[redacted]

From: Spring Ettner <[redacted]>
Sent: Tuesday, September 2, 2025 12:53 PM
To: Comments
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)

[redacted]

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

Dear Mr. Gould, Mr. McDonough, and Ms. Jones:
I am the Vice President Customer Service & Support of Prairie Community bank, a $185 million community bank located Northern Illinois. I am writing to respond to the request for information (RFI) on payments fraud.
We just opened our 4th branch and have been servicing our local communities since 1998. We serve as a financial anchor in our local markets and we are better equipped to understand the unique needs, challenges and opportunities for the communities we serve. We often know our customers personally to assist in lending decisions. We are able to make quicker decisions locally and respond quickly to economic shifts. We are here to build relationships with our customers not just complete a transaction.
I applaud the agencies for issuing this RFI and seeking input on ways that the OCC, the Federal Reserve System (FRS), and the FDIC could take actions to help consumers, businesses, and financial institutions mitigate payments fraud. Community banks continue to be challenged by a rise in fraud and scams across payment types, so agency action is much needed.
Specifically, we have been affected by payments fraud in the following ways:
*We experienced issues of Online Banking/Account Takeover fraud causing significant losses.
*We have seen several instances of checks being intercepted through the mail and cashed by a fraudster impersonating the payee or having the item altered and paid.
*We are seeing higher operating costs due to increased spending on fraud detection tools and costs for customer support and claims processing.
External Collaboration. Collaboration is important when it comes to payments fraud to assist with detection, prevention and to respond more effectively. Fraud threats evolve rapidly, often span multiple

industries and involve sophisticated tactics crossing organizational and national boundaries. Sharing of fraud indicators and behavioral patterns between stakeholders would allow for detecting fraud earlier. Collaboration should come from acquiring banks and merchants detecting anomalies at the POS, Payment Networks and Processors to facilitate cross-institution data sharing, FinTech's and Wallet Providers to work with issuers and networks to authenticate users, Regulators to enable secure cross sharing and to provide clearer definitions of the rules and responsible parties. Local, State and Federal agencies should be able to share fraud tends with the impacted industries. In addition, the USPS must play a role and hold some responsibility for the thefts occurring.

Some obstacles to overcome – inconsistent definitions and rules, the number of resources available to participate in a national initiative, safe harbor restrictions.

Consumer, Business, and Industry Education. Fraud education must combine awareness, practical skills and behavioral reinforcement. We have found that hands-on, interactive training using realistic scenarios works the best. People remember stories vs. general warnings and the knowledge of how something happens vs. just existing is extremely valuable. Joining forces to provide the same messages and campaigns from all stakeholders creating a united front against fraud. Keeping consumers and staff alert to new scams and tactics. Education resources need to be targeted and prioritized. The elderly and young need to know how to use the internet, how to prevent themselves from becoming a victim and knowledge to NEVER share their login information.

Regulation and supervision. There is a need to change and update Regulations and Supervisory Guidance. There should be added guidance on fraud risk management expectations. Community Banks face challenges in when resolving interbank disputes – there is a lack of standardized processes, delayed responses regarding claims and difficulty making contact with counterparts in a dispute. There should be a requirement to provide contact email, phone and/or fax for all parties to a dispute for access by other parties. It has been our experience large banks are not exercising sufficient CIP processes and opening accounts being leveraged by the fraudsters. We have also experienced much difficulty in locating contact information for these larger banks and when we do make contact, we don't receive a response for upwards of 60-90 days at which time they don't have any funds to return or they will tell us an altered item is counterfeit instead to avoid payment. BOFD should be required to provide CIP information and prove they followed proper rules and procedures in the case they cannot pay a claim. When dealing with debit card payment fraud certain liabilities should be shifted to the merchants when there are red flags present as well as putting additional liability on the card carrier for negligent handling.

Changes or clarification of language in the UCC should be considered. For example, consideration of extending the midnight return deadline. The discovery of alteration is often not discovered immediately and processing through the presentment warranty process is long and difficult. In these instances, the BOFD is in the best position to determine alteration as they have possession of the physical item and or mobile deposit – they are supposed to know their customer and be able to identify mobile deposit suspicious activity. Another consideration would be to have a "shared loss" rule in place for counterfeit items especially when banks are accepting these via the mobile channels and not completing any reviews. At a minimum the BOFD needs to cooperate in recovering funds, including proof of CIP and timeline for response to claims. There needs to be clear and concise language for when Hold Harmless agreements are required – some large banks are requiring this all the time including in cases of alteration when the BOFD is responsible.

Under Regulation CC the ability to place extended holds on Cashier Checks needs to be re-evaluated and these items should be treated as any other check. Fraudsters know we must give the first $6725 out the next day and are now using this to their advantage and printing Cashier Check on these fraudulent items. If you are able to reach a large bank, they will not provide funds availability or indicate if the Cashier Check is valid.

Payments fraud data collection and information sharing. Community Banks are not equipped to purchase additional services and tools for data collection, analysis and reporting tools. We are already in the business of "knowing" our customers and are already monitoring their activity. Having a centralized data reporting database for sharing payments fraud data across entities would be beneficial. Participation in this type of database sharing should not be voluntary but require.

Reserve Banks' Operator Tools and Services. Community banks can certainly benefit from the variety of products and services, including, for example, a fraud contact directory, a fraud information sharing database, an interbank check fraud breach of warranty claim mechanism, a check image and verification tool, and confirmation of payee service. Access to these types of services should not be limited and should be mandatory.

General Questions. Check fraud has seen a resurgence in the past couple of years, especially in the wake of increased mail theft and digital scams such as "romance scams" and get rich quick scams. Fraudsters are stealing checks from mailboxes and "washing" them or producing a counterfeit item duplicating legitimate layouts and using check numbers in the same the sequence. Debit card fraud also remains a significant threat, especially through compromised merchants and account takeover schemes. We have seen an increase in skimming devices placed on terminals our cardholders frequent. We have begun utilizing a transaction monitoring system to flag out of pattern checks, duplicate check numbers, large and excessive card activity then reviewed by internal staff and as needed reaching out to the customer for verification. It comes down to consumer education and the need for us to hold them accountable for some of the fraud that occurs through giving out online credentials, not securing their cards and not reviewing their account activity timely in order to report quicker.

Thank you for the opportunity to provide comments on this RFI. The Bank looks forward to continuing to work with the OCC, FRS, and FDIC, and other stakeholders to protect our customers and communities from the growing threat of payments fraud.

Sincerely,

PRAIRIE™
Community Bank

Spring Ettner
Vice President
Client Services & Support
Prairie Community Bank
Direct [redacted]
Phone [redacted]
[redacted]

received this communication in error, please notify us immediately by return e-mail or by telephone at [redacted], and destroy this communication and all copies thereof, including all attachments.