From:	Jenn R. Spartz
To:	Comments
Subject:	[EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)
Date:	Thursday, September 18, 2025 3:52:07 PM

[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 Ms. Jones, Mr. McDonough, and Mr. Gould:
I am the Chief Risk Officer for a family of banks: Glenwood State Bank, a $545 million community bank located in Glenwood, Minnesota; Lowry State Bank, an $85 million community bank located in Lowry, Minnesota; and, First National Bank of Osakis, a $95 million community bank located in Osakis, Minnesota. I am writing to respond to the Office of the Comptroller of the Currency (OCC)'s, Board of Governors of the Federal Reserve System (Board)'s, and Federal Deposit Insurance Corporation (FDIC)'s request for information (RFI) on payments fraud.

Our family of banks have been serving our local communities for over 120 years. We support our communities by providing customized guidance, resources, and products. We play a critical role in our communities by supporting our small businesses and consumer customers through lending in our local areas. We believe in servicing the needs of our customers, our communities, and our employees.

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, the Bank has been affected by payments fraud in the following ways:

- Check Fraud
  - We have customers getting scammed online and given a fraudulent check to cash and send money to fraudsters. Common scams we are seeing include secret shopper, romance scam, and online job scams.
  - We have customers who have had checks stolen out of the mail, altered, and then cashed.
- Tech Support Scam
  -

Customers are duped into thinking their computer has a virus, calls the number on the screen, gives control of their computer to the fraudster, who then gains access to their online banking and other sensitive information.

- Other Scams have included the use of AI for Deepfakes, spoofed sites, and fake products.

Consumer, Business, and Industry Education

- Community banks thrive, in part, because of their close customer relationships. We are able to talk with our customers on an individual level about various topics. A Public service announcement campaign, with real life stories, would educate our customers as well as provide an opening for our staff to have conversations around those PSAs.

Regulation and Supervision

- Broadly speaking, There are opportunities to enhance supervisory guidance around payments fraud. But these opportunities need to be appropriately tailored to community banks. It is important to have tiered compliance requirements and avoid imposing new burdens on community banks.
- Check fraud remains a significant issue for us. We have had significant difficulty resolving interbank disputes regarding fraudulent checks. The biggest hurdle is getting to the right department or person of the large financial institutions to even begin to resolve check fraud related issues. In the situations we have experienced, it has been taking around 30 days to recover funds for our customers from these large institutions. And, sometimes, they flat out deny our claim, even when they hold the liability.
- Changes to Regulation CC could help community banks prevent and mitigate check fraud. For example, when the "reasonable cause to doubt collectability" is for suspected fraud, a longer hold time should be allowed. This would give time for an item to be returned as fraudulent. It would also slow down the entire transaction giving the customer time to think it through, as well as the bank time to discuss the situation with the customer. We have experienced situations where this would have save the customer from experiencing a loss. Hold times should not be shortened as they are an essential tool for banks to detect and prevent check fraud. Overall, financial institutions should have flexibility to extend hold times under appropriate circumstances.
- Consideration should be given to Regulation E as it pertains to fraud and scams. When a customer is a repeat victim to scams, zero liability doesn't seem to help them understand the gravity of these fraudulent situations. Additionally, clarification of what constitutes a reasonable investigation when fraud and scams are involved would be helpful.
- Some form of regulation should be considered around Bitcoin ATMs. Our only experience with them is around our customers being scammed by fraudsters directing them to drive to a Bitcoin ATM to deposit money to the fraudsters. We have not heard of any customers that have used a Bitcoin ATM for any legitimate purposes.

Payments Fraud Data Collection and Information Sharing

- There are many groups and communities that offer opportunities to share information.

Community banks are reluctant to share due to privacy issues. Appropriate safe harbors would improve banks' ability and willingness to share fraud data.

- Community banks would benefit from automated data collection, analysis, and reporting tools that are integrated with services they already use and do not come with additional costs.

Reserve Banks' Operator Tools and Services

- There are a variety of specific products and services that could benefit community banks by making it easier to work with other financial institutions, especially the larger institutions. This could include, for example, a fraud contact directory, a fraud information sharing repository, an interbank check fraud breach of warranty claim mechanism, a check image analysis and verification tool, an atypical payment monitoring service, and confirmation of payee service.

General Questions

- The most common type of fraud that we are seeing is in the area of check fraud. The check fraud is either via checks that have been stolen and altered or fictitious checks. We have experienced a few different ways of check fraud being committed:
    - Our customers get caught up in an online scam and a fraudulent check is used to trick them into sending the fraudsters money. It may be an online job scam, secret shopper, romance scam, Facebook marketplace or some other fake shopping site. The fraudster either sends the customer a check to deposit or they convince the customer to give them online banking credentials so they can mobile deposit the check. The customer then sends the funds only to find out a few days later that the check they were given was fraudulent.
    - A criminal or a group of criminals steal checks out of the mail, alter them and then cash as many as they can before the bank or the business catches on.
- Another common scam that we are seeing is the tech support scam. Customers think that their computer has a virus, calls the number on the screen and the fraudster gains access to their computer. The fraudster goes into online banking and transfers funds between the customer's accounts to make it look like they refunded too much money back to the customer. Then, they convince the customer to go to the bank, withdraw funds and buy gift cards to reimburse them. We are seeing these scams generally committed against more elderly customers who are not as tech savvy and the fraudster instills a sense of panic and urgency in them. We have even witnessed where the fraudster will keep our customer on the phone while they are at the bank so they can coach them on what to say to the banker, convincing our customers to flat out lie to us. These tactics have made it difficult to protect our customers.
- The push toward faster payments has impacted the bank and customers because the fraudsters try to get the customer to use one of these methods so that the money is gone before they even have a chance to realize that it was fraud. We see fraudsters mostly using cash app and Zelle, as well as having customers withdraw cash and buy gift cards.

- We have used significant resources in our attempt to fight fraud. We created a dedicated fraud team to work with customers affected by fraud as well as take a proactive approach to fraud within our communities and with our staff. Customer outreach programs as well as ongoing customer and employee education are a priority. We utilize various fraud measures built into our existing systems to help prevent, detect, and mitigate fraud. We also recently invested a significant dollar amount for a fraud detection system through our core.

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,

Jenn Spartz
Chief Risk Officer
Glenwood State Bank, Lowry State Bank, First National Bank of Osakis

Jenn R. Spartz
Chief Risk Officer
Glenwood State Bank | Lowry State Bank | First National Bank of Osakis
[redacted]