[redacted]

From: Wendy Nagle <[redacted]>
Sent: Thursday, August 28, 2025 3:32 PM
To: Comments
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)

Follow Up Flag: Follow up
Flag Status: Flagged

[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 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. I am the Senior Operations Officer of PennCrest Bank, a $230 million community bank headquartered in Altoona, Pennsylvania. In this role, I oversee operational processes that directly impact our ability to manage risk, protect our customers, and ensure compliance. As a community bank, PennCrest serves customers who rely on us for safe and reliable financial services, and we face unique challenges in mitigating fraud while balancing resource constraints.

Like many mutual savings banks, PennCrest has been serving our communities for generations, with roots tracing back to 1886. We focus primarily on retail banking, with a strong emphasis on residential mortgage lending, and we also provide small business banking and lending, largely to support the needs of our retail customer base. This long-standing commitment to individuals, families, and businesses in our market shapes both our perspective and our priorities when it comes to fraud prevention and regulatory policy.

I commend the agencies for issuing this RFI and for seeking input on how the OCC, the Federal Reserve System (FRS), and the FDIC can take action to help consumers, businesses, and financial institutions better 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:

- Altered/Fictitious Checks
- Debit Card Fraud
- Friendly Fraud

External Collaboration

- The Bank supports collaborative stakeholder efforts to address payments fraud. Because fraud and scams often transcend state borders, a coordinated national approach is essential to effectively combat the problem. At the same time, national initiatives must take into account the resource constraints faced by individual community banks when evaluating participation.
- Collaboration at the local and regional level—among community banks, federal and state regulators, law enforcement, community organizations, and other stakeholders—can also serve as a highly effective means of building connections and facilitating the timely sharing of information within communities.

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 serving the elderly and those who may be less comfortable with technology.

Regulation and Supervision

- 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. Financial institutions should be permitted, and where appropriate required, to participate in the validation of checks to confirm their legitimacy or identify potential fraud, without concern for violating Regulation P or the requirement to have the account holder present on the call. Such participation is critical to maintaining the integrity of the payment system and protecting both customers and institutions.
- 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 be afforded the flexibility to extend hold times when circumstances warrant. Additionally, increasing the amounts required to be made available on the same day or the following day heightens the risk of losses to both customers and financial institutions. To mitigate this risk, consideration should be given to decreasing, rather than increasing, these immediate availability thresholds.

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.

PennCrest has experienced a wide range of fraud, with incidents increasing year over year. One area for immediate improvement would be requiring all financial institutions to provide valid and up-to-date contact information to assist other banks in determining the legitimacy of items. Currently, many large institutions will not verify funds, nor will they discuss suspected fraudulent items, which makes fraud prevention more difficult across the industry.

Enhanced due diligence when opening accounts, particularly online accounts, is also critical. Institutions should be required to assess the legitimacy of account applications and the rationale for opening accounts outside of a customer's normal geographic area. For example, one of our customers in Pennsylvania was victimized when a fraudster opened an account in his name at a bank in Hawaii. That institution should have denied the application or required the individual to appear in person to verify identity and justify the need for an account in that state. While our customer ultimately lost money due to this scheme, losses were limited thanks to the diligence of our customer service representative.

PennCrest has already implemented several new procedures, including required check holds, daily review of deposits over a set threshold, and verification of checks with paying banks whenever possible. We do not open accounts for individuals outside of our market area, and we have expanded fraud-awareness training for our staff. We are also evaluating additional systems to strengthen fraudulent check detection.

Debit card fraud continues to present a significant challenge. A more effective approach would include holding merchants accountable for validating customer identity before processing a transaction or incorporating two-factor authentication at the point of sale. While banks have implemented safeguards such as text, email, and phone alerts, transaction blocking by region or merchant type, and real-time monitoring, fraudulent transactions still occur.

Friendly fraud—where customers dispute legitimate transactions—adds another layer of complexity for community banks. While consumer protection is critical, regulatory approaches must strike a balance between protection and accountability. Currently, the system often places the entire burden of loss on banks, creating opportunities for abuse and increasing fraud-related costs. Potential measures to mitigate friendly fraud include encouraging merchant participation in enhanced verification methods, providing clearer standards to distinguish between fraud, scams, and disputes for consistent treatment, and creating safe harbors for banks when sufficient authentication has been obtained, thereby limiting liability for legitimate transactions later disputed by customers.

Although some enforcement measures have been applied to P2P vendors, customers are still too often directed back to "ask their bank" for resolution. Stronger accountability standards for non-bank participants in the payments system are needed to better protect both consumers and financial institutions.

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,
Wendy Nagle
Senior Operations Officer
PennCrest BANK

Wendy Nagle
Senior Operations Officer
phone: [redacted]
toll free: [redacted]
fax: [redacted]
www.penncrest.bank

[redacted]

Wendy Nagle
Senior Operations Officer
phone: [redacted]
toll free: [redacted]
fax: [redacted]
www.penncrest.bank

[redacted]