February 14, 2022

Submitted to: https://www.regulations.gov
Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: FinCEN-2021-0008, Request for Information Regarding Review of Bank Secrecy Act Regulations and Guidance

The National Consumer Law Center ("NCLC") (on behalf of its low-income clients), National Community Reinvestment Coalition, and National Consumers League appreciates the opportunity to submit comments to the Financial Crimes Enforcement Center ("FinCEN") regarding the modernization of the current Bank Secrecy Act, Anti-Money Laundering, & Counter-Financing of Terrorism (collectively, "AML") regime. **Specifically, we urge greater attention to fraud against consumers who are induced to send payments to scammers. Stronger protections for consumers who are defrauded is the best way to promote more innovative, risk-based approaches to preventing financial scams.**

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* (6th ed. 2018), updated at library.nclc.org.

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.

Payment scams take billions of dollars from consumers through both older and newer payment methods that access deposit accounts. "Bank transfer or payment" is now the top payment method used by scammers to receive funds, and many other types of vehicles for extracting payments from consumers occur through bank accounts. Thus, the Bank Secrecy Act (BSA)/AML regime plays an important role in preventing payment fraud.

We urge FinCEN to:

- In promoting risk-based approaches, consider the risks to individual consumers and families, and not merely whether the risk of a transaction is tolerable for the financial institution or payment system;
- Support liability protection for consumers who are defrauded into sending payments, which will create incentives for financial institutions and payment systems to adopt ever-improving innovative, risk-based approaches to preventing and addressing fraud;
- Enhance the suspicious activity reports (SAR) process to capture the identity of the account and institution that received the fraudulent funds;
- Promote greater fraud information sharing among financial institutions and with regulators, beyond SARs;
- Prioritize safety over speed of transactions to encourage and permit financial institutions to slow down or put holds on transactions in the rare cases when there are significant red flags of fraud;
- Support mechanisms for consumers whose accounts are mistakenly frozen to dispute those freezes, ideally within Regulation E timeframes;
- Conduct more research on payment scams to help financial institutions spot red flags of fraud.

1. **Payment scams take billions of dollars from consumers through both older and newer payment methods that access deposit accounts.**

The Federal Trade Commission (FTC) reported that Americans lost $3.4 billion due to fraud in 2020.[1] Fraud losses in 2021 will be significantly higher: Already in the first three quarters of 2021, $3.967 billion in fraud losses have been reported.[2] Even these numbers underestimate the extent of the loss, as scams are significantly underreported.

---

[1] https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/LossesContactMethods.
[2] *Id.*

Many of these scams victimized older adults, who were targeted by romance scammers, imposters, identity thieves and other fraudsters.[3] While older adults are less likely to report losing money to scams than younger consumers, their losses are significantly higher. Consumers 80 years old and over reported a median loss of $1,300 to fraud in 2020, an amount two to four times the median loss reported for consumers in other age groups.[4]

But consumers of all ages and in all communities are victim of frauds. Two-thirds of the losses reported to the FTC in 2021 were from consumers under the age of 60.[5] Scams often take the last dollar from those least able to afford it and often target immigrants and other communities of color.[6] These communities, already denied or stripped of wealth through discrimination over the centuries to the present day, can least afford to lose money to scams.

Most of these fraud losses involve bank and other deposit accounts. Bank transfer or payment is now the top payment method for frauds reported to the FTC. Other payment methods, including debit card, payment app or service, wire transfer, and check also include payments from and often to bank or other deposit accounts.

---

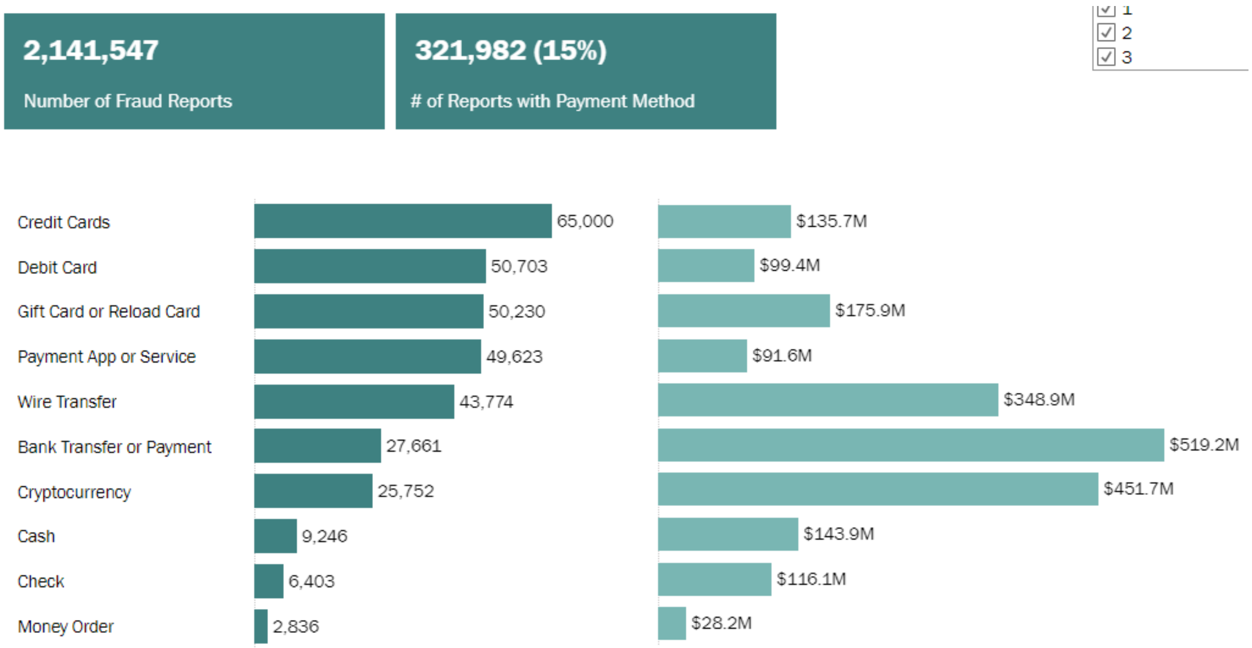
[3] *See* Testimony of Odette Williamson, National Consumer Law Center, before the Senate Special Committee on Aging on "Frauds, Scams & Covid-19: How Con Artists Have Targeted Older Americans During the Pandemic" (Sep. 23, 2021), https://www.nclc.org/images/pdf/special_projects/covid-19/Testimony_Covid_Aging.pdf.

[4] Federal Trade Commission, Consumer Sentinel Data Book 2020, February 2021, at 5, available at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book2020/csn_annual_data_book_2020.pdf.

[5] https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/LossesContactMethods.

[6] Anthony Hill, ABC Action News, "In-depth: Top scams that are targeted against the Black community; how to avoid falling victim; 41% of African Americans say they were targeted by a scam" (Aug. 12, 2021); https://www.abcactionnews.com/news/in-depth/in-depth-top-scams-that-are-targeted-against-the-black-community-how-to-avoid-falling-victim; Josh McCormack, Salud America, "Scammers Target Latinos, Blacks More Than Other Groups" (Aug. 31, 2021), https://salud-america.org/scammers-target-latinos-blacks-more-than-other-groups/; Matthew Petrie, AARP, Consumer Fraud in America: The Latino Experience (Aug. 2021), https://www.aarp.org/research/topics/economics/info-2021/scam-experiences-hispanic-latino.html.

FTC: Fraud Reports by Payment Method Jan. 1-Sept. 30, 2021



There has been a surge of complaints about Zelle,[7] and U.S. PIRG reported on the "explosion of digital wallet consumer complaints in the CFPB's Consumer Complaint Database over the past year."[8]

2. The BSA regime plays an important role in combatting payment fraud.

Any time that a payment is sent from one deposit account to another – whether that recipient account is a traditional bank account at a financial institution, a nonbank deposit account indirectly held at a depository institution, or a prepaid account – the Bank Secrecy Act (BSA) and Anti-Money Laundering Act (AML) regimes are involved. The institutions that open and hold the accounts that receive and disburse payments have duties to know their customer, to verify the identity of the accountholder, and to monitor the account to prevent it from being used for unlawful purposes. These duties encompass preventing accounts from being used to perpetrate fraud, even if accounts are not being used to send funds to terrorists abroad or to launder the fruits of other crimes.

For example, stolen or synthetic identities can be used to create accounts that can receive and quickly dispose of fraudulent funds. As more and more accounts are opened online rather than in

---

[7] Kate Berry, American Banker, Zelle is surprise lightning rod in CFPB's Big Tech inquiry (Dec. 20, 2021), https://www.americanbanker.com/news/zelle-is-surprise-lightning-rod-in-cfpbs-big-tech-inquiry; Bob Sullivan, Red Tape Chronicles, Zelle hackers 'improve' their scam, pretending to be fraud investigators; banks often won't help (Nov. 19, 2021)

[8] 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.

person, it is easier and easier for scammers to create accounts using fake identities. Even if the account identification is accurate, it can become a money mule used as a conduit between the victim and the scammer. Close attention to the authenticity of the accountholder and the activity in the account can prevent, spot and remedy payment scams.

3. Risks that are low from a financial institution's perspective may be high from a consumer's perspective.

FinCEN is seeking to a "risk-based" approach to modernizing the AML regime to ensure "that financial institutions direct more attention and resources toward higher-risk customers and activities, consistent with the risk profile of the financial institution, rather than toward lower-risk customers and activities."[9] But it is important to keep in mind that what is "risky" is a matter of perspective.

A $1,000 payment may not be risky from the perspective of a financial institution. But a $1,000 loss – or even a $500 loss – can be devasting to an individual. At a time when many consumers would not use cash savings or the equivalent to use to cover a $400 emergency expense,[10] the impact of even a single fraud loss cannot be minimized.

A risk-based approach drives choices by financial institutions – choices about which risks to try to prevent and which risks to let slide. Financial institutions make choices every day that impact whether an account can be used to perpetrate payment fraud:

- How to balance the speed and convenience of account opening with identity verification;
- What activity to permit out of a newly opened account;
- Whether to design interfaces or safety measures to ensure that money is going where the consumer intends;
- How to share and consolidate information among financial institutions and check screening agencies;
- How closely to monitor accounts for signs of unusual activities;
- How to respond to consumer complaints about unauthorized or fraudulent charges;
- How quickly to freeze or close an account that may be implicated in payment fraud.

The consequences of these choices should not fall on consumers who cannot afford to bear the risks. In many cases, the financial institutions may be tempted to choose options that favor business needs and revenue maximization over options that result in enhanced safety. It is one thing if the institution ultimately bears the risks; it is another if the choices result in more fraud against consumers that goes without a remedy.

---

[9] 86 Fed. Reg. 71201, 71202 (Dec. 15, 2021).

[10] *See* Federal Reserve Board, Report on the Economic Well-Being of U.S. Households in 2020 (May 2021), https://www.federalreserve.gov/publications/2021-economic-well-being-of-us-households-in-2020-dealing-with-unexpected-expenses.htm#:~:text=When%20faced%20with%20a%20hypothetical,from%202019%20(figure%2017).

4. **Protection for consumers who are defrauded through payment scams will lead to more innovative, risk-based approaches to preventing and addressing fraud.**

Today, when a consumer is defrauded into sending a payment to a scammer through a payment system like Zelle or another push-payment system, the consumer often has little legal protection. The protection under the Electronic Fund Transfer Act (EFTA) against unauthorized transfers only applies to transfers "initiated by a person *other than the consumer*."[11] Consumers who realize they have been defrauded and complain to their financial institution are either told "sorry, you sent the money," or at best the institution requests the funds to be returned by the recipient institution, which refuses.

This approach makes the payment system as a whole less safe and trustworthy, ultimately harming payment providers as well as consumers. Financial institutions and payment system designers have fewer incentives to prevent fraud when they can put the losses on consumers and do not have to take responsibility for the scammers they let into the system or for the choices they make in designing the system and monitoring accounts.

Instead, we have urged the Federal Reserve Board to improve its proposed rules for the coming FedNow payment system to give consumers protection when they are defrauded.[12] We have also urged the Consumer Financial Protection Bureau (CFPB) to amend Regulation E to adopt fraud protection for all person-to-person payment systems.[13] We urge FinCEN to support these protections and to encourage financial institutions to protect consumers even before regulations are changed.

The best way to ensure that financial institutions are adopting innovative and risk-based approaches to financial crimes is to give them the incentive to do so by making them responsible when they allow a scammer to receive funds. Rules that protect consumers will give financial institutions and payment provides the incentive to develop and constantly improve measures to prevent fraud in the first place and to stop it as soon as possible. In this modern era of big data, artificial intelligence, and machine learning, financial institutions and payment systems that take responsibility for fraud will develop sophisticated, ever-improving methods of preventing, detecting and remedying it that are far more effective than warnings to consumers. For that to happen, however, the system needs to

---

[11] 12 C.F.R. § 1005.2(m) (emphasis added).

[12] Comments of 43 consumer, small business, civil rights, community and legal service groups to Board of Governors of the Federal Reserve System re Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021) ("Coalition FedNow Comments"), https://www.nclc.org/images/pdf/banking_and_payment_systems/fintech/FedNow-coalition-comments-final.pdf; Comments of National Consumer Law Center, National Community Reinvestment Coalition, National Consumers League to groups to Board of Governors of the Federal Reserve System re Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021) ("NCLC/NCRC/NCL FedNow Comments"), https://www.nclc.org/images/pdf/banking_and_payment_systems/fintech/FedNowNCLC-NCRC-NCL.pdf; *see also*

[13] *See* Comments of 65 Consumer, Civil Rights, Faith, Legal Services and Community Groups to Bureau of Consumer Financial Protection re: Big Tech Payment Platforms, Docket No. CFPB-2021-0017 (Dec. 21, 2021), https://www.nclc.org/images/pdf/banking_and_payment_systems/payment-fraud/CFPB_Big_Tech_Pay_comments.pdf ("Consumer Big Tech Comments to CFPB").

incorporate incentives for the financial services providers in the payments chain to design robust fraud and error prevention and remediation methodologies.

The benefit to payment providers of protecting consumers is illustrated by developments in the United Kingdom (UK). After launch of faster payment systems led to an explosion of fraud, the largest banks and building societies decided to join together in a Contingent Reimbursement Model Code (the CRM Code) to protect consumers from fraud in the inducement.[14] Signatory firms commit to:

- protecting their customers with procedures to detect, prevent and respond to [authorized push payment (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.[15]

Banks and other providers returned to consumers and businesses £206.9 million of the £479 million losses in push payment fraud in 2020.[16] The reimbursements have been funded through an interim compensation fund from the banks, pending a more permanent arrangement.[17]

While helpful, the voluntary nature of the CRM Code may be a reason for the problems that exist with consistent implementation.[18] One recent report describes consumers having trouble getting attention or reimbursements, with decisions being made on an ad-hoc basis.[19] 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."[20] The UK Payment System Regulator supports mandatory reimbursement and noted that legislative changes will be made by the

---

[14] *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.

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

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

[17] *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.

[18] *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/

[19] 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

[20] *See id.*

government to remove the regulatory barriers that currently prevent mandatory reimbursement for scam victims.[21]

The UK has also designed methods to prevent fraud when there is an error such as a discrepancy 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. [22]

The marketplace will have the incentive to adopt these types of improvements if consumers are protected.

The credit card system is another good example of how protecting consumers results in the incentive to innovate to prevent fraud. The law does not tell institutions how to prevent fraud; it merely protects consumers and incents institutions to constantly improve their fraud prevention and monitoring tools. Thanks to this approach, credit card companies frequently spot fraudulent payments and act to freeze accounts long before consumers realize they have been defrauded.

Today, there is an explosion in the use of p2p services by illicit actors, yet these frauds receive insufficient attention by financial institutions and in AML/BSA activities. Payment scams may be too small to trigger mandatory SARS reports even when they ruin a family. Financial institutions will pay more attention to these scams and adopt risk-based, efficient and innovative approaches to preventing scams if the risks of insufficient KYC and account monitoring fall on the institutions that make those choices.

---

[21] *See* Payment Systems Regulator, APP scams, https://www.psr.org.uk/our-work/app-scams/.

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

5. **FinCEN should update the SAR to catch information about accounts that receive fraudulent funds.**

FinCEN can help in the fight against payment fraud by updating the SAR to encompass information about the accounts used to receive ill-gotten funds. The current SAR form only accommodates accounts related to the reporting institution.[23] In fraud cases where the destination account of the perpetrator is known, reporting institutions relegate the destination account to the narrative. This makes identification and aggregation of the fraudulent activity more difficult for law enforcement.

When a consumer's financial institution files a SARS report following an incident of payment fraud, if the payment was sent through a system – such as a wire transfer, ACH or p2p system – that identifies the recipient, the SARs report should identify the recipient institution and account. Allowing accounts not domiciled at the reporting institution to be reported and designated appropriately would assist FinCEN and law enforcement in identifying, aggregating, and prioritizing fraud investigations to better protect consumers.

Since fraud schemes affect many victims at various reporting institutions, fraud often results in a hub and spoke relationship with one account receiving funds from many different, unrelated accounts. This typology is recognized in the FFIEC Exam Manual[24] and should be supported at FinCEN by enhancing the SAR reporting process to include the fraud perpetrator's account at the receiving institution.

6. **Greater fraud information sharing among financial institutions is also critical.**

In order to prevent and detect payment fraud, it is important to aggregate fraud reports from various sources to detect patterns. Financial institutions and payment system providers must develop tools to aggregate and share information. They will have an incentive to develop those tools if they are responsible for payment fraud, as discussed in the previous section.

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 Protection Act of 2018 permitted the processing of personal data to prevent crime.[25] 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.[26]

[23] FinCEN SAR XML Electronic Filing Requirements: XML Schema 2.0, p. 108. (allowing only 33 – Subject and 41 Financial Institution Where Account Is Held as the only values).
[24] Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, F-2 (2014)
[25] 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.
[26] UK Finance, Fraud-The Facts 2021, *supra*, at 55.

Financial institutions should have access to information about individuals or entities that have been barred for fraud reasons from using Zelle, the FedNow system, the ACH system, SWIFT or CHIPS or any payment system used to transfer funds from bank accounts. NACHA, for example, has a terminated originator[27] 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.

7. **Speed bumps are important: Payments and funds availability should be slowed down when there are red flags of fraud.**

Greater fraud prevention efforts may, at times, slow down payments or funds availability. While faster payments have many benefits, speed should not be at the expense of fraud prevention. A risk-based system – with the risks falling on institutions that can bear them rather than consumers who cannot – can still result in most payments moving quickly, with delays for only those that bear the hallmarks of fraud. A small delay for some consumers is less problematic than the loss of thousands of dollars that families cannot afford.

In our recent comments to the Federal Reserve Board on the proposed rules governing the coming FedNow payment system, we urged the FRB to give financial institutions greater discretion to delay payments or funds availability when such red flags are present.[28] These early red flags may not yet rise to the level requiring a suspicious activity report ("SAR"), but quick action is necessary if fraud is to be addressed, before funds are gone.

Unlike credit cards and the ACH system, P2P payment systems permit almost anyone to pay almost anyone else. While there are advantages to that ubiquity, it also makes it easier for fraudsters to receive payments. In such a wide, open-loop system, permitting financial institutions to delay disbursing payments or funds availability when there are concerns is critical to the safety and success of the system.

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.

8. **Consumers whose accounts are improperly frozen should have a right to Regulation E protections for error resolution.**

When financial institutions react to potential fraud, they sometimes make mistakes. As illustrated by recent events involving Bank of America's unemployment debit cards,[29] Chime's rash of new

---

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

[28] *See* NCLC/NCRC/NCL FedNow Comments, *supra*, at 24-26.

[29] *See* Christina Spicer, Bank of America Froze 350K Unemployment Debit Cards, Alleges New Class Action Lawsuit (July 21, 2021), https://topclassactions.com/lawsuit-settlements/lawsuit-news/bank-of-america-class-action-lawsuit-and-settlement-news/bank-of-america-froze-350k-unemployment-debit-cards-alleges-new-class-action-lawsuit/#:~:text=Actions%202022%20Scholarships-

accounts opened to receive federal stimulus money,[30] and incidents at other institutions, the reaction to fraud is sometimes overbroad, resulting in the freezing of accounts of innocent consumers. In calling on financial institutions to act quickly and take more responsibility for stopping payment fraud, we recognize that information is not perfect and some innocent consumers will be impacted.

Thus, it is critical that consumers have a clear remedy and timeline when they believe their account has been improperly frozen or closed. We have heard too many accounts of consumers whose funds were frozen for weeks or even months on end. The impacted families are often those with low incomes, who simply do not have the resources to wait for their money to be released.

The EFTA and Regulation E provide a clear framework for error resolution that should generally be followed in these situations, and we have urged the CFPB to clarify that Regulation E applies when an account is frozen.[31] A frozen account or refusal to release funds from a closed account should be viewed as an "error" triggering the Regulation E error resolution obligations and timelines. When an account is frozen, the consumer is unable to complete an electronic fund transfer (EFT), whether through an ATM withdrawal, debit card transaction, transfer to another account, or another type of EFT. The transfer of $0 instead of the amount of money the consumer seeks is an "incorrect" EFT and thus an "error" under Regulation E.[32]

Under Regulation E, financial institutions have ten days to investigate and determine whether an error occurred and one business day after finding an error to correct it.[33] They may take up to 45 days to investigate if they give the consumer a provisional credit, which may be reversed if no error is found.[34] These timeframes should generally be sufficient to investigate when consumers complain that their accounts were frozen in error. If the consumer was not involved in fraud, the account should be unfrozen. If the bank has significant evidence showing that the consumer was engaged in fraud, then it can decline to unfreeze the account and should give the accountholder a written explanation of its findings and notice of the right to request the documents that the institution relied on.[35]

Of course, there may be situations when regulators, law enforcement authorities, or AML concerns require a longer hold on funds or prevent the financial institution from revealing to the accountholder/suspected scammer the evidence of fraud. But absent those considerations, especially when the amount of funds is relatively small or the account clearly belongs to a lower income consumer, the Regulation E timeframe should be followed.

,Bank%20of%20America%20Froze%20350K%20Unemployment%20Debit,Alleges%20New%20Class%20Action%20Lawsuit&text=In%20their%20class%20action%20lawsuit,access%20to%20desperately%20needed%20funds.

[30] Carson Kessler, ProPublica, A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money (July 6, 2021), https://www.propublica.org/article/chime.

[31] *See* Consumer Big Tech Comments to CFPB, *supra*, at 4.

[32] 12 C.F.R. §1005.11(a)(1)(ii).

[33] 12 C.F.R. §1005.11(d)(1).

[34] 12 C.F.R. §1005.11(c)(2).

[35] *See* 12 C.F.R. §1005.11(d)(1).

9. **We welcome greater study of payment fraud.**

FinCEN has asked if it should conduct studies or analyze data to ensure BSA reports and records are useful in countering financial crimes. We welcome studies and data analysis, and urge FinCEN to consider ways in which they can shed light on payment fraud methods and help financial institutions counter fraud.

For example, FinCEN could analyze fraud reports to identify patterns or red flags that institutions should be aware of. This could include:

- Types of accounts that are most commonly used to receive fraudulent payments,
- Patterns in how accounts are opened and the activity in new accounts,
- Types of purchases or transfers, such as international transfers, gift card purchases, large ATM withdrawals, or others that should trigger scrutiny.

There are undoubtedly many other ways in which the analysis of fraud reports can help in the fight against payment fraud.

Thank you for considering our views. If you have questions, please contact lsaunders@nclc.org.

Yours very truly,

Lauren Saunders
Associate Director
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 & Fraud
National Consumers League