MainStreetBank

22980 Shaw Road, Sterling, VA 20166
703-481-4567 | mstreetbank.com

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 Adam Sullivan, the Sr. Fraud Analyst of MainStreet Bank, a $2.1B community bank located in Fairfax, VA. 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.

MainStreet Bank is a business-focused community bank headquartered in Fairfax, with branches in Herndon, McLean, Clarendon, Leesburg and Washington, D.C. Since 2004, MainStreet Bank has provided its clients with individual attention to maximize relationships. Our decision-makers are local and accessible. Most of all, we provide the ultimate customer experience, using a combination of personal relationships and banking technology for convenient, secure and seamless mobile and online banking transactions. MainStreet serves as a consultant, partner, and friend to our clients because we are committed to building long-lasting relationships. We strive to make personal connections with each and every customer and will do whatever it takes to reduce the burden of doing business.

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, the Bank has been affected by payments fraud in the following ways:

- Multiple instances of business or consumer check fraud where the bank took a loss or the recovery process lasted several months.
- Business customers that experienced business email compromise scams via ACH payments that resulted in a loss for either the customer or the bank.

External Collaboration:

- To increase collaboration among stakeholders and prevent fraud, MainStreet Bank believes that it is essential to educate stakeholders about secure payment systems, strong authentication measures and services available such as Positive Pay and online banking. In addition to encouraging regular monitoring of transactions to prevent suspicious activities, or malicious actors.
- To increase collaboration across the financial industry and beyond, MainStreet Bank believes that fraud intelligence sharing hubs, near real-time data exchanges across institutions, shared fraud reimbursement burdens across financial institutions and P2P systems, shared common standards and protocols, and joint technology investments would be effective initial collaborations among various industries to address fraud.
- Businesses should train their employees to recognize suspicious behavior, conduct thorough background checks on personnel, and utilize all organizational resources to optimize business operations and electronic processing environments. Businesses should also prioritize encrypted gateways, multi-factor authentication, or tokenization, avoid using unencrypted email, cross-reference bank details with vendor records and require dual authorization for large payments, limit employee access to sensitive financial data and enforce strong access controls. This will reduce vulnerability to financial fraud and cyber threats.

Regulation and Supervision:

- MainStreet Bank recommends creating a reimbursement duty for authorized push-payment scams with clear timelines and caps and splitting costs between sending and receiving institutions. The UK's Payment Systems Regulator now requires mandatory reimbursement for Faster Payments APP scams with monitoring resolution expectations. MainStreet Bank also recommends Clarifying Reg E so that "fraudulently induced" credit-push P2P transfers are treated as unauthorized when a third party initiates or commandeers the session, standardizing fraud reporting and data sharing and strengthening ACH risk controls.
- MainStreet Bank has found that when customers are faced with unexpected account restrictions, both businesses and consumers occasionally experience cash flow disruptions such as payroll obligation, relationship strains with the bank and business or personal operational burdens.

- Banks are increasingly targeted by fraudsters using advanced technology, which leads to premature access to funds from fraudulent checks. To balance fraud prevention with the need for quicker access to funds, Regulation CC should be amended. Potential changes include: Extended Deadlines: Give banks more time to identify fraudulent transactions by extending return deadlines for large or high-risk checks. Streamlined Fraudulent Check Identification: Improve tools and provide more flexibility for institutions identifying fraudulent instruments. This could involve expanding reserve bank services or encouraging collaboration among institutions to better support financial institutions in fraud detection, promoting fair and consistent application of regulations.
- Fraud is likely to increase if funds availability requirements are shortened, as fraudsters would gain quicker access to funds before checks are confirmed as fraudulent. This would result in higher losses and increased operational costs for depository institutions. Such a change could also be a disadvantage to consumers who rely on timely access to their money, as banks might need to implement more holds or face fines for early releases. A balance is needed between timely access for legitimate customers and robust fraud protection.
- To better balance check return times with fraud investigation, the Federal Reserve should investigate potential changes to Regulation CC. This could include the Board mandating uniform timelines for banks to respond to fraud claims, which would facilitate more prompt investigation and fund recovery. Additionally, the Board could require the bank of first deposit to cooperate in recovering funds from fraudulent checks, including freezing funds upon notice of fraud to allow for investigation.

Payments Fraud Data Collection and Information Sharing:

- The various industries associated with fraud, would benefit from a classification standard of fraud definitions and categories, secure cross-Institution data sharing, safe harbor and liability protection when banks share suspected fraud data in good faith and expand information sharing beyond banks to P2P apps, law enforcement, fintech's, processors and require these groups to contribute to a fraud database. Also, instead of filing with multiple agencies (FTC, FBI/IC3, FinCEN), create a single intake channel to route fraud reports to all relevant authorities.

Reserve Banks' Operator Tools and Services:

- The Reserve Banks should continue to address risk by facilitating the collection and sharing of improved data. This would strengthen fraud prevention efforts and standardize industry-wide education.
- To combat payment fraud, the Federal Reserve Banks should prioritize developing robust risk management tools. A centralized payments fraud contact directory would help

financial institutions report suspicious activity, share information, and coordinate responses with law enforcement and other organizations. Implementing real-time alerts for unusual payment activity (e.g., large transfers, new beneficiaries, unfamiliar locations) would empower users to quickly identify and challenge unauthorized payments and leveraging advanced analytics. Robust confirmation of payee services, which cross-reference recipient names with account holders' names, would prevent payments to unintended recipients, especially for high-value transactions. These recommendations, rooted in regulatory frameworks and public input, are crucial for safeguarding the payment system, protecting consumers and businesses, and fostering a secure financial environment against evolving payment technologies and sophisticated fraudsters.

General Questions:

- MainStreet Bank continues to see a high number of check fraud cases. Most of these instances occur through duplicate presentation of checks, altered checks or checks with forged endorsements and signatures. Another recurring issue for MainStreet is the rise of wire and ACH fraud through business email compromise scams. A common theme around the continued success of various scams, is the lack of customer knowledge and awareness in recognizing the scam.
- MainStreet Bank has employed transaction monitoring utilizing A.I., Mult-factor authentication and behavioral biometric Analytics monitoring systems, positive pay and transaction limits on suspicious accounts to help with fraud detection and to reduce the overall number of fraudulent transactions. There has also been a recent emphasis on customer awareness and better training for the frontline staff.

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,

Adam Sullivan

Adam Sullivan
Sr. Fraud Analyst
MainStreet Bank