AMERICA'S CREDIT UNIONS, ANDREW MORRIS

Proposal and Comment Information

Title: Request for Information on Potential Actions to Address Payments Fraud, OP-1866

Comment ID: FR-2025-0036-01-C69

Subject

ACU Comment re: [Docket No. OP-1866] [RIN:3064-ZA49] Request for Information on Potential Actions To Address Payments Fraud

Submitter Information

Organization Name: America's Credit Unions

Organization Type: Organization

Name: Andrew Morris

Submitted Date: 09/18/2025

On behalf of America's Credit Unions, please find attached our comments regarding the interagency notice titled "Request for Information on Potential Actions To Address Payments Fraud " [Docket No. OP-1866] [RIN:3064-ZA49]. Thank you.

Best,
Andrew Morris

[photo-logo]

Andrew Morris
Director, Innovation and Technology
America's Credit Unions

Direct 703 842 2266
Cell
amorris@americascreditunions.org<mailto:username@americascreditunions.org>
americascreditunions.org<https://americascreditunions.org/>

America's Credit Unions

September 18, 2025

Ann Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Jennifer M. Jones
Deputy Executive Secretary
Attention: Comments—RIN 3064-ZA49
Federal Deposit Insurance Corporation,
550 17th Street NW
Washington, DC 20429

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW Suite 3E-218
Washington, DC 20219

RE: Request for Information on Potential Actions To Address Payments Fraud (RIN 3064-ZA49)

Dear Madams and Sirs:

On behalf of America's Credit Unions, I am writing in response to the Request for Information (RFI) titled "Potential Actions to Address Payments Fraud" issued by the Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC)—collectively, the "Agencies." America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the industry to effectively meet the needs of their over 144 million members nationwide.

America's Credit Unions supports interagency coordination, private-sector partnership, and close collaboration with law enforcement to address the growing and persistent problem of payments fraud. Industry reports indicate that fraud losses totaled $132 billion in 2023 and the Federal Trade Commission (FTC) has published data indicating that scams alone cost American consumers $12.5 billion in 2024.[1] The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) has also reported that cyber-related crime contributed to a record $16.6 billion in losses in 2024 and fraud contributed to the bulk of the losses.[2]

[1] Nasdaq – Verafin, 2024 Global Financial Crime Report; FTC, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024" (March 10, 2025), *available at* https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.
[2] FBI, 2024 IC3 Report, 3 (2004).

The FBI and FTC have also noted a surge in investments scams, which have contributed to abnormally high fraud losses among consumers. Often these scams involve cryptocurrencies, highlighting the need for clarification regarding the responsibilities of parties involved in digital asset transactions.[3] Often these scams involve impersonators pretending to work for call centers at cryptocurrency exchanges—but their targets are not limited to any particular industry.[4] Impersonation and call spoofing tactics highlight the fact a significant percentage of fraud lies outside the financial sector and beyond the ability of financial institutions to fully control.

Despite significant investments in fraud detection tools, consumer education, and data security, credit unions report each year that fraud remains a top concern. For smaller credit unions, where the risk of a significant fraud loss could impact the financial health of the institution, there is a sense that if regulatory limits on liability for fraud were to shift, it would be difficult to manage the monetary costs of providing basic banking services like debit cards—particularly in an environment where the Board may be considering further reductions in the interchange rate cap. Credit unions and financial institutions are obligated under the Electronic Fund Transfer Act (EFTA) to reimburse consumers for unauthorized electronic fund transfers. Absent appropriate fraud-related adjustments in Regulation II, the mounting cost of such reimbursements could impair the availability of affordable financial services.[5]

The Agencies should recognize that financial institutions are often limited in their ability to target the root causes of fraud. Criminals can easily adopt new tactics which prey on weaknesses in human judgment or the vulnerabilities present in less regulated parts of the economy, such as online marketplaces. Accordingly, a whole-of-government approach is necessary to effectively combat payments fraud in all its forms, and agencies like the Federal Communications Commission (FCC) and FTC should join the work of the federal financial regulators, under the leadership of the U.S. Department of the Treasury (Treasury), to determine what actions can be taken to stop impersonators.

More generally, an effective strategy to mitigate fraud and improve early warning capabilities should emphasize the use of innovative technology, efficient information exchange, regulatory modernization (particularly for funds availability rules), and consumer education. Although the RFI already suggests an interagency focus, we recommend that future efforts include the Consumer Financial Protection Bureau (CFPB) and the National Credit Union Administration (NCUA) to account for all segments of the financial services industry and ensure that where joint rulemaking is required (i.e., Regulation CC) the appropriate federal agencies are involved.

The collection and centralized sharing of fraud-related information would also aid efforts to develop better tools designed to stop suspicious transactions before they occur. While credit unions already file Suspicious Activity Reports (SARs) with the Financial Crimes Enforcement Network (FinCEN), access to this information is generally limited. As discussed in greater detail

---

[3] *See* FTC, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024" (March 10, 2025),
[4] *Supra* note 2 at 11.
[5] *See* America's Credit Unions Comment Letter re: Debit Card Interchange Fees and Routing (May 10, 2024), *available at* https://americascus.widen.net/view/pdf/38738a24-f35c-4260-ad22-a0c9e67e98ea/Docket-No.-R-1818-ACU-Letter-to-Boad-of-Governors-of-Federal-Reserve-Debit-Interchange-5.10.24.pdf.

below, the development of more comprehensive information sharing safe harbors, directories, and centralized databases for accessing intelligence that agencies and law enforcement possess would improve credit unions' ability to fight fraud.

Question 1 - What actions could increase collaboration among stakeholders to address payments fraud?

Federal financial regulators should take steps to reduce uncertainty regarding the permissibility of sharing information between financial institutions for the purpose of preventing or identifying payments fraud.

Section 314(b) of the USA PATRIOT Act currently provides financial institutions with the ability to share information under a safe harbor that offers protections from liability (e.g., "under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision thereof, or under any contract or other legally enforceable agreement"), in order to better identify and report activities that may involve money laundering or terrorist activities.

The information sharing safe harbor created by Section 314(b) is limited to reports of unlawful transactions involving money laundering or terrorist financing—not general payments fraud. For a transaction to constitute a form of money laundering, it must generally involve one or more specified unlawful activities (SUAs), as described in 18 U.S.C. § 1956, which lists the predicate crimes that apply to a money laundering offense.

A 2020 Fact Sheet issued by FinCEN clarified that in some situations, a financial institution may take advantage of the Section 314(b) safe harbor even if it does not "have specific information indicating that the activity in regards to which it proposes to share information directly relates to proceeds of an SUA."[6] Likewise, a financial institution does not need to have reached a conclusive determination that the activity is suspicious. Instead, according to FinCEN, it is "sufficient that the financial institution or association has a reasonable basis to believe that the information shared relates to activities that may involve money laundering or terrorist activity, and it is sharing the information for an appropriate purpose under Section 314(b) and its implementing regulations."[7] Therefore, a financial institution "can share information in reliance on the Section 314(b) safe harbor relating to activities it suspects may involve money laundering or terrorist activity, even if the financial institution or association cannot identify specific proceeds of an SUA being laundered."[8]

Additionally, FinCEN's fact sheet notes that financial institutions may share information about attempts to engage in transactions that a financial institution suspects may involve money laundering or terrorist financing, including "attempts to induce others to engage in transactions, such as in a money mule scheme." As a result, the shared information could be related to activities that may involve possible terrorist activity or money laundering even if such activities

[6] FinCEN, Section 314(b) Fact Sheet (December 2020), *available at* https://www.fincen.gov/system/files/shared/314bfactsheet.pdf.
[7] *Id.*
[8] *Id.*

do not constitute a "transaction," as defined in 31 CFR 1010.100(bbb). However, the information must still relate to suspected money laundering or terrorist financing, so sharing information about any suspected criminal activity—such as fraudulent check transactions–may be inappropriate unless the credit union suspects the activity could be related to possible money laundering or terrorism.

Given uncertainty about the scope of the safe harbor under Section 314(b) when a transaction does not clearly involve money laundering or terrorist financing, the Agencies should adopt guidance designed to maximize the scope of permissible information sharing to target general financial fraud. To the extent that such guidance depends on corresponding amendments to established data privacy frameworks, such as the Gramm-Leach-Bliley Act (GLBA), we encourage the Agencies to identify and promote legislation that would permit financial institutions to securely share payment fraud information within a legal framework.

In addition to providing the legal framework and standards for data sharing, providing limitations on liability to protect institutions when sharing sensitive data in accordance with the framework and standards would greatly aid in preventing, detecting, and responding to fraud.

Question 2 - What types of collaboration, including standard setting, could be most effective in addressing payments fraud? What are some of the biggest obstacles to these types of collaboration?

Voluntary information sharing between financial institutions, law enforcement, and financial regulatory agencies can be enhanced by promoting the use of consistent taxonomies to describe the various forms of payments fraud. The Federal Reserve has already developed tools to assist in consistent classification by publishing its FraudClassifier and ScamClassifier models.[9] Standardization of fraud terminology could also improve interactions with law enforcement, where investigators may delineate fraud based on differing standards. Partnerships with local and federal law enforcement could also be enhanced by providing training to credit unions on how to package information in a way that is useful for investigation efforts and eventual prosecution of criminals.

Some credit unions report uncertainty about which law enforcement agencies should be the first points of contact depending on the nature of reported fraud (e.g., money mule activity).[10] Differing monetary thresholds for the involvement of certain law enforcement offices has also contributed to uncertainty regarding whether action will be taken on fraud related information that is assembled by credit unions. Standardization of investigational thresholds across jurisdictions (to the extent practicable) and outreach to financial institutions to advise on their applicability would ensure that financial institution efforts to supply law enforcement with actionable information will be guided by appropriate prioritization.

---

[9] *See* https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/; *see also* https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/.
[10] *See e.g.*, Department of Justice, Money Mule Initiative, *available at* https://www.justice.gov/civil/consumer-protection-branch/money-mule-initiative, last updated October 21, 2024.

Financial institutions would also benefit from better processes for sharing customer data breach and identity theft information, including standardized formats and faster communication. Currently, financial institutions face limitations with sharing fraud-related information, and to the extent they do share some information, it is done using a variety of ways. These each present limitations:

- Informal information sharing using peer networks or cold calling is often limited by staff resources and further constrained by conservative assessments of legal liability.
- Paid services offer limited access to fraud data and are not universally adopted.
- SARs rarely result in receiving feedback or shared insights on combatting fraud.
- IC3 is a federal reporting tool but lacks real-time collaboration.

Question 3 - Which organizations outside of the payments or banking industry might provide additional insights related to payments fraud and be effective collaborators in detecting, preventing, and mitigating payments fraud?

Law enforcement and financial regulators should be encouraged to provide meaningful information that can better position financial institutions to combat payment fraud while also protecting due process and privacy rights.

Strengthening collaboration among financial institutions, law enforcement, and regulatory bodies is of paramount importance. Opportunities for improvement include:

- Establishing local and regional fraud task forces to coordinate investigation and recovery efforts and share intelligence.
- Establishing dedicated financial sector liaisons within regional federal law enforcement offices to promote intelligence exchange with industry partners.
- Encouraging membership in organizations like the International Association of Financial Crimes Investigators (IAFCI) to foster industry-wide collaboration.
- Creating secure platforms for FI-to-FI exchange information, including scam data, while protecting PII.
- Expanding and encouraging full participation in the 314(b) Program.
- Encouraging more willingness on the part of financial institutions to report payment fraud to law enforcement authorities, and more willingness on the part of those authorities to take and share responsive action.

Question 4 - Could increased collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?

Collaboration among state and federal agencies and financial institutions would aid financial institutions' ability to combat payments fraud. FinCEN might consider developing dashboards that provide anonymized trend data to trusted financial partners, or developing in-house tools to analyze patterns of financial crime which can be shared with financial institutions to aid in the identification of fraudulent transaction patterns. The FCC should also take steps to work

more closely with Treasury and other financial regulators to prevent call spoofing, a tactic that exploits weaknesses in caller ID to trick consumers into giving up sensitive payment credentials. Recent FTC data reveals a fourfold increase in reports of impersonation scammers stealing from older Americans.[11] America's Credit Unions and other trade associations have called upon the FCC to quickly implement technical standards that would improve defenses against impersonators using spoofed caller IDs; however, greater collaboration between the FCC and financial sector agencies is needed to combat fraud. Today, many financial institutions must rely upon service providers to provide digitally signed (i.e., authenticated) caller ID; however, these services can involve significant cost. The FCC and Agencies should consider policy initiatives to improve access to affordable, digitally authenticated caller ID services for financial institutions that are on the front lines of protecting Americans against robocalling and other impersonation scams. The Agencies should also work with the FCC to gather insights about the sources and patterns of caller ID spoofing to develop effective fraud mitigation strategies and pool shared intelligence.

Question 5 - In general, what types of payments fraud education are most effective, and why? Would different audiences (for example, industry and consumers) benefit from different types of payments fraud education?

Credit unions report that where a member has fallen victim to a payment fraud scam, the ideal response is to provide outreach on an individual basis with examples of how to recognize and avoid similar situations in the future. Consumers who are victims of fraud sometimes report that shame or embarrassment prevents them from reaching out to their financial institution to ask what they might have done differently to prevent loss of funds. Consumer education should be presented in a way that helps to overcome this stigma.

Credit unions often provide resources and tips for avoiding future payment fraud scams. However, such personalized education is not scalable and typically occurs after the member has already fallen for a scam. Many financial institutions have explored just in time intervention, such as push notifications, to alert members of suspicious account or transaction activity; however, these systems are not a substitute for sound judgement and the exercise of caution.

Increased and sustained public messaging from trusted sources involving multiple media channels would be useful in educating consumers on how to better protect themselves from payment fraud scams.

Question 6 - Would additional education informing consumers and businesses about safe payment practices be helpful to reduce payments fraud and promote access to safe, secure payment options?

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

Treasury should consider developing official materials for credit unions and other financial institutions to share that promote the benefits of direct deposit arrangements for receiving payments. As Treasury prepares to reduce disbursements of physical checks, an opportunity exists to remind consumers—particularly older Americans—that receiving checks by mail involves greater risk.

Question 7 - Which approaches could make existing payments fraud education more effective? For example, would targeting outreach to particular audiences or conducting additional education in collaboration with other key stakeholders be effective?

Federal partnerships with agencies such as the FCC and FTC would be helpful in terms of promoting awareness of common scams and criminal tactics which propagate on platforms that credit unions and financial institutions do not control. For example, online marketplaces should be encouraged to advise users of common scam tactics and warn against the use of payment instruments (e.g., checks) that could increase susceptibility to fraud.

Question 8 - Are current online resources effective in providing education on payments fraud? If not, how could they be improved?

Online advisories concerning fraud are most effective when they are seen at the right time by the consumer. In many cases, the ability to interject time critical information about the risks of a particular transaction will be limited because credit unions do not control online commerce platforms, check-out pages, or apps that support peer-to-peer (P2P) payments. On these platforms, which are typically operated by nonbanks, consumers should be given salient information about the entity or person they are preparing to pay (e.g., age of account, ratings, complaints, etc.) along with brief information about common criminal tactics, such as confidence or romance scams.

Question 9 - What potential changes to regulations (apart from the Board's Regulation CC, discussed separately below) could address payments fraud and mitigate the harms from payments fraud to consumers, businesses, and supervised institutions?

Credit unions would benefit from greater regulatory clarity over parties responsible for payments fraud and liability, especially for electronic transfers. For example, updated commentary to Regulation E could clarify how digital asset transactions are evaluated in terms of error resolution obligations. Additional guidance could also help credit unions understand the scope of financial institution, consumer, or issuer liability for unauthorized transactions involving new forms of money, such as stablecoins. Such clarification would be useful as Congress considers legislation that might classify certain digital assets as neither securities nor commodities. A legislative framework that follows such a classification scheme[12] could potentially complicate the applicability of certain definitional exceptions under the EFTA, one of which states that an electronic fund transfer is not a transaction for the purchase or sale of a security or commodity.[13]

[12] *See e.g.*, The Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) Sec.2(22).
[13] *See* 12 USC 1693a(7).

However, the recommended vehicle for any substantive clarifications under Regulation E should be a formal notice of proposed rulemaking instead of issuance of an interpretative rule.[14]

Question 10 - The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payments fraud detection, prevention, and mitigation. Is existing supervisory guidance related to payments fraud sufficient and clear? If not, what new or revised supervisory guidance should the Board, FDIC, and OCC consider issuing on this topic within the respective authorities?

Financial institutions would benefit from guidance issued to broaden the types of data that may be shared between financial institutions, and under what circumstances, to combat payments fraud.

Financial institutions would benefit from more flexibility in funds availability and provisional credit requirements for both checks and electronic transactions. The existing regulatory frameworks could be enhanced to increase flexibility for financial institutions to detect fraud before suffering losses. If time frames for provisional credits or balance adjustments under Regulations E and Z respectively were relaxed in order to give institutions more time to better investigate payments fraud claims, they would be better positioned to prevent the withdrawal of fraudulent funds prior to completion of the investigation.

Additionally, financial institutions would be better equipped to protect consumers from harm if given legal authority and protection from liability when acting in good faith to decline services to protect members from fraudulent actors, e.g., declining to complete a customer's requested transaction that presents clear indicia of fraud or elder abuse. Currently the FTC maintains a list of state laws governing financial holds relevant to cases involving elder financial exploitation.[15] The Agencies should consider hosting this reference as a regularly updated resource, and should expand its scope to any other state legal laws that would either permit or require a financial institution to hold funds or report suspected fraud.

Question 11 - How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payments fraud?

As noted previously, guidance focused on information sharing would be helpful to promote industry collaboration. Likewise, efforts to improve communications and cooperation with law enforcement through the development of guides or best practices could help improve prosecution of financial crimes.

---

[14] *See* America's Credit Unions, Comments re: Electronic Fund Transfers Through Accounts Established Primarily for Personal, Family, or Household Purposes Using Emerging Payment Mechanisms (CFPB-2025-0003) (March 31, 2025), *available at* https://americascus.widen.net/view/pdf/77baf3de-bf73-4e39-8409-39f52116f313/ACU%20Comment%20Letter%20CFPB_RegE%20Interpretive%20Proposal_3.31.25_final.pdf.

[15] *See* FTC, Financial Institution Transaction Holds (October 2024), *available at* https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/FinancialInstitutionTransactionHoldsStateOverview.pdf

However, small credit unions and community financial institutions must often contend with limited resources. The acquisition of commercial analytics (e.g., AI based tools), tokenization schemes, or sophisticated heuristics to monitor consumer behavior is not always a viable strategy for contending with the asymmetrical tactics of criminals, particularly when budgets and staffing must be balanced with the mission of providing affordable financial services. With these limitations in mind, the Agencies should ensure that any enumeration of best practices to prevent or detect fraud does not constitute a mandate to adopt specific technical solutions. The Agencies should ensure that any future guidance is tech-neutral and appropriately tailored to the complexity and activities of individual financial institutions. A one-size-fits-all approach for achieving policy objectives rarely serves the best interests of financial institutions or consumers.

Question 12 - What is the experience of consumers and businesses when supervised institutions place holds on depositors' funds because of suspected payments fraud?

Consumers benefit when their respective financial institutions set clear expectations and timelines for resolving account freezes, holds, or disputes as much as possible. For example, customers respond positively when they are informed how long the recovery and claims process will generally take, what documentation is likely to be needed, and when they can expect resolution. Such information helps manage anxiety and builds confidence in the financial institution. However, the ability of financial institutions to meet these expectations and timelines often depends on the cooperation and timeliness of other financial institutions.

Delays in responding to requests for verification or information, refusals to honor valid payments fraud claims, and the inability to obtain hold harmless letters frustrate a financial institution's ability to resolve fraud concerns and disputes in a timely or satisfactory manner. Regulators should consider whether a financial institution's refusal to reasonably cooperate when presented with a good faith fraud inquiry about a fraudulent transaction should bear upon its liability, particularly in cases where there may be shared responsibilities under the EFTA and Regulation E.[16]

Additionally, consumers expect transparency as to why a fraud claim has been denied or why their accounts have been restricted. Under existing Regulation CC, an explanation of why funds were held and when they will be made available for withdrawal must be provided when exercising an exception to delay funds availability.[17] The existing notice requirement generally provides adequate information to consumers; however, a more flexible approach for documenting why a financial institution has reasonable cause to doubt collectibility would be useful (see comments to question 15).

---

[16] For example, certain pass-through transactions involving the funding of a digital wallet can result in both the institution holding the wallet account and the institution holding the account providing the funds both being liable under Regulation E. *See* CFPB, Electronic Fund Transfer FAQs ("[I]f an entity, including a non-bank P2P payment provider, enters into an agreement with a consumer to provide EFT services and issues an access device, and initiates a debit card "pass-through" payment, then that entity would be covered as a financial institution under Regulation E"), *available at* https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/.

[17] *See* 12 CFR 229.13(g).

Question 13 - The Board, FDIC, and OCC have received complaints from supervised institutions regarding challenges in resolving disputes about liability for allegedly fraudulent checks. What is the experience of supervised institutions when trying to resolve these types of interbank disputes regarding allegedly fraudulent checks?

Not all financial institutions possess the same capacity to provide timely responses to check and electronic fund transfer fraud inquiries from other financial institutions. Some credit unions report difficulty obtaining hold harmless letters or receiving acknowledgment of inquiries about specific transactions that may be fraudulent. Adopting appropriate safe harbors to encourage cooperation among financial institutions and providing model hold harmless letters would alleviate some of the causes of interbank disputes. Similar actions could also help address cases of wire fraud.

Additionally, financial institutions would benefit from regulatory guidance regarding due diligence and good faith in handling claims of fraudulent funds. Some credit unions report that financial institutions will make unfounded counter claims of counterfeit checks to deny alteration claims. The Federal Reserve might consider conducting a survey of its supervised institutions to determine how often such counterclaims are made and how often they result in liability shifting from a depositary bank to a drawee bank.

Question 14 - Regulation CC seeks to balance prompt funds availability with the risk of checks being returned unpaid for reasons that include fraud. What potential amendments to Regulation CC would support timely access to funds from check deposits while providing depository institutions with sufficient time to identify suspected payments fraud?

For more than a decade, annual check volume has been in decline relative to electronic alternatives such as ACH and card payments. From 2018 to 2021, the Federal Reserve reported that the total volume of consumer checks declined at a rate of 9.3 percent per year.[18] At the same time, the value of noncash payments in the United States grew faster from 2018 to 2021 than in any previous Federal Reserve measurement period since 2000.[19]

Despite declining volumes, the value of check payments has increased, and consumers still use checks to pay a variety of bills such as rent and utilities. As long as checks remain in usage, credit unions must comply with the funds availability rules under the Expedited Funds Availability Act (EFA Act) and Regulation CC while maintaining vigilance against the fraud risks inherent to check processing. However, current check regulations are outdated and badly in need of modernization to prevent continued exploitation by criminals.

Credit unions report that check fraud has increased in recent years and industry reports estimate the total value of check fraud losses exceeded $21 billion in 2023.[20] Reports from the U.S. Postal

[18] Federal Reserve, *Depository and Financial Institutions Payments Survey* (CY 2021), available at: https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm.
[19] *Id.*
[20] Nasdaq Verafin – 2024 Global Financial Crime Report.

Inspection Service indicate that the U.S. Postal Service (USPS) recovers over $1 billion in counterfeit checks & money orders each year.[21] Other USPS reports have drawn attention to checks being stolen out of mailboxes, including the theft of U.S. Treasury checks, which are generally granted next-day funds availability when deposited.[22]

Regulation CC should be modernized to better address check fraud that takes advantage of check processing vulnerabilities and limitations on hold times. Common schemes—such as check washing and the use of counterfeit cashier's checks (along with other items which grant faster access to funds) remain significant concerns. Adopting greater flexibility under Regulation CC's hold provisions would give credit unions more time to determine if a check is counterfeit or fraudulently presented. Likewise, updating rules to grant financial institutions greater discretion with respect to high-risk checks, such as cashier's checks, could help prevent abuse of funds availability requirements—although this may require legislative intervention.

Regulation CC's current framework often imposes unnecessary risk on credit unions and their members by not providing sufficient time to verify check authenticity or confirm available funds. Accordingly, funds availability requirements for checks, including those deposited in non-proprietary ATMs, should not be shortened. Shortening the funds availability requirements would most certainly increase fraud losses by financial institutions, which are already significant—owing both to the many and various types of fraud and delay caused by untimely responses to fraud inquiries.

Question 15 - Regulation CC provides six exceptions that allow depository institutions to extend deposit hold periods for certain types of deposits, including deposits for which the depository institution has reasonable cause to doubt the collectability of a check. Is this exception effective in allowing depository institutions to mitigate check fraud while also allowing timely access to funds?

Financial institutions would benefit from a more flexible interpretation of Regulation CC's reasonable cause to doubt the collectability exception. There are two components to this exception which the Federal Reserve should consider. The first component relates to the reasons for doubting an item's collectiblity, which can be numerous and complex. Because of this, the requirement in 12 CFR 229.13(e)(1) to include the bank's reason for believing that the check is uncollectible in the notice required under 229.13(g) can pose great challenges. Credit unions report difficulty in scaling systems when attempting to generate meaningful and understandable reasons for invoking the exception—a difficulty that reflects the fact that checks are often processed using systems with multiple data points which are subject to complex multi-factored analysis. Explaining the finer points of such analysis to comply with notice requirements could reveal proprietary fraud detection methods to criminals and inadvertently lead to the development of new evasion tactics.

[21] *See* https://www.uspis.gov/news/scam-article/check-washing.
[22] *See* https://www.uspsoig.gov/investigative-work/case-highlights/taking-down-24m-check-theft-conspiracy.

Financial institutions would benefit from greater flexibility in determining when this exception may be invoked, such that the permissible bases may, under appropriate circumstances, extend to the type and/or amount of the check and the history of the depositor.

The other component of the exception relates to the length of time that funds may be held, which is defined in the EFA Act as a "reasonable period," which is subject to the Board's interpretation. More flexibility regarding the length of extended holds (i.e., the reasonable period) that applies to checks under this exception would be helpful in investigating fraud. Five business days is often insufficient time to determine the collectability of a check. The Federal Reserve has not attempted to conduct a representative survey of the sufficiency of existing holds times under Regulation CC since its Report to Congress on the Check Clearing for the 21st Century Act of 2003. Notably, the 2003 Report concluded that advances in technology and regulatory changes leading to an overall reduction in return times were not sufficient to enable banks to receive "most" (i.e., two-thirds) of the returned checks from any category of check before they were required by law to make funds available.[23] If the Board doubts the necessity of extending permissible hold times by revising its interpretation of a "reasonable period," it should consider conducting a new survey to determine what share of checks are returned unpaid after funds must be made available when the maximum permissible hold is placed on the deposit.

RFI Question 16 – Broadly, how could payments fraud data collection and information sharing be improved?

The Agencies should work to promote financial institution access to real-time data that can be used to prevent fraud before it occurs. Currently, not all financial institutions participate in payment networks that facilitate real time information exchange, and not all financial institutions can afford such access. Better partnerships with private sector and public sector actors are needed to reduce costs and promote voluntary participation. Government sponsored data sharing standards for elements such as consistent labeling and file types could incentivize broader participation. Similarly, definitions of various types of fraud could be standardized to assist in tracking, reporting, and response.

Better mechanisms are needed for reporting fraud among all stakeholders and for maximizing the accuracy of such reporting. Guidance from regulators on the proper means of contacting customers affected by fraud and the contents of such notices may be beneficial. Efforts to make victims whole by following the money trail to gain recovery for the victim would meet with greater success if there were better data sharing among financial institutions and between government agencies and the banking industry.

One increasing area of payment fraud is P2P platforms. More attention aimed at increasing the robustness of fraud detection and data sharing and reporting regimes associated with these platforms is welcome.

[23] *See* Board of Governors of the Federal Reserve System, 2003 Report to Congress on the Check Clearing for the 21st Century Act, 15 (April 2007).

Legal complexities and liability currently surrounding data sharing could be reduced by 1) implementing a safe harbor framework to protect financial institutions when sharing sensitive data to combat fraud, and 2) standardizing information sharing protocols, allowing for increased visibility of data across financial institutions.

The Agencies should also consider how commercial entities outside the financial sector can aid in a broader strategy to combat fraud. While financial institutions possess relevant information that can be used to detect and track fraud, many scams originate outside of credit unions, leveraging platforms that have few, if any, reporting obligations because they do not transmit funds (e.g., dating apps). Likewise, merchants are often able to observe fraudulent patterns, such as large volume purchases of gift cards, but may not be required under federal law to report unusual sales activity to law enforcement or federal agencies. The Agencies should strengthen partnerships with federal law enforcement agencies to develop recommendations that will help address fraudulent activity that financial institutions alone cannot control and which may be easier to thwart through a multi-sector approach.

Question 17 – What barriers limit the collection and sharing of payments fraud data between industry stakeholders, and how could these barriers be alleviated? For example, have specific barriers limited development of solutions or participation in bilateral or multilateral payments fraud data collection and information sharing? What changes would address these barriers?

Concerns around the legality of sharing individual financial information is often the primary barrier which limits voluntary information sharing between financial institutions and regulators. As noted in the response to question 1, existing legal safe harbors are not comprehensive and do not cover instances of general financial fraud. Accordingly, the Agencies should work with Congress to develop appropriate legislative language to either expand the existing safe harbor under Section 314b of the PATRIOT Act or develop a new set of exceptions under the GLBA to facilitate the secure exchange of fraud related information.

The limited resources of individual institutions also present a barrier. Not every fraud department will have the same capacity to field calls from other financial institutions or provide detailed analysis regarding a specific transaction. Likewise, not every institution will have the ability to curate data-rich repositories of transactional data to support advanced analysis. To improve financial sector capacity to participate in voluntary information sharing programs or associations, the Agencies should develop recommendations for Congress to consider that would expand funding and eligibility for technical assistance grants. New grant programs could improve fraud fighting capabilities at smaller credit unions and other community financial institutions by helping to fund data quality improvements and the staff necessary to manage robust information sharing programs.

Question 18 - What role should the FRS, FDIC, or OCC take in supporting further standardization of payments fraud data? For instance, can the FRS better leverage or improve the FraudClassifier and ScamClassifier models?

Promotion of the FraudClassifier and ScamClassifier models would help improve the consistency of data sharing efforts. The Agencies should consider hosting workshops and other training events to develop and encourage financial institutions' use of shared frameworks, standards, and definitions that are consistent across agencies. The Agencies should also socialize fraud and scam taxonomies with law enforcement to improve utilization of financial institution data that follows a standard format.

A guiding principle in the development of any standard fraud taxonomy should be to prioritize the data's usefulness to entities capable of stopping financial crime rather than those interested in compliance-focused supervisory data collection. Credit unions have a vested interest in seeing the successful prosecution of financial crime and already collect data to aid in this objective; however, it is sometimes unclear if regulatory terminology or legal distinctions used to describe specific fraudulent transactions are useful to law enforcement. The Agencies should seek to convene working groups of federal law enforcement agencies and individual financial institutions to improve understanding of what information best aids prosecutorial efforts.

Question 19 - What types of payments fraud data, if available, would have the largest impact on addressing payments fraud? If these data are not currently being collected or shared, what entities are best positioned to collect and share such data?

One of the most impactful opportunities in stopping payments fraud is having real-time insight into payments fraud activity across other financial institutions. Some of this data may be available in the form of SARs or reports transmitted directly to local or regional law enforcement offices. The synthesis of such information to create a shared intelligence pool could help alert financial institutions to ongoing fraud activities, patterns, and actors, improve early detection capabilities, and help stop fraud before it occurs.

Question 20 - Is there a need for centralized databases or repositories for the sharing of payments fraud data across entities? What legal, privacy, or practical risks and challenges could such a centralized database or repository pose? Which entities are best positioned to develop and participate in a centralized database or repository?

Centralized databases could facilitate faster and more efficient information exchange; however, the collection of fraud data should be pursued to the greatest extent possible on a voluntary basis. The Agencies should explore a no-cost model for end users of any centralized database which incentivizes voluntary submission of fraud information (conditioned on the applicability of legal safe harbors) in exchange for access. Currently there is limited standardization of payments fraud labeling across institutions. Centralized clearinghouses or databases that can ingest existing data sources while automating the labeling process (potentially through the use of AI)

could improve the quality of industry data and coordination among institutions, law enforcement, and regulatory agencies.

Ideally, a central database would be maintained by a coalition of financial sector agencies and law enforcement to provide the greatest level of threat awareness. The Agencies should also ensure that any data submitted voluntarily to a centralized database is used to prevent and detect fraud and not for other supervisory purposes.

The Agencies should also consider developing a federated directory of trusted fraud contacts which could be used by financial institutions to contact each other to share information or ask questions about fraudulent transactions. The Federal Reserve's "Exception Resolution Service" is an example of how establishing a dedicated communication channel to resolve disputes or questions about specific FedACH or FedNow transactions can save time and enhance coordination.[24]

Question 21 - How can the Reserve Banks enhance their existing risk management tools and services, operations, rules, or procedures to better meet the needs of participating financial institutions in addressing payments fraud? For example, should the Reserve Banks consider requiring fraud reporting for payment rails (as they already do for the FedNow Service) or adopting any particular payments fraud standards?

To better support fraud prevention across the financial ecosystem, the Federal Reserve Banks could:

- Establish trusted contact directories to promote information sharing, enabling faster fraud detection and response.
- Implement secure PII confirmation protocols for both sending and receiving institutions.
- Incentivize consumers to transition away from physical checks, which remain a high-risk payment method vulnerable to theft and alteration.[25]
- Adopt more flexible standards for financial institutions invoking the reasonable cause to doubt collectibility exception, including less prescriptive documentation requirements.
- Adopt a new interpretation of "reasonable period" under Regulation CC's hold provisions for the purpose of granting financial institutions additional flexibility when reviewing deposits for potential fraud.

Question 22 - Are there risk management tools or services that the Reserve Banks should consider offering or expanding, such as (a) developing a payments fraud contact directory for financial institutions, (b) offering tools that can provide notification of atypical payment activity, or (c) introducing confirmation of payee services to help mitigate fraudulent payment origination?

---

[24] *See* Federal Reserve Financial Services, Exception Resolution Service now includes FedNow® Service transactions (September 15, 2025) *available at* https://explore.fednow.org/explore-the-city?id=3&building=news-center&postId=94.
[25] *See e.g.*, Federal Reserve Financial Services, FedNow® Service powering instant payments for disaster relief disbursements (September 17, 2025), *available at* https://explore.fednow.org/explore-the-city?id=3&building=news-center&postId=93.

Credit unions have expressed positive support for request for payment features deployed with the FedNow Service, which can provide an extra layer of confidence that a payment will reach its intended recipient. Credit unions are also supportive of Federal Reserve efforts to explore the creation of a directory service for FedNow, which would not only improve consumer access to real-time payments, but could help improve coordination between individual financial institutions that can use directory information (e.g., aliases such as phone number, email, address) which could help flag accounts used by criminals.

Question 23 - What types of payments fraud have most impacted your organization and its stakeholders? What tactics have criminals employed when perpetrating these types of payments fraud?

Today's prevalent payments fraud spans a wide range of products and tactics targeting individuals, business customers, and financial institutions. Key threats that have impacted credit unions include:

- Romance scams
- Check fraud (stolen, altered, kiting)
- Late check returns
- IRS refund and Treasury-related fraud
- ACH and card transaction fraud
- Breakout schemes involving synthetic identities
- In-person deposits involving instant withdrawals
- Business email compromise
- Impersonator fraud (criminals claiming to be financial institution representatives, government representatives, or other third parties who may have commercial relationships with consumers)
- Wire fraud
- Personal and business identity theft
- Lending fraud
- Credit card fraud
- Loan fraud

Advances in technology, such as artificial intelligence, have made impersonation scams particularly dangerous, with criminals now having access to tools that can cheaply recreate a person's voice and appearance. Consumer behavior, legal liability rules, and economic conditions have also favored an environment where some consumers have a false sense of security, and criminals are emboldened to exploit the limits of regulatory frameworks which allocate responsibility for fraud. Recent criminal tactics include:

- Increased use of money mules to move stolen funds and obscure the fraud trail.

- Exploitation of faster payment systems, where fraudsters take advantage of limited time for detection and reversal.
- Rise in scams, including social engineering and phishing, often targeting vulnerable individuals and businesses.
- Use of social engineering tactics to intimate, coerce or manipulate victims, increasing their susceptibility to fraud.
- Friendly fraud, where chargebacks are initiated based on false claims of undelivered goods.

Question 24 - What measures, including technological solutions or services, have been most effective in identifying, preventing, and mitigating payments fraud at your institution? Are there actions that consumers can take that help institutions? For example, do financial institutions find it helpful when consumers alert the institution in advance when making large purchases, transferring large amounts of money, and traveling abroad?

While no single technology can defeat fraud in every instance, primarily due to the fact that no technology can completely compensate for poor consumer judgement or lack of care in managing personal financial security, access to real-time data tends to have the greatest defensive benefit. The Agencies should explore incentives and programs to make real-time fraud data available to all financial institutions.

Credit unions have also noted that cloud-based tools can improve scalability, data management, and system integration across platforms for the purpose of orchestrating fraud detection services. Emerging technologies (e.g., AI, biometrics) can also play significant roles in fraud prevention going forward and regulatory guidance issued by the Agencies should aim to ease adoption of these new technologies rather than create supervisory friction. The Agencies should consider hosting workshops of financial institutions to identify best practices around deployment of innovative anti-fraud technologies with the aim of improving industry understanding of how these tools can be integrated into core environments.

Question 25 - To the extent not already addressed here, are there other actions that would support stakeholders in identifying, preventing, and mitigating payments fraud?

Regulation of the various payment channels is accomplished by several regulations, promulgated by different agencies (Regulation CC, Regulation E, Regulation Z, etc.)—each with its own requirements for addressing payments fraud. Some rules governing certain payment methods are promulgated by associations, networks, or vendors. What may be the proper course of action for a financial institution to take when it identifies or receives an allegation of fraud by a customer or another institution in one payment channel may not be correct when the fraud is alleged or is found to have occurred in another. For example, the timelines for responding to suspicions, allegations, or findings of fraud can vary depending on the type of check or payment method involved.

While flexibility is required to address the myriad methods used by fraud perpetrators and types of victims, maintaining several response frameworks to comply with the several different funds availability, fraud, and dispute claims schemes present unnecessary cost and complexity to preventing, investigating, and mitigating payment fraud. To the extent possible, the regulations and rules should be evaluated to look for opportunities to align on timeframes, process, and liability, commensurate with the risks associated with particular payment methods.

The Board should also take steps to ensure that its implementation of Regulation II properly accounts for the cost of mitigating payments fraud. A recent court decision has called into question the Board's ability to incorporate in its debit interchange cap formula an ad-valorem adjustment for fraud losses.[26] The Board, and the Agencies, should recognize that any reduction in the debit interchange cap will have a negative impact on financial institutions' ability to fund strong anti-fraud programs as part of their debit card offerings. Furthermore, credit unions are less able to absorb reductions in interchange revenue. Due to their unique, not-for-profit structure, credit unions must build capital primarily through retained earnings, a slow process which can face setbacks in the event of substantial fraud losses. Interchange revenue helps to offset the cost of debit payments fraud losses and is necessary in an environment where the Durbin Amendment's secondary cost recovery component—the fraud *prevention* adjustment—is insufficient by itself to compensate for all the externalities which enable fraud and which financial institutions cannot control.[27]

Question 26 - Are there specific actions that commenters believe could encourage the use of payment methods with strong security features?

The Federal Reserve Board could publicly discourage the use of checks in favor of more secure payment methods.

Emerging payment technologies offer speed and convenience but also introduce new vulnerabilities.

- Automated systems can act on inaccurate or incomplete information, leading to fraud or errors.
- Real-time decisioning limits opportunities for manual verification and fraud detection.
- Faster, decentralized systems make it easier to move illicit funds undetected.
- Fraudsters often adapt faster than the technology meant to stop them.

The Federal Reserve should prioritize initiatives that aim to promote cooperation among financial institutions, reduce the monetary cost of adopting new anti-fraud tools, and strengthen emerging payment technologies' security features.

[26] *See* Corner Post, Inc. v. Bd. of Governors of the Fed. Reserve Sys., No. 1:21-cv-00095 (D.N.D. Aug. 6, 2025).
[27] *See supra* note 5.

Conclusion

America's Credit Unions appreciates the opportunity to share our recommendations regarding ways to improve financial sector efforts to combat payments fraud. We encourage the Agencies to work closely with the NCUA and CFPB to explore regulatory and policy solutions that would benefit from close interagency collaboration or potential joint rulemakings. If you have any questions, please do not hesitate to contact me at 703-842-2266 or amorris@americascreditunions.org.

Sincerely,

Andrew Morris
Director, Innovation and Technology