


From: [John Mark Williams](#)
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 18, 2025 4:40:21 PM
Attachments: [image001.png](#)
[image002.png](#)



Ms. Jennifer M. Jones
Deputy Executive Secretary
Federal Deposit Insurance Corporation
Attention: Comments—RIN 3064-ZA49

Mr. 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

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

I am the Executive Vice President and Chief Operations Officer of PriorityOne Bank, a \$1.2 billion community bank located in south/central Mississippi. 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.

Our bank has been serving mostly rural markets and local communities in Mississippi since 1905. Many of these communities would not have access to credit if it were not for local community banks such as ours.

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:

- One of our business customers informed us of two checks (\$56,301.53 and \$8,350.00) that had cleared their account with payees different from the payees on the original issued checks. Our

investigation revealed that both of these checks had been “altered”, and we made claim to the bank-of-first-deposit (“BOFD”) for reimbursement. The BOFD responded, saying these checks were “counterfeit”, not “altered” and refused to reimburse. We have since placed these funds back into our customer’s account and charged off \$64,651.53.

- Another business customer reported a check in the amount of \$162,818.27 cleared their account with a payee different from the payee on the original issued check. The company suspects the fraudsters obtained the original check through mail theft. We determined the check had been “altered” and have submitted a claim to the BOFD. We are still awaiting their response.
- A consumer received a phone call from a fraudster, pretending to be PriorityOne Bank and the customer to provide their online banking credentials to the fraudster. The fraudster then initiated six external transfers of \$1,000 each from another financial institution (“FI”) and deposited them into our customer’s account. Shortly after the funds were received, the entire amount was withdrawn via Cash App transactions. All six external transfers were subsequently returned against our customer’s account due to the originating FI not authorizing them. As a result, the account is now overdrawn by \$6,083.41 and will likely be charged off.

External Collaboration

- The 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. 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 and messaging 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 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.

- A business customer was a victim of business email compromise. The fraudster monitored this email account and, when they saw a wire transfer about to be made, they impersonated the business customer and presented the Bank with an imposter wire transfer request matching all details of the actual wire transfer except for the wiring instructions. The wire was sent but the Bank was soon notified that the business had not sent that request. The Bank immediately notified the “large financial institution” that the wire was fraudulent and to place a hold on the funds, pending investigation. We spent much of that day and the next day communicating with the “large financial institution” but were only able to get results when the Bank got the Secret Service involved. The “large financial institution” finally returned the funds to our business customer 90 days later.
- One of our business customers informed us of two checks (\$56,301.53 and \$8,350.00) that had cleared their account with payees different from the payees on the original issued checks. Our investigation revealed that both of these checks had been “altered”, and we made claim to the BOFD for reimbursement. The BOFD responded, saying these checks were “counterfeit”, not “altered” and refused to reimburse.
- 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.

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.

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.

General Questions

- Types of fraud that has impacted our bank and ways that criminals have tried to perpetrate those frauds.
 - Mail theft leading to check fraud is a huge issue; the fraudsters are getting checks that are being mailed for payment. They then either wash the check or create multiple counterfeit checks for distribution. We also see that ACH fraud starts shortly after this as well. They have the account number, so they start fraudulent ACH transactions.
 - Social engineering that leads to compromised online banking accounts and debit cards; the fraudsters use many different schemes to convince our customers to give them their online banking information, then they access our customers' funds and set up ACH payments to steal the money. They also use various schemes to take compromised debit card data and convince the customer to provide additional information that allow them to add our customers' card to the fraudster's mobile wallet. Then the fraudster uses the mobile wallet to spend our customers' funds.
 - Fraudulent "loan company" solicitations of our customers. Customers believe they are applying for a loan with excessive good terms and conditions. The fraudulent "loan company" then uses mobile deposit to deposit a fraudulent check into the customer's account for more than the loan amount requested. The customer is then instructed to return the overage via payment methods dictated by the fraudster. Obviously, the deposited check is then returned against our customer's account.
- Measures we have employed to prevent, detect, and mitigate fraud.
 - We use a third-party risk management software that is integrated with our core processing systems to prevent, detect and mitigate potential fraud. This software provides us with Our daily alerts on all check activity, in real-time as well as all check transactions from the previous day. This software also provides alerts, both real-time and previous day transactions for online banking activity, ACH activity, mobile banking activity and other channels.
 - We continuously communicate discovered fraud schemes within our markets with all of our personnel, particularly our front-line staff. We conduct regular training on fraud schemes, with a focus on proper procedures when encountering a suspicious transaction, as well as standard training for placing holds and declining to accept deposits if fraud is suspected. Our tellers also utilize a shared email group across all branches to timely notify one another of suspicious customers who may attempt the same scheme at different locations.
 - We coordinate with other financial institutions that participate in Section 314(b) information sharing. However, when reaching out to larger institutions, response times are significantly longer, often reducing the usefulness of the information due to delays.

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,

John Mark Williams
Executive Vice President & Chief Operations Officer
PriorityOne Bank

