

From: [Amy Evans](#)
To: [Comments](#)
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)
Date: Monday, August 25, 2025 2:02:01 PM

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 the Vice President Corporate Security Officer of D.L. Evans Bank, a 4.75-billion-dollar community bank located in Idaho. 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.

D.L. Evans Bank is a community bank with a footprint in southern Idaho and Northern Utah. We have been in business since 1904 and have a diverse portfolio that includes consumer, small to medium size business (We are a preferred lender for the Small Business Administration) and agricultural clientele. We are the largest community bank in the state of Idaho, and our employees regularly give back on average over 8,000 hours per year to the communities we serve through volunteerism, which often includes educating community members about current fraud trends and how to avoid being victimized.

I applaud the agencies for issuing this RFI and seeking input on ways that the OCC, Federal Reserve System (FRS), and the FDIC could take action 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:

- Numerous customers have been affected by invoice fraud where a fraudster will use business email compromise or account takeover to re-direct payments for goods or services to a fraudster. Often by way of wired funds or ACH payments.
- Numerous customers have fallen victim to imposter scams where they believed they were communicating with a bank employee and provided account details, account numbers and log in credentials.
- Numerous customers have had their checks stolen and counterfeited, where fraudsters were able to either successfully cash checks or purchase goods or services.

- Customers have been victimized by mobile payment fraud, through numerous P2P applications.
- Numerous customers have been victims of debit and credit card fraud because of data breaches where card details were sold on the dark web.
- Numerous elderly customers have fallen victim to romance and other online scams that were the result of emotional manipulation – taking significant amounts, if not all their retirement savings.

I would suggest the following actions to mitigate these types of payment fraud:

- 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.
- 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.
- 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 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. Large institutions will not talk to our fraud department or if they do, they only provide limited information. They will not verify funds or provide basic, non-personally identifiable information related to checks being presented at our institution.
- 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 definition could be revised (i.e. “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.
- 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.

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,

Amy Evans

Amy Evans Vice President Senior Administrative Officer | Corporate Security Officer



Tel [REDACTED] | [REDACTED]
D.L. Evans Bank | www.dlevans.com

Disclosure Statement: The information contained in this e-mail transmission is intended only for the recipient named above. If the reader of this message is not the intended recipient or the intended recipient's agent, you are hereby notified that any dissemination, distribution or copying of the information contained in the e-mail transmission (other than to the intended recipient) is prohibited. If this transmission has reached you in error, you are asked to notify us as soon as possible and destroy the e-mail documents. Thank you for your cooperation.