

[REDACTED]

From: Sharon Anderson <[REDACTED]>
Sent: Friday, September 5, 2025 4:27 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]

Jennifer M. Jones
Deputy Executive Secretary, Federal Deposit Insurance Corporation
RIN 3064-ZA49

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

I am the President and CEO of Williamstown Bank, a \$225 million community bank located in Williamstown, WV. 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.

Williamstown Bank has proudly served the Wood County, WV region since 1919. As one of the few locally owned and operated institutions in our area, we focus on offering products and services to small businesses and consumers which help them thrive. We especially pride ourselves on our niche, personalized financing we can offer our customers, as our lenders still have local lending authority and can work with our customers on a case by case level.

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, my Bank has been affected by payments fraud in many ways including:

- Increase in Friendly Fraud claims – the burden of proof is on the financial institution and current regulations such as Reg E requiring banks to give provisional credit pose great risk for especially community banks.
- The addition of multiple employees/roles/systems to combat fraud. Fraud investigation and mitigation is a timely matter, often causing hours dedicated to researching fraud (again the burden of proof is on the institutions). There is no centralized system to share information that would allow a database for banks to search when working fraud cases. The additional systems and employees are expensive, especially considering the scalability of the community banking system.
- The inability to collect or even contact larger banks for things such as breach of warranty in a timely manner that allows small banks like mine to recover losses. Many of these larger institutions can skirt

Know Your Customer rules, etc. forcing smaller banks to take losses on things such as mobile deposit items. This is especially frustrating in cases the bank of first deposit (usually larger banks) doesn't require endorsements such as "For Mobile Deposit" only allowing checks to be presented for payment multiple times. Many fraudsters open accounts at these larger banks because they can easily perpetrate fraud. If a small bank like mine were to behave in the way of these larger institutions we would be held accountable, the larger institutions need to be treated the same.

- Fraud payments from check to ACH, debit, and wire have all increased significantly. Our losses have increased greatly in recent years, and we have limited resources from which to report and research for information that could allow us to be proactive in fighting fraud.
- The need for education is so great, trying to hit as many platforms as possible, along with grass roots efforts can again be timely and costly.

I have given some general examples of how my bank overall has been affected by fraud payments, but I want to give one specific example that shows first, the level to which some will go to claim fraud, but also the challenges of an antiquated regulatory system that has not yet caught up to the challenges of today. I do want to also mention how collaboration worked to help us prevent a large loss.

Recently, we had a customer claim \$140,000 in ACH fraud with the online gambling platform Draft Kings. We believed the customer had initiated these transactions due to past history, but they insisted and were willing to sign affidavits for each of the over 800 individual transactions within the 60-day timeframe. We also were bound by Reg E requiring us to give provisional credit within a 10-day period if we knew the investigation would exceed that timeframe. We had extensive legal fees, calls with regulators, and about 4 full-time employees working this one case for multiple days.

We were fortunately able to contact the fraud department at Draft Kings, where the customer had also filed a claim for fraudulent activity, in hopes of gathering enough information to prove the customer had initiated the transactions. Due to the size and scope of the investigation, and having to work with Draft Kings, we knew we would be outside the 10-day timeframe and were required to give this customer provisional credit. At the time, the process was manual, and it took one employee four full days to provide individual credit for each transaction, and we had to hope the customer wouldn't run with the provisional credit. Draft Kings was able to provide us with everything from IP addresses, geo tagging of transactions to within two miles of the customer's house, and all the information we needed to prove the customer initiated the activity. We were fortunate this time, the customer admitted to having an online gambling addiction, and that they had read on an online forum they could just go to their bank and contest the charges, and we would be required to reimburse them for the losses. The requirement to provide provisional credit in this case put us at a tremendous risk had the customer run, as we could not even put a hold on the credit given despite being sure it was legitimate activity.

The collaboration we had with Draft Kings proved to be vital and would be a great example for the entities within the financial system, law enforcement, etc. to follow.

The concern is, the information customers read online is not always accurate, can cause them to make large claims on losses due to things such as gambling, crypto, and the requirement to provide provisional credit in such a short timeframe greatly increases the risk for small banks like mine to realize what could be catastrophic losses. Timeframes for large claims where friendly fraud is suspected should be considered before providing provisional credit. We need regulations to match the size of the risk and to be tiered.

This is just one example of many I could provide. We recently suffered a loss due to a customer being used as a mule to move stolen money because of a romance scam. We reported the loss to local law enforcement, and they now have uncovered what has grown into what appears to be a multi-million-dollar scam ring involving multiple local financial institutions. Law enforcement working the case have stated more collaboration between the

financial system and law enforcement would help track and prevent future losses, along with bettering the chances of catching the perpetrators.

I am a lifelong community banker. We proudly serve our community and the relationships we build truly differentiate us from the larger banks. We often are the economic backbone of our rural communities, and the challenges we face today because of fraud only hamper our ability to serve our customers.

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,

Sharon K. Anderson
President & CEO
Williamstown Bank
Phone: [REDACTED]
Fax: [REDACTED]



The Email communication and any attachments may contain confidential and privileged information intended only for the addressee. If you are not the addressee, any review, disclosure, use, dissemination, or disclosure of this information by you is prohibited. If you have received this transmission in error, please delete it, destroy all copies, and notify me at Williamstown Bank by telephone at [REDACTED].