



September 18, 2025

Subject: Request for Information on Potential Actions to Address Payments Fraud  
Re: Docket ID OCC-2025-0009

---

As the Chief Executive Officer of a community bank, I appreciate the opportunity to provide feedback on the topic of *Collaboration to Detect, Prevent, and Mitigate Payments Fraud*. Like many institutions, First Bank has experienced an increase in fraud cases. We value the chance to contribute any input that may help shape future policy and procedures in this critical area.

---

## REGULATION AND SUPERVISION

### ***Regulation E:***

Though not specifically requested here, a review of Regulation E, in connection with this request for information on payment fraud is, in our view, crucial. The Electronic Fund Transfer Act of 1978 provides guidelines designed to safeguard consumers who engage in electronic funds transfers (EFTs). These protections include clear reporting mechanisms, investigation timelines, notice requirements, and provisions to reimburse consumers under defined circumstances. EFTs encompass transfers through ATMs, point-of-sale terminals, and the ACH network, among others, though important exclusions remain, such as paper checks and domestic wire transfers.

In practice, fraudulent activity often crosses regulatory boundaries, exploiting gaps in oversight. One common example we encounter involves fraudsters persuading customers to use debit cards to purchase gift cards, then demanding the gift card details. Because the transaction is technically authorized by the consumer, it typically falls outside the definition of an “unauthorized electronic fund transfer” under Regulation E. This leaves the consumer responsible, but banks expend significant resources fulfilling investigation and notice requirements and, in many cases, reimburse the consumer to preserve the customer relationship.

The 60-day liability window established by the regulation is outdated in today’s rapidly evolving fraud landscape, frequently resulting in banks absorbing the cost of multiple

fraudulent transactions on a single account. In this digital world, consumers are notified more quickly of fraudulent activity, given their access to electronic bank statements and fraud detection systems many banks utilize. Likewise, Regulation E allows for instances of consumer negligence, requiring banks to absorb losses even when customers compromise their own security—such as storing debit card information in easily accessible places.

Another area of concern is Regulation E's ambiguity surrounding error resolution in transactions conducted through non-bank P2P providers, such as Cash App and PayPal. Frequently, the consumer's bank, despite having no role in the underlying transaction, is left to bear the burden of resolving disputes, often without meaningful support from the non-bank provider. Although the CFPB once issued a final rule (now repealed) to extend supervisory authority over certain non-bank P2P companies, that rule did not resolve the fundamental question of how liability and responsibility should be allocated between banks and non-banks in fraud situations.

***Regulation CC:***

While cashier's checks are backed by a bank, counterfeit versions are increasingly used by fraudsters in various scams. Advanced printing technology and online scams have made fake checks more convincing, and victims are often left responsible for the losses. Many banks must eventually charge off the customer loss, which in return creates a financial loss for the bank. There is no justified reason to allow cashier's checks faster availability given the fact check and bank fraud is becoming more common. Being that check fraud is so prevalent, revising Reg CC to allow banks to hold more types of checks and money orders may not only prevent the customer from incurring a loss, but also the bank. In addition to allowing more types of checks to be held, as one of the six exceptions within Reg CC, "reasonable cause to doubt collectability" should be expanded to include "suspected fraud".

---

## **PAYMENTS FRAUD DATA COLLECTION AND INFORMATION SHARING**

A centralized fraud database could greatly enhance early detection among financial institutions; however, privacy would be a great concern unless there were some safe harbor provisions built in. Information sharing between financial institutions helps combat fraud by potentially revealing patterns not seen by a single financial institution, allowing for faster fraud detection as well as prevention. It could also benefit by potentially blocking suspicious activity in real-time across different organizations. While 314(b) information

can be used in certain circumstances such as suspected money laundering, there is no guarantee that a response will be timely or given at all by the receiving bank.

---

One of the most pressing needs for community banks is stronger notification requirements to the bank of first deposit (BOFD) for all fraudulent checks. Such measures would help banks of every size, but particularly smaller institutions, mitigate losses more effectively. If banks were able to delay funds availability when fraud indicators or red flags appear on a customer's account, it would provide critical time to validate transactions and protect consumers. Similarly, the ability to place longer holds on altered checks, without making funds immediately available, would better align with today's fraud environment.

Community banks also need greater protection when it comes to timely collections, as the current system places higher risk and operational burdens on smaller institutions. Clearer interpretations of UCC and Regulation CC would help reduce confusion, while the current two-day deadline for investigations is simply too short to properly address altered or fictitious checks. Flexibility for banks to exercise prudent judgment without fear of examiner criticism would also improve fraud prevention practices.


Unfortunately, small banks often struggle to obtain cooperation from the largest institutions. Many community banks cannot even reach a live representative at the nation's top five banks, leaving them with little to no support in resolving fraud cases. Larger banks' high mobile deposit limits also create additional exposure, opening a "back door" for fraud that disproportionately impacts smaller banks tasked with collecting. To address this imbalance, the Federal Reserve could consider requiring fraud reporting across all payment rails, including checks, to strengthen system-wide detection.

Fraud is also increasingly not local, which highlights the need for a unified governing body that enables collaboration among financial institutions and enforcement agencies. In addition, encouraging businesses to use ACH instead of mailing paper checks for accounts payable could help reduce fraud exposure. Regulations should also extend more clearly to non-bank money movement providers, ensuring consistent oversight across the financial system. Finally, concise, straightforward guidance that reflects the scale and operational realities of community banks would go a long way in reducing uncertainty and supporting recovery efforts in fraud cases.

---

In conclusion, banks and regulators face the same adversaries in financial criminals and we are united in our commitment to protecting consumers. As banking technologies continue to evolve, collaboration is the key component to combat payment fraud and redefine solutions. Strengthening collaboration across the industry and modernizing guidance and regulations to reflect the realities of online banking will be key to reducing fraud.

Thank you for your attention, consideration, and support.



Charlie Lewis  
President & CEO  
First Bank

First Bank

