New Market BANK

www.newmarket.bank

September 17, 2025

Federal Deposit Insurance Corporation
Jennifer M Jones, Deputy Executive Secretary
Attention: Comments-RIN 3064-ZA49
550 17th Street NW
Washington, DC 20429

RE: Request for Information on Potential Actions to Address Payment Fraud

Dear Madam:

New Market Bank ("NMB") appreciates the opportunity to respond to the Federal Deposit Insurance Corporation's ("FDIC") Request for Information ("RFI") on Potential Actions to Address Payment Fraud. NMB is a community bank with $185MM in assets in the south metro area of the Twin Cities in MN. We celebrated 120-years of serving our communities this year through small business lending, mortgage originations and providing all other financial related services. We also work hard to educate and protect our customers from various fraud schemes which have become increasingly common and hard over the last few years. We applaud the agencies for issuing this RFI to seek input on ways the FDIC, OCC and Federal Reserve can take actions to help consumers, businesses and financial institutions mitigate payments fraud.

Specifically, the bank and our customers have been affected by numerous types of payments fraud including:

- Internet banking takeovers in order to initiate external transfers to the fraudsters' bank accounts elsewhere.
- Wire fraud is usually through romance scams such as our customers believe someone they met online, and are sure they are their significant other, needs money for an investment or to help them afford to come visit the customer.
- Check fraud through check washing usually after checks were stolen from our customer's mailbox.
- Mobile deposits where a customer will deposit a check through mobile deposit they received and then take the cash out and the check is eventually returned as fraudulent.

This is just a summary of some of the frauds we and our customers have experienced. Additional examples are included below in the responses for the various areas of the RFI.

[redacted]

External Collaboration:

We strongly support enhanced external collaboration between regulatory agencies and financial institutions of all sizes, particularly through shared fraud intelligence platforms and real-time alerts. We face challenges in collaborating with other financial institutions on fraud-related matters. The current scope of 314(b) is too narrow and does not encompass all types of fraud that financial institutions encounter. This limitation hinders our ability to work together on suspected fraud cases. There is a need for a more comprehensive method for financial institutions to communicate on fraud-related topics. Ideas related to expanding external collaboration are:

- We recommend expanding the permissible use of Section 314(b) information sharing to include fraud beyond money laundering and terrorist financing. This would be a powerful tool to foster broader collaboration among financial institutions in identifying and preventing a wider range of fraudulent activities.
- We also request regulators to consider policies that allow financial institutions to share relevant fraud-related information with trusted relatives or friends of victims or potential victims, when appropriate, to help prevent further harm and protect vulnerable customers.

Consumer, Business & Industry Education:

As a community bank, customer relationships are our primary focus. Those relationships are often built face-to-face but increasingly are also built through other platforms such as online banking and social media. Both in-branch materials and messaging as well as online resources are needed to meet each customer where their preferences lie. We believe there is a need for accessible, standardized fraud education materials tailored to both consumers and businesses that community banks could use instead of having to create resources themselves. These materials could include printed brochures, electronic messages to use on in-branch TVs or signage, social media posts or videos that could be shared online. Another resource could be a tool kit to use if the bank wanted to host an information session such as a lunch and learn with impactful stories highlighting various fraud scams which would make an impact on the attendee as well as resources the attendees and bank could use to help prevent fraud scams.

Regulation & Supervision:

Overall, payments fraud regulations along with examiner expectations should be tailored to community banks with tiered compliance requirements. Enhanced supervisory guidance for appropriate controls, use of technology, reporting and incident response while not imposing new burdens on community banks would be welcome. Some areas of enhanced guidance could include:

- Regulatory guidance that encourages innovation in fraud detection—while being mindful of the operational constraints of smaller banks—would further empower us to protect our customers and maintain trust in the payments system.
- Appropriate safe harbors would improve banks' ability and willingness to share fraud data without fear of regulatory or legal repercussions.

The following are responses to the Questions presented in the RFI:

- Question 13:
  - *What is the experience of supervised institutions when trying to resolve these types of interbank disputes regarding allegedly fraudulent checks? Do these types of interbank disputes arise more frequently in connection with certain types of checks or parties?* Our experience is poor, especially with trying to address altered checks or checks with forged endorsements drawn on our customers bank account that are deposited into an account at a large bank (bank of first deposit (BOFD)). We often are unable to speak with an actual person or identify the department at the larger bank to file a Breach of Warranty Claim as the BOFD is liable. On the rare occasion when we are able to contact a larger institution, response times can be in excess of 90 days.
  - It is also challenging when we're trying to identify fraudulent checks deposited into our customers bank account that are drawn on an account at a larger bank as we are often unable to speak to someone at the larger bank and if we are fortunate to speak to someone it is common practice that they will not provide feedback whether a check is legitimate.
  - A centralized database of fraud contacts at financial institutions could be beneficial in these scenarios.
  - We also believe that there should be a way to express concerns about not receiving a response in order to hold these financial institutions responsible as it often feels as if they believe by not responding the other bank will eat the loss.
  - *What actions could the Board, FDIC, and OCC consider, including potential amendments by the Board to Regulation CC, that could improve supervised institutions' ability to resolve interbank disputes over liability for allegedly fraudulent checks?* Cashier's check fraud has significantly increased in part because fraudsters are aware Reg CC requires banks to provide next day availability on the first $6,725.00 of the cashier's check deposited. Technology has increased substantially to allow for fraudulent cashier's checks to be created that appear to be authentic and the time to become aware that the check is not authentic is often greater than the next day availability rule allows. Therefore, cashier's checks should be treated consistently with other types of checks and allow for a greater number of days before they are available.
- Question 14:
  - *a. Have technological advancements in check processing reduced the time it takes for depository institutions to learn of nonpayment or fraud such that funds availability requirements for local checks and nonproprietary ATMs should be shortened?* No, it has not, and unfortunately fraudsters have access to new technology that allows them to print very realistic looking checks
  - *b. What effects would shortening funds availability requirements have on payments fraud, consumers who rely on timely access to funds, and depository institutions?* The shortening of hold times will increase payment fraud losses because fraudsters will have access to the money before a consumer or financial institution discovers the fraud. This will result in increased losses to financial institutions and ultimately consumers.
  - *c. Are there any changes the Board should consider to the expeditious return requirement to better balance providing expeditious notice to the receiving depository institution with ensuring adequate time for the paying depository institution to investigate potentially fraudulent checks*?

Fraudsters are aware of regulatory compliance requirements, including aspects of Reg CC. For example, some fraudsters are aware that Reg CC allows us to deem an account new for 30 days and will wait until a new account is seasoned past the 30 days before transacting fraudulent transactions. Updating Reg CC to mitigate actions of fraudsters would be helpful.

- Question 15:
  - *Is this exception effective in allowing depository institutions to mitigate check fraud while also allowing timely access to funds?* No, the time to mitigate check fraud can frequently take more time than allowed to hold funds. Therefore, hold times should not be shortened and in fact banks should have flexibility to hold funds longer than Reg CC currently allows when relevant fraud circumstances exist.
  - *Would depository institutions benefit from further clarification on when it may be appropriate to invoke this exception?* Yes, clarification of the "reasonable cause to doubt collectability" of a check would be helpful including a definition of "altered" and "alteration".
  - *What are the experiences of businesses and consumers when depository institutions invoke this exception in order to delay the availability of depositors' funds?* The experiences are mixed and effective communication by our team members is the best tool to help customers understand that the increased fraud environment is the root cause for most holds currently being placed and our intention is to help mitigate loss to both the customer and our bank.

<u>Payments Fraud Data Collection and Information Sharing:</u>

Community banks would especially benefit from automated data collection, analysis, and reporting tools that integrate with existing systems and services and are made available without additional cost burdens. Smaller community banks especially have budget constraints that often don't provide the ability to invest in expensive technology to assist in detecting various types of fraud. The development of a centralized framework for payments fraud data collection and information sharing would enable institutions to better understand emerging threats, benchmark their own fraud experiences, and contribute to a more resilient financial ecosystem. Since most payments flow through the Federal Reserve Bank, such as checks, ACH transactions and wires, it would be ideal for the Fed to create a database of known fraud accounts that could be used to filter checks, ACHs, and wires which could assist with detecting fraudulent transactions.

<u>General Information:</u>

As mentioned above, the bank has experienced a high level of fraud in the last five years. This increased fraud is spread across types including check fraud, wire fraud, debit card fraud, phishing scams of customers, internet banking account takeovers, external transfers, mobile deposits, etc. Below are a couple specific examples of some of the most recent fraud attempts/scams that we have experienced and the controls we have had to put in place to try and prevent more of this activity.

- Recently, we have encountered a significant amount of fraud involving mobile deposits. New customers have opened accounts, maintained minimal transactions for a few weeks, and then deposited fraudulent checks via mobile deposit, withdrawing the funds in cash before the checks are

returned. Long-time customers have also been scammed into depositing fraudulent checks and withdrawing the cash to send to fraudsters, sometimes using services like Cash App. We have implemented restrictions on mobile deposits and now manually review the majority of them, which requires substantial manual effort to mitigate fraud and increased labor costs.

- We recently had an elderly customer trying to deposit a check that was larger than her normal banking activity and wanted to immediately receive a large amount of cash back. Thankfully our team members identified this as unusual activity as the check had fraudulent characteristics and therefore politely but firmly asked our customer questions. Our customer acknowledged the funds were from an individual that she's only known through social media for nearly 5 years, had previously sent large amounts of money to them, filed police reports over 2 years ago regarding fraud and the individual was now re-contacting her to "repay" her, which she once again fell prey to their tactics. These chain of events show the amount of time and veracity fraudsters pray on victims.
- Internet banking, customers can perform external transfers from their accounts at New Market Bank to their accounts at other financial institutions. Fraudsters have exploited this feature, leading us to lower the transaction limits and manually review these transactions. Despite these measures, fraud persisted, and we ultimately disabled external transfers for most customers and restricted new customers from using this feature. While this decision was necessary to mitigate fraud, it was disappointing to remove a valuable service from our customers.

Thank you again for the opportunity to provide comments on this RFI. The topic of combatting fraud and working to prevent it is extremely important to our bank and the community banking industry. We look forward to working with the FDIC, OCC and FRS as well as other stakeholders to protect our customers and communities from this growing threat of payment fraud.

Sincerely,

/s/

Anita Drentlaw
CEO, CFO, & President

/s/

Jeff Jacobson
Vice President, Compliance Officer