From:	Jessica Bradford
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, August 26, 2025 9:06:14 AM
Attachments:	image003.png image002.png

[redacted]

Ms. Jennifer M. Jones
Deputy Executive Secretary
Attention: Comments—RIN 3064-ZA49
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

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 Officer of Connect Bank, a 122M community bank located in Star City, 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 Federal Deposit Insurance Corporation (FDIC)'s request for information (RFI) on payments fraud.

Connect Bank is proud to be a cornerstone of financial stability and growth in Star City, Arkansas. Since our founding in 1925, we've remained deeply committed to serving the families, farmers, and small business owners who make up the heart of our rural community. Our history is rooted in trust, resilience, and a belief that banking should be personal, accessible, and empowering.

As a community bank, we play a critical role in supporting local economic development. We provide essential lending services to small businesses, construction loans for families, and

everyday consumers whether it be residential or personal—many of whom might not have access to traditional financial resources elsewhere. Whether it's helping a local entrepreneur launch their dream or guiding a family through their first home construction, Connect Bank is here to make financial opportunity a reality for everyone in our area.

We're not just a bank—we're neighbors, friends, and advocates for a stronger, more connected community.

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:

1. Check Theft and Washing: One incident involved a check stolen from the mail, altered (washed), and fraudulently deposited. This case resulted in financial losses for the bank, requiring extensive investigation and reimbursement efforts.
2. Money Muling via Other Banks: Fraudsters have used unsuspecting individuals as intermediaries to move illicit funds through accounts at larger financial institutions. While Connect Bank was not the originator of these transactions, we were impacted when funds were sent to unwitting customers under false pretenses, complicating recovery and compliance procedures.
3. Phone-Based Scams Targeting Customers: Some customers have been victims of phone scams where fraudsters acted as someone they are not or would threaten elderly into thinking they have to give them money and tricking them into logging into their online banking. These scams led to unauthorized transfers and compromised account security, requiring urgent intervention to freeze accounts and educate customers on fraud prevention.
4. Fraudulent checks received in the mail: These counterfeit checks often appear legitimate, bearing the names of real businesses or government entities, and are designed to trick recipients into depositing them and unwittingly participating in scams. When customers attempt to cash or deposit these checks, banks are forced to investigate and absorb the financial and operational burden of reversing transactions, protecting account holders, and maintaining trust. The fallout can be especially damaging for smaller banks with limited fraud detection resources, as they must navigate reputational risks and increased scrutiny while continuing to serve their local communities.

Regardless, people in our area have low-income and can easily be deceived into thinking a fraudulent check is a good check – because they need the funds.

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 are 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. We have educational handouts in our lobbies to educate on check fraud.
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. Larger banks are hard to contact a "real person", and they do not want to speak with us. Larger banks do not verify checks and do not want to cooperate to resolve issues regarding fraudulent checks drawn on them.
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. The dollar threshold is too large for community banks, as well. 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.
General Questions

Connect Bank has faced several types of fraud in recent years, each with its own set of challenges and criminal tactics. One of the most recent issues has been check fraud, where criminals steal checks and chemically "wash" them to alter the payee names and amounts. These altered checks are then deposited through mobile banking apps or at other institutions before the original account holder notices anything suspicious.

Social engineering and phone scams have also posed a significant threat. In these cases, fraudsters deceive customers into revealing sensitive information or authorizing transfers. These scams often target vulnerable individuals, including the elderly, and can result in substantial financial losses.

Another concerning trend involves money muling, where customers unknowingly receive and forward funds from unknown sources. These funds typically originate from larger institutions and are part of broader fraud schemes. The customer may be misled into thinking they're helping someone or earning a commission, when in fact they're facilitating illegal activity.

Online scams have also impacted customers. In these schemes, individuals receive fraudulent checks as part of a supposed transaction. The checks are usually for more than expected, and the recipient is instructed to send the excess funds elsewhere. When the check inevitably bounces, the customer is left liable for the loss.

Lastly, account takeovers have become increasingly sophisticated. Criminals use stolen credentials or manipulate customers into revealing login details, allowing unauthorized access to accounts. Once inside, they initiate transfers, change contact information, and attempt to drain funds before detection.

In response to these threats, Connect Bank has strengthened its fraud monitoring, increased customer education efforts, and collaborated closely with law enforcement to prevent future incidents. We have given our Frontline staff endless amount of training. I think all banks should be required to cooperate by verifying checks and if a fraudulent check is deposited, the bank that it is drawn on should be held liable for opening accounts for these fraudsters.

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,
Jessica Bradford, CCBCO
Compliance Officer
Connect Bank

Jessica Bradford, CCBCO
Compliance Officer
Phone: [redacted]
Fax: [redacted]