[redacted]

**From:** David K. Mulvany <[redacted]>
**Sent:** Sunday, September 7, 2025 11:12 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]

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 EVP/Chief Operations Officer of Security Bank of Kansas City (Bank), a $3.6 billion community bank located in Kansas City. 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.

Founded in 1933, Security Bank of Kansas City has been serving the Greater Kansas City area for nearly a century, and we currently have 34 branches in both Kansas and Missouri. As a locally and privately owned, state-chartered community bank, the Bank was born from a single idea: a bank dedicated to its local community. We take pride in lasting relationships — many households have banked here for multiple generations, underscoring our enduring commitment and stability. Recognized for our strength and performance, we have been ranked the Strongest Large Bank in Kansas City by the Kansas City Business Journal in 2024 and 2025, reinforcing our financial soundness and reputation. Through generations of service, robust small-business lending, and personalized consumer banking, we continue to play a vital role in nurturing financial resilience and opportunity throughout the Kansas City region.

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, we have been affected by payments fraud in the following ways:

- **Check Fraud**- We see fraud starting with checks intercepted from mailboxes and/or the U.S. Postal Service by fraudsters. The checks are then either washed, altered, or counterfeited, and then deposited into the fraudsters' accounts at other banks. Working directly with other

financial institutions, especially larger banks, is a very difficult and lengthy process, and often the BOFD is uncooperative even though their customer is depositing fraudulent funds. They will delay responding and returning credits hoping you do not have the means to take legal action. We are concerned that some larger financial institutions are not exercising sufficient CIP/KYC processes and opening accounts that are being leveraged by fraudsters.

- **ACH and Wire Fraud** - We see fraud starting with phone spoofing or email compromises to gain access into online banking in order to facilitate ACH or wire payments. Once the fraudsters gain access and create an outgoing payment, we then have to work directly with the banks receiving those payments. Because each bank's primary focus is to protect their best interests (and not stopping fraud), many times banks are less than willing to cooperate in returning payments sent due to fraud. Again, insufficient CIP/KYC processes with larger financial institutions are allowing fraudsters to structure fraudulent payments throughout the banking system with no watch or accountability from the banks.

The Bank supports collaborative stakeholder efforts to address payments fraud. Criminal networks operate globally, while defenses are fragmented and siloed. 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. There is no single, standard mechanism or source for collecting or reporting fraud data. Barriers to collecting data, including operational, legal, and regulatory constraints, make it difficult to provide actionable, centralized fraud data. If FinCEN or a like organization created a central depository for fraud data that all banks could utilize, it would allow the banks to work collectively against fraud opposed to every bank for itself. The fraudsters are working in unison, the banking system is not.

Payments fraud is no longer a nuisance — it's a systemic crisis. Banks face rising losses, regulators are pushing liability onto them, and fraudsters keep outpacing defenses. Without stronger industry collaboration, smarter fraud detection, and more robust consumer protections, payments fraud will continue to spiral.

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,

**David Mulvany**
***Executive Vice President***
***Chief Operations Officer/Cashier***
[redacted]
SECURITY BANK
OF KANSAS CITY