

From: [Nicole Simmons](#)
To: [Comments](#)
Cc: [Scott Cocanougher](#); [Daniel Watson](#)
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)
Date: Thursday, September 18, 2025 3:37:54 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 BSA/Compliance Officer of First Community Bank of Tennessee (FCB), headquartered in Shelbyville, Tennessee with a consolidated asset size of \$859 million as of 8/31/2025. I appreciate the opportunity to respond to the Request for Information (RFI) issued by the Office of the Comptroller of the Currency (OCC), the Federal Reserve System (FRS), and the Federal Deposit Insurance Corporation (FDIC) regarding payments fraud. We commend the agencies for seeking input on how to better support consumers, businesses, and financial institutions in mitigating this growing threat.

First Community Bancorp, Inc, a one-bank holding company wholly owns the bank. FCB operates a wholly-owned mortgage subsidiary, First Community Mortgage (FCM), which lends in 48 states. All of our entities are headquartered in Shelbyville, Tennessee. The bank has three branches in addition to our main office and offers various products and services including commercial, agricultural, residential and consumer loans, with commercial and residential lending serving as the primary business focus. In addition, the bank offers a variety of deposit products including checking, savings, money market, and certificate of deposit accounts.

According to FDIC Deposit Market Share data as of June 30, 2024, FCB ranked 1st out of 8 financial institutions operating in our area, with a 47% deposit market share. FCB's subsidiary, First Community Mortgage (FCM) ranked 1st compared to other lenders in our local area with 10.1% in dollar and 18.8% in volume in 2023 HMDA reporting.

As a community bank, we continue to face increasing challenges from fraud and scams that originate both locally and nationally, and across various payment channels. Coordinated agency action is essential to address these threats effectively.

Examples of Payments Fraud Impacting Our Institution

- **Business Email Compromise (BEC):**

Our customers have been targeted in BEC schemes where incoming wires are redirected based on fraudulent instructions. These funds are often made available immediately to our customers who then send funds to the scammers, and the fraud is only discovered during end-of-month reconciliations by the victim. Outreach to sending institutions and potential victims is complicated by privacy considerations, making timely intervention difficult.

- **Counterfeit Checks:**

Both consumer and commercial customers have been affected by counterfeit checks created using their account information. If these checks are cashed or deposited before detection, the bank may be liable for reimbursement. Account closures and reissuance are often necessary, which is particularly burdensome for elderly customers managing benefit payments and for businesses facing payroll or vendor disruptions.

- **Romance Scams and Money Mule Activity:**

Customers unknowingly involved in romance scams may become money mules, facilitating fraudulent transactions across multiple institutions. These cases consume significant resources from our frontline and compliance teams. Convincing customers of the scam and halting the activity remains a persistent challenge.

Educational Resources and Community Engagement

We appreciate the educational initiatives provided by regulatory agencies and industry groups. Our bank serves elderly customers, small businesses, and consumers in rural and agricultural communities. Tailored educational materials for these demographics are especially valuable.

We actively share digital resources on our website and social media, and we engage in financial education efforts within our community, including outreach to youth, seniors, and small businesses. The *Money Smart for Older Adults Resource Guide* has been a particularly effective tool during presentations at senior centers and community events. We regret that this booklet is no longer available for order and encourage its reinstatement. Printed materials with trusted internet links and interactive tools like fraud bingo have proven to be highly engaging and impactful.

Collaboration and Technology

We support collaborative efforts among stakeholders to address payments fraud. Because fraud often crosses state lines, national coordination is essential. Clear guidance on safe harbors and designated points of contact for interbank communication would greatly enhance our ability to respond swiftly—especially when customers are present in the branch during fraud discovery.

Our bank has invested in transaction monitoring software to detect and mitigate fraud, and we continue to train employees to recognize suspicious activity. We utilize Regulation CC to place exception holds on checks with questionable collectability. We would benefit from automated data collection and reporting tools that integrate with existing systems—provided these enhancements are cost-effective.

Conclusion

Thank you for the opportunity to provide feedback on this important issue. We look forward to continued collaboration with the OCC, FRS, FDIC, and other stakeholders to protect our

customers and community from the evolving threat of payments fraud.

Sincerely,

Nicole Simmons

NICOLE SIMMONS, CAMS, CRCM & CAFP

EVP, Compliance & BSA Officer

