From: Tom Oliver
To: Comments
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)
Date: Wednesday, September 17, 2025 5:26:03 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:

About The Bank of Tampa

I am the Chief Administrative Officer of The Bank of Tampa (Bank), a community bank with assets exceeding $3 billion, located in Tampa, Florida. I am responding to the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), and the Federal Deposit Insurance Corporation (FDIC) regarding their request for information on payments fraud.

Founded in 1984, The Bank of Tampa is one of the largest privately held community banks in the Tampa Bay area. Throughout its history, the Bank has earned a reputation for delivering personalized, relationship-driven financial services to individuals, families, and businesses in the region. Ownership remains local, comprised of staff, directors, and clients, demonstrating our enduring commitment to the community.

The Bank's evolution from a traditional commercial bank to a full-service financial institution has expanded our capabilities to include middle market banking, commercial real estate lending, SBA lending, personal banking, wealth management, and trust services.

The Bank of Tampa serves as a critical lender to small businesses and consumers across the Tampa Bay area. Through our community banking services, wealth management offerings, and a commitment to digital innovation, The Bank of Tampa remains a cornerstone of financial support in the Tampa Bay region.

Regulatory Engagement

I commend the agencies for issuing this request for information and for seeking input on how

the OCC, the Federal Reserve System, and the FDIC can help consumers, businesses, and financial institutions mitigate payments fraud. Community banks, including ours, are increasingly challenged by rising fraud and scams across various payment types, making agency action particularly important.

Payments Fraud Trends and Examples

Over the past year, our institution has observed a significant increase in fraud attempts impacting both clients and internal operations. These incidents have disrupted business continuity and have necessitated considerable resources to investigate, mitigate, and prevent future occurrences. Below are several types of payments fraud that have affected our bank:

- Business Email Compromise (BEC): Fraudsters impersonated executives and vendors to initiate unauthorized wire transfers or ACH transactions. These schemes were sophisticated, often mimicking legitimate transaction patterns and language, leading to financial loss.
- Check Fraud: Multiple incidents involved altered, counterfeit, or forged checks processed through external institutions. While some losses were recovered, the unrecoverable losses are significant, and each instance required immediate response and regulatory reporting, including the individual filing of Suspicious Activity Reports (SARs) for each item greater than $5,000.
- Debit and Credit Card Fraud: This type of fraud has also posed significant challenges for the Bank. Fraudsters have used stolen card information to make unauthorized purchases or withdrawals, often through online transactions or point-of-sale terminals. These incidents require immediate action to secure the affected accounts, reimburse clients, and collaborate with card networks for investigation and resolution.
- Zelle-Related Fraud: Instances of Zelle-related fraud have emerged as a significant concern, mirroring trends seen across the industry. Fraudsters increasingly exploit the speed and convenience of Zelle's real-time payments to deceive clients into authorizing transfers under false pretenses, resulting in losses for affected clients. The rapid nature of Zelle transactions limits our ability to recover funds once sent, in many cases ultimately resulting in loss to the Bank.
- Phishing and Smishing Attacks: Clients received deceptive emails and text messages designed to harvest credentials and initiate fraudulent payments. These attacks have become more frequent and increasingly difficult to detect.
- Caller ID Spoofing: Fraudsters used spoofed phone numbers to impersonate bank staff, persuading clients to share sensitive information or authorize payments under false pretenses.

These examples highlight the urgent need for improved fraud prevention tools, regulatory support, and enhanced public-private collaboration to safeguard financial institutions and their customers.

Recommendations for Regulatory and Supervisory Enhancements

To better support community banks in combating payments fraud, we urge the OCC, Board/FRS, and FDIC to consider regulatory and supervisory enhancements that are appropriately scaled to the size and complexity of community institutions. Examiner expectations should be tiered and allow for realistic implementation timelines.

For example, check fraud remains a significant challenge. Community banks often face delays

and obstacles when resolving breach of warranty claims with larger institutions, sometimes waiting weeks for responses to fraudulent check disputes, with limited recourse or resolution. We recommend the following updates to Regulation CC:

- Extend return deadlines for suspected fraud.
- Clarify the “reasonable cause to doubt collectability” exception.
- Refine definitions such as “altered” and “alteration.”
- Maintain current hold times; do not shorten them, allowing banks flexibility to extend holds when fraud is suspected.

Additionally, centralized fraud data reporting should be encouraged through safe harbors and automation, rather than imposed as a burden. Community banks would benefit from integrated tools such as a fraud contact directory, an interbank check fraud resolution mechanism, and a confirmation of payee service—provided these align with existing platforms and are priced appropriately for smaller institutions.

Conclusion

Thank you for the opportunity to provide comments on this request for information. The Bank of Tampa looks forward to continuing to work with the OCC, FRS, FDIC, and other stakeholders to protect our customers and communities from the growing threat of payments fraud.

Respectfully,

Thomas W. Oliver

Chief Administrative Officer

The Bank of Tampa