[redacted]

From: Melinda A. Shaffer <[redacted]> on behalf of Christopher Palmer <[redacted]>
Sent: Tuesday, September 9, 2025 5:06 PM
To: Comments
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)

[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 President and Chief Executive Officer of Pioneer Bank, a $1B community bank headquartered in Roswell, New Mexico. I am writing to respond to the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), and Federal Deposit Insurance Corporation (FDIC) request for information (RFI) on payments fraud.

Pioneer Bank, originally established in 1901 as Roswell Savings & Loan, has grown into a cornerstone of financial services in New Mexico. With a steadfast commitment to community banking, the institution has played a pivotal role in supporting the economic vitality of the region. Pioneer Bank is a trusted financial partner for both small businesses and individual consumers, offering essential lending services that drive local growth and opportunity.

The bank's community-first philosophy is reflected in its strategic expansion across New Mexico, including branches in Las Cruces, Roswell, Hobbs, Carlsbad, Alamogordo, and Ruidoso. These developments not only enhance accessibility and service delivery but also contribute to local economic development through job creation and infrastructure investment.

Community banks continue to face significant challenges due to the increasing prevalence of fraud and scams across various payment channels. I appreciate the agencies' efforts to gather input on how the OCC, Federal Reserve, and FDIC can help reduce payments fraud for consumers, businesses, and financial institutions. Timely and coordinated agency action is both necessary and welcomed.

<u>Check Fraud</u>

Our institution has observed a notable increase in check related fraud incidents. These cases often involve checks being stolen from mailboxes, businesses, or individuals. Once obtained, the checks are typically altered, forged, or fraudulently deposited. While some customers are able to detect and report

the fraud in a timely manner, others are not, resulting in delayed return requests. In many instances, by the time a return is submitted, the funds are no longer recoverable, leading to financial losses for the bank.

In addition to the misuse of the physical check, fraudsters are increasingly leveraging the account and routing information printed on checks to initiate unauthorized ACH transactions. This creates a dual exposure—both check fraud and ACH fraud—from a single compromised item, compounding the risk to consumers and financial institutions alike.

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.

Mobile Deposit Fraud

Our institution has encountered several instances of mobile deposit fraud involving social engineering tactics. In a typical scenario, a customer is persuaded—often through online communication—to deposit a check via their mobile banking app with the promise of receiving a portion of the funds. These checks are later determined to be counterfeit. In some cases, the customer receives the check electronically, is instructed to print it, and is explicitly told to deposit it using mobile deposit only. Once the deposit is made, the customer is directed to forward a portion of the funds to a third party. While many of these attempts are intercepted, there are cases where the check is returned after the funds have already been sent, resulting in a loss to the customer.

Additionally, we have observed cases where a check is deposited via mobile deposit and then presented again in physical form at another financial institution. By the time the duplicate transaction is identified and the check is returned, the funds are often unrecoverable.

These examples underscore the growing sophistication of fraud schemes targeting mobile deposit channels and the need for enhanced safeguards and interbank collaboration. We recommend the development of industry wide standards for detecting and preventing duplicate check presentment across institutions, including mobile and physical deposits, to mitigate losses and improve fraud detection.

ACH Fraud

One recent case illustrates the complexity and evolving nature of ACH related fraud. A customer received multiple incoming ACH deposits—each in the amount of $2,500—for a total of $10,000. All transactions were posted under the customer's name. On the same day, the customer initiated outgoing wire transfers totaling $4,900. The first wire was processed; the second was halted after internal review. Upon investigation, it was discovered that the customer had been manipulated through an online relationship initiated via social media. The individual was led to believe the incoming funds were legitimate and was instructed to forward the money to a third party under the pretense of securing VIP event access.

This case highlights a recurring challenge: the originating institution was a large bank that proved extremely difficult to contact or collaborate with during the resolution process. As a precaution, the remaining funds were removed from the customer's account and placed into a general ledger account, pending any future inquiry from the originating institution.

We urge the agencies to establish clearer obligations for originating institutions to respond promptly to fraud inquiries and participate in collaborative resolution efforts.

Thank you for the opportunity to provide feedback on this Request for Information. Pioneer Bank appreciates the agencies' efforts and looks forward to continued collaboration with the OCC, Federal Reserve System, FDIC, and other stakeholders to strengthen protections against the growing threat of payments fraud impacting our customers and communities.

Christopher G. Palmer, CPA

President

Chief Executive Officer

Pioneer Bank

[redacted]

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**.

Unintended recipients should notify the bank upon receipt of the email.

Personal opinions, conclusions, or other information expressed in this email are neither given nor endorsed by the bank.

Pioneer Bank will never request personal or financial information via unsecured email. Please report to us any suspicious emails you receive claiming to be Pioneer Bank and requesting such information.