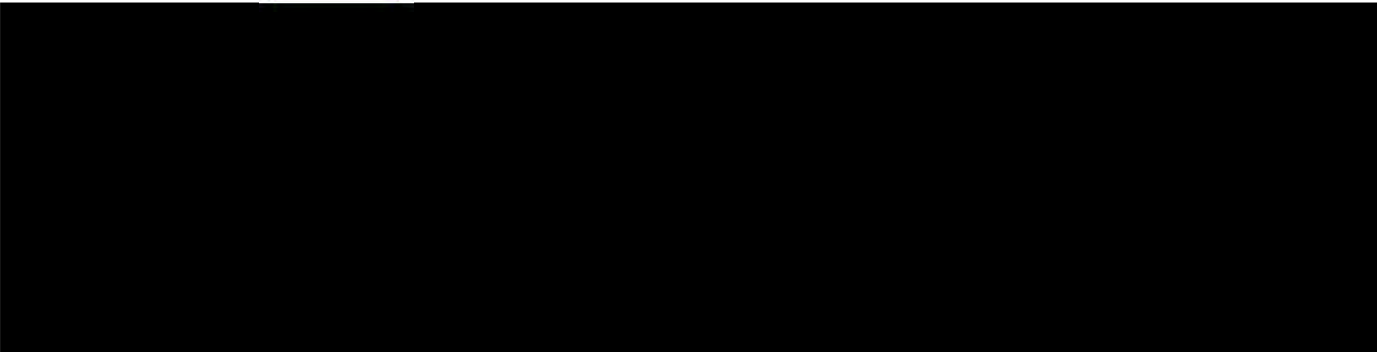


From: [Janet Silveria](#)
To: [Comments](#)
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)
Date: Thursday, September 18, 2025 7:51:24 PM
Attachments: [image001.png](#)



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

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

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

I am the President and Chief Executive Officer of Community Bank of Santa Maria (Bank). We are a 25-year-old community bank with \$400 million in assets with two branch locations in Santa Maria, California. 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.

As a cornerstone of our community, our bank is deeply committed to serving all stakeholders—shareholders, customers, employees, and the broader public. We prioritize the safety and protection of those we serve and actively participate in fraud prevention efforts. Through partnerships with local organizations like senior centers and schools, we work to raise awareness and provide resources. Each March, we host free, community-wide document shredding events every weekend to help safeguard personal information and promote security by taking the opportunity to share information about prevalent fraud and scams.

We commend the agencies for releasing this RFI and inviting feedback on how the OCC, Federal Reserve System, and FDIC can support consumers, businesses, and financial institutions in combating payments fraud. With community banks facing increasing threats from fraud and scams across various payment channels, decisive agency intervention is both

timely and essential.

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

- We have incurred additional training costs and constantly run the risk of alienating our customers: we have found it necessary to strengthen our staff training to include effective strategies for discussing fraud prevention and detection with customers. Because financial transactions can be deeply personal, it's essential that our team communicates the purpose behind these conversations with empathy and clarity—emphasizing that our questions are rooted in a commitment to protecting our customers. While certain regulatory requirements like KYC and CTR reporting are standard across all financial institutions, these proactive fraud prevention efforts can sometimes be perceived as overly inquisitive or intrusive, as they are not occurring at other institutions. It's crucial to strike the right balance between vigilance and the risk of compromising the trust and respect we've built with our customers.
- We have incurred additional data processing expenses: we have invested in additional fraud detection software including positive pay and fraudulent payment identification systems. These costs are essentially absorbed by the bank. While in some instances we can partially recoup costs on positive pay, what we can competitively charge falls significantly short of actual expenses.
- We have fallen victim to outdated check return policies and regulations: check fraud is increasing exponentially, and it is difficult for both the Bank and our customers to recoup losses. In almost every instance of check fraud, the bank of first deposit is a large bank. This creates significant challenges when attempting to follow up on a fraudulent check claim. It is difficult to get a live person on the phone who can assist, and there is no one to hold accountable when a return request is denied.
- We have difficulty recalling fraudulent wires: similar to fraudulent checks, the receiving bank is typically a large institution. We are consistently challenged with getting someone to assist and respond.

We believe appropriate actions from the OCC, Board/FRS, and FDIC include the following:

- Facilitate external collaboration through centralized data collection and information sharing: we support collaborative stakeholder efforts to address payments fraud. Fraud and scams persist across state borders, so national stakeholder collaboration is necessary. Collaboration should include banks, regulators, law enforcement, and community organizations. Currently available reporting mechanisms are 'one-way' communications and frequently do not result in any type of acknowledgement or response. Further, the information is not shared amongst all stakeholders. An automated data collection and analysis reporting system that provides a safe harbor for participants would be beneficial. It would be important to consider the operational impact on the organizations using the system and ensure additional costs and operational burden are prevented or minimized.
- Consumer, Business, and Industry Education: The most impactful form of fraud education lies in proactive transaction intervention. However, as noted earlier, this practice is not consistently applied across financial institutions. Educating the public about specific fraud schemes should go hand-in-hand with setting expectations that their financial institution may ask detailed questions as part of a broader effort to safeguard their assets. Additionally, equipping businesses with guidance on sound banking practices—such as account oversight, separation of duties, timely review of financial records, and implementing secondary controls—can significantly enhance early

detection and reporting of fraudulent activity. It would be important to provide education via multiple channels as different demographics receive information differently. For example, senior citizens and persons in rural areas may not be comfortable with, or able to access, web-based information.

- Regulation and Supervision: check and wire fraud are a significant issue, often involving much larger amounts than other forms of electronic payment fraud. We are concerned that some large financial institutions are not exercising sufficient CIP/KYC processes and are opening accounts that are leveraged by fraudsters. Additionally, as previously stated, we have encountered significant difficulty resolving interbank disputes regarding fraudulent checks and wires. We have instances of successful collection, but it requires extensive intervention and follow-up on our part and can take several months. We also have instances where claims are simply denied and we have no further avenue to explore and are unable to speak to anyone at the depositing institution. Regulatory intervention to ensure large financial institutions are held accountable for losses when opening fraudulent accounts and requiring them to actively participate and engage with the victim bank would help prevent losses to customers and banks.

Changes to Regulation CC could significantly enhance our ability to prevent and mitigate check fraud. For instance, extending the return deadline for fraud-related items, clarifying the 'reasonable cause to doubt collectability' exception, and revising key definitions—such as 'altered' and 'alteration'—would provide greater clarity and flexibility in addressing fraudulent activity. We strongly caution against any reduction in check hold times. These holds are a critical safeguard, allowing institutions time to detect and respond to potential fraud. In numerous cases, we have received timely check returns after the hold period expired, resulting in financial losses for our customers. Preserving adequate hold times is essential to maintaining consumer protection and institutional integrity.

In response to the General Questions, we note the following:

- Check fraud remains one of the most damaging forms of financial crime, affecting both banks and their customers. Techniques such as check washing have grown increasingly sophisticated and harder to detect, particularly under the Check 21 electronic presentment framework. Many of these fraudulent checks originate from mail theft, yet there appears to be limited action from the U.S. Postal Service to address this growing threat. As part of broader efforts under the banner of “external collaboration,” the USPS should be recognized and engaged as a critical stakeholder in combating check fraud. Their involvement is essential to addressing the root of this issue and enhancing protections across the financial ecosystem.
- Fraud detection programs for debit and credit card transactions have proven highly effective, largely because they rely on reactive customer involvement—such as confirming suspicious activity—rather than proactive engagement. In contrast, other fraud prevention tools like ‘Positive Pay’ require customers to take a more active role, such as submitting files of authorized payments. This added responsibility often discourages participation. Similarly, expecting customers to notify the bank in advance of large purchases or transfers would likely face significant resistance and, subsequently, little effectiveness. The success of fraud prevention efforts often hinges on minimizing friction and aligning with customer behavior and expectations.

We again wish to express our gratitude to the OCC, FRS, and FDIC for seeking public input

on ways in which these agencies may help banks and other stakeholders mitigate and combat fraud and I personally thank you for the opportunity to participate.

