MICHIGAN CREDIT UNION LEAGUE & AFFILIATES

September 17, 2025

“Request for Information on Potential Actions to Address Payments Fraud”

Re: Docket ID OCC-2025-0009

On behalf of the Michigan Credit Union League and our Michigan credit union members, we appreciate the opportunity to provide comments on the potential actions that federal agencies can take to address and combat the issue of payments fraud. Below, you will find responses to several questions asked in the Request for Information.

1. **What actions could increase collaboration among stakeholders to address payments fraud?**

   We believe that if FinCEN were to expand what 314(b) could be used for that this could be beneficial in terms of increased collaboration among stakeholders. We recommend broadening the use to allow for depository institutions to utilize that channel for any sort of potential fraud.

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?**

   Collaboration currently proves challenging for all depository institutions due to the restrictions on the type of information that can be shared when fraud occurs. The existing statutory and regulatory language surrounding information-sharing exceptions lack clarity, often leaving credit unions uncertain about whether an exception applies.

   Once information is shared, it cannot be retracted, which creates a significant compliance risk. As a result, many credit unions err on the side of caution and retain more information internally rather than risk inadvertently disclosing information that may not meet an exception. Greater clarity from federal agencies on what meets those information-sharing exceptions would directly cultivate increased collaboration and information sharing.

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?**

   Credit unions, as community-based depository institutions, frequently partner with external organizations to educate consumers about payments, fraud and scams. It is crucial to expand and formalize these collaborative networks on a larger scale as we look for ways to combat payments fraud.

   Organizations such as AARP, the Social Security Administration and law enforcement agencies are in the best position to provide additional insight and serve as effective collaborators in detecting, preventing and mitigating payments fraud. In addition, telecommunication providers and peer-to-peer (P2P) payment platforms should be more engaged given their role as common channels that fraudsters utilize to perpetrate said payments fraud. Securing their assistance is crucial in mitigating and combatting payments fraud.

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

   Increased collaboration among federal and state agencies could substantially improve detection, prevention and mitigation of payments fraud. State Attorneys General should be engaged as active collaborators in this space. In engaging them, the creation of enhanced channels for information sharing between depository institutions and the state attorneys general on emerging fraud trends would be highly beneficial to both parties. Giving them the information needed to be able to monitor and anticipate trending payments fraud schemes.

   The same principle applies to other state and local partners, including law enforcement agencies, Adult Protective Services and Department of Health and Human Services who should also be active collaborators in this space seeking to prevent payments fraud. Expanding the definition of vulnerable adults or allowing these organizations to assist individuals that don't meet these definitions could reduce the impact of fraud on certain victims.

   In addition to collaboration among state and federal agencies, we strongly encourage the avoidance of rules and regulations that impede information sharing between protective agencies and/or law enforcement and financial institutions. As in Michigan, where state law provides for a partnership between a reporting financial institution and the receiving agency, providing the financial institution with enough information to continue protecting member assets during ongoing fraud or abuse scenarios is critical for the potential victim.

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?**

   Payments fraud education is most effective when tailored to the target audience. Different demographics absorb information in different ways, and education must meet consumers where they are.

   For depository institutions, there is little value in providing broad education and general alerts about new fraud trends. Credit unions would benefit more from education that focuses on identifying red flags, methods to uncover instances of fraud in real time, and alerts when increases in a particular type of fraud occurs. Effective education should move beyond awareness and seek to provide actionable guidance that can be utilized to detect, mitigate and ultimately stop fraud from happening.

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

   There are some online resources that are indeed effective. For example, AARP provides great educational resources addressing fraud, and the Federal Trade Commission (FTC) offers training resources for internal teams and education materials for consumers and businesses. However, more online educational resources that are tailored for different audiences would be extremely beneficial. The inclusion of practical tips, checklists and examples of current fraud trends would also increase the usefulness of online educational resources and significantly enhance effectiveness. The examples should include some specifics about certain scams, so it is easier for financial institutions to link red flags they have noticed with a particular type of scam or tactic.

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

   Section 314(b): The existing framework could be expanded to explicitly include fraud. Currently, it really only applies to money laundering and financial terrorism. By expanding this framework, it would allow depository institutions to leverage an already existing process to facilitate additional fraud-related information sharing.

   NACHA rules: The current NACHA requirements focus on matching account numbers without requiring name matching when reviewing ACH transactions. Revising the rules to mandate name verification, at least where red flags are present, could prove beneficial in mitigating payments fraud.

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?**

    Supervisory guidance is valuable; however, it is insufficient on its own. If depository institutions were to rely solely on the guidance that has been provided to stay informed, they would be missing out on time-sensitive information and insights on payments fraud detection, prevention and mitigation.

    Instead, we think that it would be more beneficial to transition away from providing guidance but rather begin proving a monthly fraud report. Shifting the information from guidance to alerts really ensures that financial institutions have the information they need to be able to detect, prevent and mitigate payments fraud.

12. **What is the experience of consumers and businesses when supervised institutions place holds on depositors' funds because of suspected payments fraud? (Regulation CC's "reasonable cause to doubt collectability" exception is discussed separately below).**

    a. **For instance, how frequently are consumers and businesses affected by holds, delays or account freezes, and how responsive are supervised institutions to inquiries from consumers and businesses regarding these issues?**

       We recognize that account holds, delays or freezes can be frustrating for our members. However, these measures are used to protect the accountholder and their funds.

       When it is necessary for a hold, delay or freeze to be put on an account, credit unions generally work closely with their members to ensure that they have continued access to necessary funds. In many cases, institutions may shorten hold periods at the member's request if the risk can be resolved. Nonetheless, our first priority remains safeguarding members' funds. If suspicious activity is detected, depository institutions must use the tools at their disposal to protect both the individual member and the broader membership.

b. **Do current disclosure requirements effectively address consumers and business concerns when supervised institutions hold customers funds due to suspected payments fraud? For example, should changes be considered with respect to permissible customer communications under SAR confidentiality rules?**

   These items should be considered separately. A Suspicious Activity Report (SAR) is not always filed when a hold is placed.

   Under Regulation CC, the reasons that institutions are able to provide for a hold are often vague, giving members little meaningful explanation of why their funds are restricted. Additional regulatory clarity would be beneficial. For example, creating a distinct category specifically for fraud or suspected suspicious activity would provide greater transparency and the potential for better data collection.

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 type of interbank disputes regarding allegedly fraudulent checks? Do these types of interbank disputes arise more frequently in connection with certain types of checks or parties? What actions could the Board, FDIC, and OCC consider, including potential amendments by the Board to Regulation CC, that could improve supervised institutions' ability to resolve interbank disputes over liability for allegedly fraudulent checks?**

    Interbank disputes often arise when the consumer or business did in fact initiate the payment but did so under fraudulent circumstances (i.e. scams). In these cases, the payment itself is not unauthorized, but rather it was authorized through deception. Currently, the receiving institution has no ability to return the item. They have to rely on the paying institution to initiate the return. The issue comes when the receiving institution is the one that must convince the paying institution that their member/customer is a victim. If the receiving institution can make contact with someone at the paying institution, sometimes they are able to convince the institution to return the item. This highlights the need for a process for the receiving institution to be able to return a check for suspicious activity as part of the solution to combat payments fraud.

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?**

    While we recognize the balance that Regulation CC seeks to strike balancing funds availability and fraud risk, the current thirty (30) day extended hold timeframe is not always sufficient for suspected fraud or suspicious activity investigations. Investigations can be complex and may require more than thirty (30) days to fully resolve. Extending this timeframe to address these circumstances would better equip depository institutions with the timeframe needed to properly investigate instances of fraud or suspicious activity and ensure that members funds are going where they intended and not to fraudsters.

Technological advancements in check processing have not meaningfully shortened the time it takes for depository institutions to detect nonpayment or fraud. Additionally, we feel it pertinent to note that the distinction between "local" and "non-local" checks is outdated under Check21 and should be removed. The current two (2) day hold period for checks deposited via ATMs is insufficient. Typically, the credit union receives the transaction report the following day, and obtaining the actual check image may take an additional day or two. By that time, the hold often expires, and funds likely are already withdrawn.

If a real-time reporting system were to be implemented to show all ATM-deposited checks immediately (or as close to real-time as possible), institutions could verify authenticity quicker. Until such infrastructure exists, shortening of hold times would not advance fraud prevention, but would in fact expose consumers and institutions to even greater losses. Fraud schemes would exploit the shortened hold periods, leaving even less time to detect fraudulent transactions before funds are withdrawn.

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? Would depository institutions benefit from further clarification on when it may be appropriate to invoke this exception? What are the experiences of businesses and consumers when depository institutions invoke this exception in order to delay the availability of depositors' funds?**

    The current reasonable cause to doubt collectability exception under Regulation CC does not provide sufficient time. This is because the hold period is only two (2) days, it often expires before a meaningful investigation can occur. At a minimum, institutions should be provided five (5) business days when invoking this exception which would allow for adequate time to research and respond. Further clarity on when and how the exceptions under Regulation CC may be applied would also be beneficial to ensure consistent and meaningful application.

16. **Broadly, how could payments fraud data collection and information sharing be improved?**

    Current data collection practices are not sufficiently helping depository institutions like credit unions combat fraud. Both the timeliness and type of information being shared is insufficient in helping to combat payments fraud.

    Credit unions recognize the need to balance transparency with the risk of sensitive information falling into the hands of fraudsters. However, creating a secure, centralized, real-time database accessible to depository institutions would significantly enhance the industry's ability to identify patterns, share information, respond proactively and ultimately mitigate and stop fraud losses.

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?**

There are significant barriers limiting the collection and sharing of payment fraud data between industry stakeholders. These barriers include a lack of clear and consistent guidance on what data may be shared and under which exception it applies. If the relevant agencies provided explicit, practical parameters covering what types of information can be shared, and any safe harbors that exist, depository institutions would be far more willing and able to share timely, pertinent information among themselves and with other partners. In the absence of clarity, institutions are defaulting to either not sharing any information or only sharing broad, generalized statements that lack value in preventing and detecting fraud.

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?

We believe the most impactful data includes stories and examples of the types of fraud being perpetrated. Real-world case descriptions help depository institutions recognize patterns and allow them to further train their staff on what to be on the lookout for. Numbers have their place but it's the red flags to look out for that really are what we believe is the most beneficial in identifying and combating payments fraud.

We also recommend the addition of a distinct fraud/scam category on the SAR filings to enable easier aggregation and analysis across the sector. Equally important is timely sharing of the collected data in a meaningful, searchable format that the industry can utilize. Entities best positioned to collect and share this data include FinCEN for the SAR-derived insight and then we believe the Federal Reserve Board, FDIC, Department of Treasury and OCC also play a role here with the potential to provide insight into systemic trends. We need to ensure that data is not only collected but also shared with the industry

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?

Yes, a centralized, secure repository would improve cross-industry detection and response. We believe FinCEN's 314(b) infrastructure offers a great foundation that could be adapted and expanded to support broader fraud-related information sharing well beyond money laundering and financial terrorism. Participants of the repository should include depository institutions, relevant federal and state agencies, and potentially even key private-sector partners like telecom and P2P platforms all who are subject to clear data-use rules.

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?

We are seeing increases in P2P payment fraud, social-engineering schemes that elicit online banking credentials and Multi-Factor Authorization (MFA) codes, and romance/family impersonation scams, which are increasingly amplified by generative AI. We also continue to observe that victims are being coached in real-time by the fraudsters. They are being kept on the line during transactions and being instructed on how to circumvent common controls and respond to certain questions. As fraudsters evolve, training, public education and vigilance will continue to be essential to depository institutions, consumers and businesses.

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?**

    We have found that the most consistent and effective control is human interaction. We train staff how to engage with members and ask them targeted questions when transactions appear to be out of the ordinary for that particular member. While analytics and technology are a critical piece of the puzzle, they cannot be replaced by human judgement informed by knowledge of our members and behavioral red flags.

    A holistic approach including information sharing, staff training and continued public education is required. Members can also proactively assist depository institutions by continuing to alert us of large or unusual transfers, travel or other abnormal transactions/behaviors ahead of time. This improves detection and reduces false negatives that some of the automated systems might flag or miss.

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

    Beyond continued collaboration among agencies, regulators, and depository institutions, we should build structured partnerships with non-financial sectors that fraudsters frequently exploit like social media platforms, P2P networks, telecom and retail. Cross-sector participation should be supported by clear, reciprocal information sharing protocols — so the "loop" truly circulates insights rather than stopping at sector boundaries. Reducing artificial barriers and enabling rapid reporting will materially improve the industry's ability to identify, prevent and mitigate payment fraud.

Closing Remarks

We appreciate the opportunity to provide input as the agencies explore the most effective strategies to address the continuing challenge of payments fraud. Fraud schemes continue to evolve in complexity and scale, creating significant risks not only for our credit unions but for our members as well. We encourage the agencies to explore enhanced coordination, information sharing and cross-industry collaboration to bolster the ability to identify, mitigate and ultimately stop payments fraud altogether.

Sincerely,

Patty Corkery
President and CEO
Michigan Credit Union League & CUSG