

[REDACTED]

From: Kim Jones [REDACTED]
Sent: Wednesday, August 27, 2025 12:18 PM
To: Comments
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)

Importance: High

[REDACTED]

Jonathan Gould
Comptroller of the Currency, Office of the Comptroller of the Currency
Docket ID OCC-2025-0009

Benjamin W. McDonough
Deputy Secretary, Board of Governors of the Federal Reserve System
Docket No. OP-1866

Jennifer M. Jones
Deputy Executive Secretary, Federal Deposit Insurance Corporation
RIN 3064-ZA49

Dear Mr. Gould, Mr. McDonough, and Ms. Jones:

I am the Compliance/BSA Officer of The First National Bank of Eagle Lake (Bank), a \$159M small community bank located in Eagle Lake, Texas. 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.

The First National Bank of Eagle Lake is proud to be recognized as a leading community financial institution in the area. Since our founding in 1904, we have remained strong and committed to serving our customers. We focus on delivering quality financial products and services at exceptional value, while building long-term relationships through outstanding customer service. Our mission is to be the community bank of choice in every market we serve.

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:

- Major losses from mail-theft related fraud

- Major losses from altered checks
- Major losses due to lack of real-time tracking systems
- Major losses caused by fraudsters exploiting weaknesses in the payments system
- Major losses resulting from large banks' lack of cooperation with smaller institutions

External Collaboration

The Bank supports collaborative stakeholder efforts to address payments fraud. Fraud and scams persist across state borders, so national stakeholder collaboration is necessary to effectively combat the problem. However, national efforts must recognize the resource constraints individual community banks face when deciding whether to participate. Local and regional collaboration across community banks, federal and state regulators, law enforcement, community organizations, and other stakeholders can be an effective way to build connections and share information at the community level.

Consumer, Business, and Industry Education

Community banks thrive, in part, because of their close customer relationships, so face-to-face engagement is one of the most effective tools to reach community bank customers. In-branch material and messaging is especially valuable for community banks.

Community banks serve elderly customers, as well as consumers and small businesses in rural and agricultural areas, so educational materials tailored to these groups would be valuable. Some community banks are in areas that do not have widespread, reliable Internet access, so web-based resources are not always accessible to customers.

Regulation and Supervision

Broadly speaking, payments fraud regulations and examiner expectations need to be appropriately tailored to community banks with tiered compliance requirements and deadlines. There are opportunities to enhance supervisory guidance around appropriate controls, suitable technology, reporting, and incident response, but it is important to avoid imposing new burdens on community banks.

Check fraud, in particular, remains a significant issue. Community banks are concerned that some large financial institutions are not exercising sufficient CIP/KYC processes and opening accounts that are being leveraged by fraudsters. Similarly, community banks have had significant difficulty resolving interbank disputes regarding fraudulent checks. Several years ago, during the peak of mail-theft related fraud, we experienced an altered check dispute with a large financial institution. Our potential loss was nearly \$50,000, and it ultimately required about eight months and legal involvement before we were able to recover the funds.

Changes to Regulation CC could help community banks prevent and mitigate check fraud. For example, the return deadline related to fraud could be extended, the "reasonable cause to doubt collectability" exception could be clarified, and relevant definitions could be revised (e.g., "altered" and "alteration"). However, hold times should not be shortened; they are an essential tool for banks to detect and prevent check fraud. Financial institutions should have flexibility to extend hold times under appropriate circumstances.

Payments Fraud Data Collection and Information Sharing

While centralized data reporting would be valuable for the ecosystem, agencies should avoid imposing additional data collection requirements on community banks. 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

Community banks would benefit from tools and services that integrate with third-party services they already use and pricing that is appropriate for their size and complexity.

There are a variety of specific products and services that could benefit community banks, including, 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 Bank has been impacted by several types of fraud, including but not limited to check fraud, push credit scams, a compromised BIN, debit card fraud, and ACH fraud. Fraudsters frequently use money mules in attempts to move illicit funds through the payments system.

To combat these threats, the Bank has implemented a number of measures to help deter fraud. This includes adjusting system parameters, closely reviewing daily reports, and accessing systems first thing in the morning to monitor incoming and outgoing items. Employees have also been instructed to ask detailed questions to verify customer transactions and to carefully vet individuals outside our normal lending area who seek to open new accounts.

Even with these efforts, it often feels like it's never enough—the tactics used by bad actors continue to evolve, requiring us to stay vigilant and adapt constantly.

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,

Kimberly Jones, CAMS
SVP/Compliance,BSA,AML,SAFE Act Officer
First National Bank of Eagle Lake

Send your Personally Identifiable Information(PII) Content with our Zixmail portal at

Notice: The information contained in this message may be privileged, confidential, and protected from disclosure. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by replying to this message, and then delete it from your computer.

This message was secured by [Zix®](#).