From:	Marty Sellars
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 11, 2025 1:57:18 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 CEO of FNBC Bank, an $825 million asset community bank headquartered in Ash Flat, AR. 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 the Federal Deposit Insurance Corporation (FDIC)'s request for information (RFI) on payments fraud.

FNBC was founded in 1912 as the Bank of Ash Flat and today serves communities throughout North Central and Northeast Arkansas, as well as South Central Missouri. Located in the underserved Ozark foothills, FNBC strives to build profitable relationships and foster economic development through financial products and customer-driven services. We received Community Development Financial Institution (CDFI) designation in 2016.

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

- Customers receive phone calls that they believe are from FNBC stating they have been hacked, and they need to wire money to a different bank so they can begin an investigation. They instruct the customer to say they are wiring money to a friend and to not tell relatives. One recent customer lost $16,000 and was trying to wire an additional

$19,000 when our community bankers were able to intervene.

- Customers may receive an "invoice" stating their payment was received for a known service, such as Adobe or Microsoft. When they call the number on the invoice, the fraudster has them download an app onto their computer so they can investigate the charge. They then watch them log into Online Banking, gaining their credentials. They will tell the customer they are going to refund them the money they were charged but are only transferring money from their savings account into their checking. It is always for too much - $30,000 instead of $300, for example – and they instruct the customer to just withdraw the money, take it to a local courier and they will get the money back to them. We recently had a customer lose $130,000 over three transactions in this exact scenario.
- We estimate that between April and August 2025, FNBC customers lost $552,000 to payments fraud.

Suggested Actions the OCC, Board/FRS, and FDIC Could Take:

External Collaboration:

- FNBC 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.

Consumer, Business, & 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 are especially valuable for community banks.
- Simple videos to share with customers or local businesses/groups such as nursing homes, large box stores (where fraudsters often have victims buy gift cards), area VFWs, community centers and schools that can educate on current scams and how to respond.
- Our most vulnerable customers are not always on social media or checking emails where we regularly provide education on payments fraud. Cost is a barrier for community banks to mail regular education and information to those customers, so we would support exploring ways to make mailing these critical education pieces more affordable.

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.
    - It is nearly impossible to get a person on the phone at a big bank, and once you do, they make you jump through hoops to get a recall. They simply are not community banks and do not care for customers the way we do.
    - When trying to return a check to a larger bank, they do not always detail out their expectations at the front end, so they will send the recalls back repeatedly for resubmission. It will be for simple things like the form not being signed by a VP or higher, or they want each check on a separate form and submitted separately in its own case even though they were negotiated by the same individual, or even failing to include (Indemnified Bank) after their bank's name. They do not read the whole form, so they will send it back for corrections before they see if there's anything else that needs addressed. It simply drags out the process for us and the customer.
    - FNBC has had several instances where our customers were scammed and sent wires to larger banks. Despite the name on the wire not matching the account, the larger bank accepted it and gave the fraudster customer access to the funds, which were spent immediately. There needs to be accountability for the bank accepting the wire to know their customer and what type of activity is suspicious.
- Changes to Reg 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 "alternation"). 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.
    - Larger banks refused to verify funds on check, so when a hold falls off and the customer has access to the funds, there is still risk for the check to be returned. We had this happen to a customer recently. A check was returned 2 days after the hold fell off and now they have a -$4,000.00 balance, which is devastating for a customer.

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.
- Additionally, we believe a regional forum that allowed community banks to share information on the types of fraud and scams presenting in their area would help bank employees to spot potential fraud attempts more easily.

Thank you for the opportunity to provide comments on this RFI. FNBC looks forward to continuing to work together to protect our customers and communities from the growing threat of payments fraud.

Sincerely,

Marty Sellars

Chief Executive Officer

FNBC Bank