



RED RIVER BANK

A Louisiana Community Bank • Member FDIC

September 15, 2025

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

Re: *June 16, 2025 Request for Information on Potential Actions to Address Payments Fraud*

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

I am the President and Chief Executive Officer of Red River Bank, a \$3.17B community bank headquartered in Alexandria, Louisiana. I am writing to respond to the Officer 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") regarding payments fraud.

Red River Bank was established in Alexandria, Louisiana in 1999 and has been proudly serving the State of Louisiana since then. We currently operate 28 banking centers and two loan production/deposit production offices ("LDPO"), and are the sixth largest Louisiana-headquartered bank based on assets as of June 30, 2025. Our banking centers are located in the following Louisiana markets: Central, which includes the Alexandria metropolitan statistical area ("MSA"); Northwest, which includes the Shreveport-Bossier City MSA; Capital, which includes the Baton Rouge MSA; Southwest, which includes the Lake Charles MSA; Northshore, which includes Covington; Acadiana, which includes the Lafayette MSA; and New Orleans. Our combined LDPO locations are located in Lafayette and New Orleans.

Red River Bank is a community bank with a relationship-driven client focus and a consistent lending philosophy that has earned us a loyal customer base. We have a strong history of serving



our local communities, including being one of the first banks in Louisiana to receive applications and fund loans under the Small Business Administration's Paycheck Protection Program.

I, along with Red River Bank's Board of Directors and the rest of our executive management team, 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.

Red River Bank continues to be impacted by payment fraud in recent years. Our largest fraud losses stem from consumer debit card fraud. We also experience significant levels of fraud related to real-time person-to-person transfers through various apps. Check fraud remains prevalent, with our most common losses stemming from fraudulent instruments deposited at large banks. Despite being clearly obligated to bear these losses under UCC rules, large banks often delay returning funds to us, or refuse entirely. Large banks also frequently refuse to respond timely to our requests for information, despite our communication to an email we have been told is dedicated to handling fraud. Significant Red River Bank employee time is consumed in efforts to recover funds lost due to fraud.

We appreciate the opportunity to suggest actions the OCC, Board/FRS, and FDIC could take to help combat fraud and offer the following.

External Collaboration

Red River 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. 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. However, national efforts must recognize the resource constraints that individual community banks face when deciding whether to participate.

Financial Crimes Enforcement Network should play a cooperating role in combating fraud. In many cases, fraudulent instruments are deposited in accounts at large banks, with criminals quickly removing the funds. It seems like these funds should be able to be tracked down and recovered. Establishing some kind of central reporting structure for banks to use to report instances of fraud would be helpful. In addition, the U.S. Postal Services should get involved. Most, if not all, of the washed and altered checks targeting our customers were stolen from the postal service.

Regulation and Supervision

Broadly speaking, payments fraud regulations and examiner expectations should 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.

Community banks are concerned that some large financial institutions are not exercising sufficient Customer Identification Program (CIP)/Know Your Customer (KYC) processes and opening accounts that are being leveraged by fraudsters. Similarly, community banks have had significant difficulty resolving interbank disputes regarding fraudulent checks. Specifically, in our experience, large banks simply respond that a check that is plainly altered is instead counterfeit, thereby refusing to honor their transfer and presentment warranties under the UCC. We expend significant resources in making repeated requests to large banks to honor warranties, in some cases without success. These large banks rely on a smaller bank's reluctance to incur the expense of litigation. They should be held accountable to honor their warranty obligations.

Below are our specific suggestions to address issues surrounding check fraud.

- 1) Extend the midnight deadline rule to 30 days. Paying banks are required to return fraudulent items by midnight following the day the item is presented, but an alteration or counterfeit item is often not discovered until the customer receives his or her bank statement, which could be up to 30 days later. A paying bank's relief at that point is limited to enforcing its presentment warranty against the bank of first deposit. This process is often lengthy and time-consuming. And, if the item is counterfeit, there is no breach of warranty claim. The bank of first deposit is in the best position to stop a fraudulent item at the point the item enters the payment stream. That bank has the physical item in hand (except in the case of a mobile deposit) and has the obligation to know its customer.
- 2) Impose a duty of good faith under the UCC on the bank of first deposit to act in good faith participation in loss recovery. Regardless of whether a check is altered or counterfeit, the UCC should require the bank of first deposit to cooperate in recovering funds, including by responding promptly to written demands, disclosure of account activity, and freezing funds promptly upon written notice of fraud for a period of time to allow an investigation.
- 3) Impose more responsibility on customers when they are negligent in handling their debit cards and accounts. Current law does not consider a consumer's negligence, and it should. For example, if a customer leaves her debit card on a restaurant table with her PIN on a piece of tape on the back of it, the bank is liable for losses resulting from a thief's use of the debit card. In cases like this, the customer should bear the responsibility for her own conduct. Likewise, if a customer fails to act reasonably and becomes the victim of a scam, the bank should not be responsible for resulting losses.
- 4) Impose more responsibility on customers when losses are caused by their failure to promptly review account statements or online activity. Regulation E currently states that a consumer must report an unauthorized electronic fund transfer that appears on a periodic statement within 60 days of the financial institution's transmittal of the statement to avoid liability for subsequent transfers. In today's world, 60 days is too long.

- 5) In no circumstances should hold times be shortened, as they are an essential tool for banks to detect and prevent check fraud. Additionally, 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. 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.

Red River Bank supports creating a line item on the call report that requires financial institutions to report the amount of payment fraud losses each quarter. Currently, these losses are included in non-interest expense. Breaking these losses out will enable regulators to understand the gravity of fraud losses. We also support requiring large banks to report the amount of claims being made against them as the bank of first deposit on a quarterly basis, as well as amounts they have paid in response to such claims.

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. These tools will also protect consumers, as they will enable banks to more quickly recover stolen funds. In many cases, the criminal has already withdrawn funds from the bank of first deposit by the time Red River Bank is able to communicate with that bank. All banks should be required to participate in an expedited fraud communication process.

Thank you for reading this letter and for the opportunity to provide comments on this RFI. Red River 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. I would be happy to discuss this letter, and to provide any additional information that you might like to see. I am available at [REDACTED] or [REDACTED]

Sincerely,

[REDACTED]

R. Blake Chatelain
President and Chief Executive Officer