---

[88] 15 U.S.C. § 1693*o*-1, as amended by Pub. L. 111–203, title X, §§ 1073(a)(4), 1084(1), 124 Stat. 2060, 2081 (2010).

[89] *See* 12 C.F.R. §§ 1005.30, 1005.31, 1005.33, 1005.34.

[90] 12 C.F.R. § 1005.34(a)(2) (emphasis added).

But if the consumer exercises their right to cancel, even assuming that the funds have not yet been picked up, it is unclear how the funds will be returned in the FedNow system. The fact that an international bank is involved on the other side could make it especially difficult to obtain cooperation if the sending bank does not have the ability to unilaterally cancel the transfer.

The FRB should either make clear that international use is not permitted by FedNow or should add provisions dealing with this situation to ensure that consumers can exercise their right to cancel. For example, as discussed in Section II.D, the FRB should give sending banks the ability to reverse a payment. Receiving banks also should be allowed to delay funds availability of international remittances for 30 minutes. These changes would provide a method of retrieving the funds and returning them to the consumer.

IV. Conclusion

The existing P2P systems have far too many problems. The FRB must not simply add one more unsafe P2P system to the market. People make mistakes. Machines make mistakes. Fraud exists in the marketplace, and our payments systems will be used by fraudsters. It is both the broader reach of P2P payments and the speed of the faster payment systems that often makes them particularly dangerous to small users.

The FRB must not sacrifice safety to achieve speed. Systems can be created that are both fast and safe: safety can be fully incorporated into the system. But so long as the fraudsters can choose the method of payments, they will gravitate towards the method with the least level of resistance. The system created by the FRB can discourage fraudulent use and protect small users, providing a gold standard for a system that is both safe and fast.

We support the development of a faster payment system by the FRB in order to provide competition and to ensure that all users and financial institutions of all sizes have access to faster payments. However, the system built by the Federal Reserve first and foremost must be safe and give people protection and confidence when using it. Without the essential guardrails built into the system, the users, as well as the financial institutions providing the services, will instead face greater risks from engaging in faster payments.

The public has the right to expect better from a publicly sponsored payments process. The FRB, with the substantial input of the CFPB, should launch the FedNow service only when it includes appropriate and safe protections for all parties involved, especially small users.

Thank you for the opportunity to provide comments on these new rules.

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