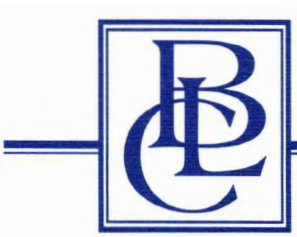

BANK OF LINCOLN COUNTY

[redacted]

September 18, 2025

Jonathan Gould
Comptroller of the Currency, Office of the Comptroller of the Currency
Docket ID OCC-2025-0009

Benjamin W. McDonough
Deputy Secretary, Board of Governors of the Federal Reserve System
Docket No. OP-1866

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

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

I am the Chief Executive Officer of the Bank of Lincoln County, a $222 million community bank located in Fayetteville, Tennessee. I appreciate the opportunity to respond to the joint Request for Information (RFI) on payment fraud issued by the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (FRS), and the Federal Deposit Insurance Corporation (FDIC).

Unfortunately, like many community banks across the country, our institution has faced numerous instances of check fraud, which one check alone costing us over $100,000. These challenges have made me a committed advocate for community banks and have driven me to gain a deep understanding of fraud prevention and mitigation strategies. Frauds and scams affect our bottom line as well as our relationships with our customers and our reputation in our communities.

In addition to my role at the Bank of Lincoln County, I currently serve as the Chair Elect of the Tennessee Bankers Association, Tennessee's Federal Delegate to the Independent Community Bankers of America (ICBA), Vice Chair of ICBA's Operations Committee, and as an At-Large Delegate on ICBA's Board of Directors. Through these roles, I have had the opportunity to participate in a national Check Fraud Task Force and to engage with the UCC Permanent Editorial Board to discuss the evolving threats of check and wire fraud.

Thank you for the opportunity to provide feedback on the five areas identified in the RFI. I respectfully offer the following insights based on my experience as a community bank CEO who has dealt with numerous incidents of check fraud:

1. External Collaboration

Improved communication and collaboration among banks, regulators, law enforcement, and other stakeholders is essential to combating fraud. While fraud is a frequent topic of discussion across the industry, my experience suggests that many participants, including well-meaning stakeholders, do not fully understand the relevant laws, the operational processes involved, or the full impact on financial institutions and customers.

Meaningful collaboration must go beyond discussion. It should include clear channels for information sharing, prompt responses from larger financial institutions, and a shared understanding of each party's responsibilities under current law. Without that, smaller institutions are left bearing the brunt of fraud with little recourse.

2. Consumer, Business, and Industry Education

In my experience, the most effective fraud education happens through direct and ongoing contact with customers. At the Bank of Lincoln County, we proactively communicate with customers through social media, in-app alerts, and presentations at locations like our local senior center. Despite these efforts, scams still occur often.

We also work with small businesses to educate them on best practices and offer fraud prevention services. While printed materials can support these efforts, they are not effective on their own. Education must be active, frequent, and tailored to the specific vulnerabilities of each customer segment.

3. Regulation and Supervision

Fraud-related regulations must be appropriately tailored to institutions of varying sizes. Tiered compliance requirements and flexible deadlines are essential for community banks with limited resources. There is also an opportunity to enhance supervisory guidance around internal controls and fraud response expectations.

Our most frequent experience with fraud involves altered checks that were originally stolen from the mail and then deposited, often via mobile deposit, at large financial institutions. In these cases, the perpetrators frequently exploit gaps in Know Your Customer (KYC) and Customer Identification Program (CIP) compliance.

We've seen a recurring pattern: LLCs are established, accounts are opened and then closed without the LLC ever filing an annual report. The same individuals then open new accounts under new LLCs. In some cases, I've traced the registered addresses of these fraudulent accounts to virtual office spaces that were never occupied by the business. Despite having clear evidence of fraud, we've been unable to pursue negligence claims due to the courts' interpretation that banks owe a duty of care only to their own customers.

One such case resulted in a loss of over $100,000 for our small bank.

During a meeting with the UCC Permanent Editorial Board and other banking representatives, a large institution's participant stated, "It is impossible for us to know our customers." That statement, unfortunately, reflects the core of the problem. Community banks *do* know our customers, and when we suspect a check is fraudulent, we act accordingly. We place holds, review deposits, and ensure our customers can cover returns. We do not allow high-dollar checks (some over $50M) to be mobile-deposited without direct review yet we see those practices occurring at much larger institutions. In relation to this, Reg CC hold times should not be shortened, and could even be extended.

My attempts to work with larger financial institutions to resolve fraud issues have been time-consuming and ineffective. In one instance, it took me over six months to receive a response, and this was only after asking ICBA and ABA to help locate a contact.

In May 2024, I discovered that some banks retain funds on checks returned beyond the 24-hour window but do not proactively return those funds unless explicitly asked. After following up three times on one such case from May 2023, I was eventually reimbursed. This same issue happened to another community bank in Tennessee just last week. Without my guidance, they would not have asked and would not have received the funds.

Fraudsters are becoming more sophisticated. What once was limited to altering the payee is now escalating to digital manipulation of the entire check: borders, dates, security language. This delays identification, and by the time the fraud is discovered, the check often falls outside the 24-hour return window. Initially, these items are returned for breach of warranty, making the bank of first deposit responsible. However, increasingly, these banks later claim the checks are counterfeit, shifting liability to the drawee bank. Most community banks lack the resources to pursue legal action in these disputes and must absorb the loss which I believe is fundamentally unjust.

The bank of first deposit is in the best position to prevent fraudulent items from entering the financial system. They are responsible for account onboarding, fraud analytics, and customer due diligence. Shifting liability away from them discourages rigorous controls and enables bad actors. While solutions like Positive Pay offer some protection, they are not universally available and can be difficult for customers to use.

If community banks are forced to absorb these losses, while large banks with weak KYC practices remain shielded, then the playing field is anything but level. If these losses were borne by *consumers* or *small businesses* instead of community banks, I believe that regulatory action may have already have been taken.

4. Payments Fraud Data Collection and Information Sharing

Most community banks already track losses related to debit card fraud, check fraud, and wire fraud, and this data could be reported in a straightforward and consolidated manner. Reporting

total loss figures would not be burdensome and could provide valuable insight at an industry level.

Banks are often hesitant to share customer-related fraud data with other financial institutions due to concerns about potential liability or conflicts with existing privacy regulations and policies. To address this, clear regulatory guidance would be helpful in outlining what types of information can be shared and under what circumstances. Additionally, the establishment of a safe harbor provision, applicable when certain conditions are met, would go a long way in encouraging financial institutions to share meaningful fraud-related data without fear of legal repercussions. Currently, even if we call another financial institution, they will not even validate if a check is authentic or if funds are available.

5. Reserve Bank Operator Tools and Services

The FRS could implement mandatory fraud reporting for ACH, wire transfers, and checks that are similar to the requirements in place for FedNow. Collecting this data would create a valuable resource for identifying fraud patterns and improving prevention efforts across the industry. However, it is essential that any reporting requirements be designed to minimize the burden on community banks, ensuring that compliance is both practical and proportional to the resources available.

Thank you so much for the opportunity to respond to the RFI. I am passionate about these issues and am hopeful that we can work together to combat fraud and better protect our industry. I would welcome a call or an email to discuss these issues further.

Sincerely,

Gay G. Dempsey, CEO