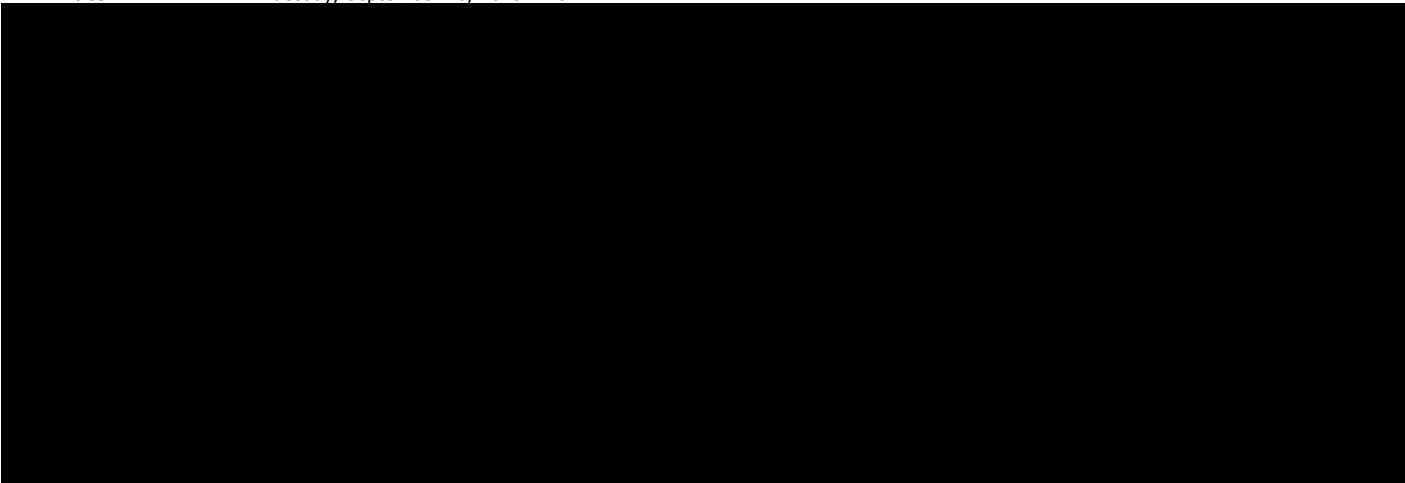


**From:** [Sada Theut](#)  
**To:** [Comments](#)  
**Subject:** [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud;  
Comment Request (RIN 3064-ZA49)  
**Date:** Tuesday, September 16, 2025 12:52:12 PM



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 SVP of The First National Bank of Central Texas(FNBCT), a \$1.5 billion dollar community bank located in the Central Texas area. 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 payment fraud.

We are a locally owned and operated community bank dedicated to serving the financial needs of our area. With deep roots in the region, our bank has a long standing history of supporting local families, small business and entrepreneurs. We take pride in being a trusted lender and financial partner, helping our community grow and thrive through personalized service and a commitment to local values.

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 payments types, so agency action is much needed.

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

- Impersonation and Debit Card Fraud: A fraudster impersonated a customer to activate Apple Pay and successfully processed two Bitcoin transactions.
- Check Fraud: This is still increasing across the board. From business checks to personal checks to cashier's checks.
- Bill Pay Fraud: Fraudulent check were used to fund bill payments to third parties.
- Wire Fraud and BEC: Wire transfers have been processed for customers who used spoofed emails resembling current vendors.
- Elder Financial Exploitation: Elderly customers have been contacted by customers and tricked into draining their life savings. We've seen an increase of this and even our first instance of customers being told to drop the cash into Bitcoin machines.

#### External Collaboration

- FNBCT 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 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 expectation need to be appropriately tailored to community banks with tiered compliance requirements and deadlines. There are opportunities to enhance 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 difficulty resolving interbank disputes regarding fraudulent checks. We were told by one such institution, that they do not research anything under \$1000. While this may fit in with their business model, not all community banks are willing to take that loss or communicate that to customers.

- 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 essential tools for banks to detect and prevent check fraud. Financial institutions should have flexibility to extend hold times under appropriate circumstance, and the burden of compliance should not overshadow the fraud mitigation.

#### 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 we already use and do not come with additional costs.

FNBCT has encountered significant fraud threats, particularly wire fraud stemming from business email compromise (BEC), debit card fraud, check fraud and elder financial exploitation. Criminals have impersonated trusted contacts to redirect wire transfer, exploited the mail system to process fraudulent checks and targeted vulnerable seniors through deceptive schemes. In response, we have implemented rigorous controls including mandatory callbacks for all wire transfers, enhanced fraud detection protocols, and staff training.

Thank you for the opportunity to provide comment on this RFI. FNBCT 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.

**Sada Theut**

Senior Vice President - BSA Officer, The First National Bank of Central Texas

