First Bank OF ALABAMA
www.fbal.bank

September 17, 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

Re: Request for Information—Potential Actions to Address Payments Fraud

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

On behalf of First Bank of Alabama, a $1.1 billion-dollar community bank proudly serving East Central Alabama since 1848, thank you for the opportunity to comment on the interagency Request for Information regarding payments fraud. As a community bank, we face persistent challenges—particularly related to check fraud and increasingly sophisticated scams—that are exacerbated when accounts at larger institutions are opened or maintained without adequate customer due diligence. We support targeted reforms that reduce fraud across the ecosystem, preserve safe and timely access to funds, and recognize the resource constraints of community banks.

Question 1: *What actions could increase collaboration among stakeholders to address payments fraud?*

Response:

- Establish a national fraud coordination network spanning community banks, large banks, law enforcement, regulators, and payment operators. The network should support real-time alerts, shared fraud typologies, and standardized interbank resolution protocols.
- Require same-day reporting of altered and counterfeit return items and have clearing houses forward those notifications to a centralized repository that integrates with banks' item processing systems. Items flagged from this repository should qualify for a "reasonable cause to doubt collectability" hold under Regulation CC.
- Ensure national initiatives account for community banks' limited staff and budgets by offering streamlined participation options, templates, and low-cost integrations.

Question 2: *What types of collaboration, including standard setting, could be most effective in addressing payments fraud? What are some of the biggest obstacles to these types of collaboration?*

Response:

- Adopt standardized fraud classification and reporting across rails and institutions (uniform scam/fraud typologies) and promote consistent breach-of-warranty and dispute-handling standards.
- Primary obstacles include data-sharing liability concerns, uneven incentives for larger institutions to participate, and integration costs for smaller banks.

Question 3: *Which organizations outside of the payments or banking industry might provide additional insights related to payments fraud and be effective collaborators in detecting, preventing, and mitigating payments fraud?*

Response: Postal services (mail theft), telecommunications providers (caller ID spoofing and SMS scams), cybersecurity firms (threat intelligence), and law enforcement (local education and victim support) add critical insight and outreach capacity.

Question 4: *Could increased collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?*

Response: Yes. Unify agency efforts through a joint fraud registry accessible to financial institutions and law enforcement, with coordinated enforcement and standardized reporting to reduce duplication and response delays.

Question 5: *In general, what types of payments fraud education are most effective, and why? Would different audiences (for example, industry and consumers) benefit from different types of payments fraud education?*

Response:

- Community banks' face-to-face engagement is especially effective; in-branch materials and teller-line conversations resonate with our customers.
- Scenario-based training and real-time alerts help consumers recognize scams.
- Business customers benefit from practical training on account monitoring responsibilities and the use of Positive Pay with payee match, dual authorization, and out-of-band verification.

Question 6: *Would additional education informing consumers and businesses about safe payment practices be helpful to reduce payments fraud and promote access to safe, secure payment options?*

Response: Yes. Expand education on secure payment practices and common red flags, while emphasizing regular account review to limit losses if fraud does occur. Prioritize rural and underserved communities.

Question 7: *Which approaches could make existing payments fraud education more effective? For example, would targeting outreach to particular audiences or conducting additional education in collaboration with other key stakeholders be effective?*

Response:

- Partner with local banks, schools, senior centers, small-business groups, and community organizations for coordinated campaigns and events.
- Work with core processors and digital banking providers to embed timely fraud tips and warnings within online and mobile channels.

Question 8: *Are current online resources effective in providing education on payments fraud? If not, how could they be improved?*

Response: Current resources can be fragmented. A centralized portal with interactive content, printable handouts, and multilingual materials would help. Recognize that some customers lack reliable internet access; provide offline materials and in-person sessions.

Question 9: *What potential changes to regulations (apart from the Board's Regulation CC, discussed separately below) could address payments fraud and mitigate the harms from payments fraud to consumers, businesses, and supervised institutions?*

Response:

- Establish minimum, enforceable KYC/CIP standards across institutions. Where the bank of first deposit cannot evidence adequate KYC/CIP, assign appropriate liability for fraudulent checks.
- Require risk-based mobile deposit limits that consider relationship length, enhanced due diligence at onboarding, anomaly indicators, and evolving fraud trends.

Question 10: *The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payments fraud detection, prevention, and mitigation. Is existing supervisory guidance related to payments fraud sufficient and clear? If not, what new or revised supervisory guidance should the Board, FDIC, and OCC consider issuing on this topic within the respective authorities?*

Response: Issue targeted check-fraud guidance covering controls, suitable technologies, documentation standards, breach-of-warranty processes, and timely interbank response expectations.

Question 11: *How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payments fraud?*

Response: Provide model policies, reference control frameworks, and safe harbors for community banks that act in good faith and follow prescribed processes.

Question 12: *What is the experience of consumers and businesses when supervised institutions place holds on depositors' funds because of suspected payments fraud? (Regulation CC's "reasonable cause to doubt collectability" exception is discussed separately below.) (a) For instance, how frequently are consumers and businesses affected by holds, delays, or account freezes, and how responsive are supervised institutions to inquiries from consumers and businesses regarding these issues? (b) Do current disclosure requirements effectively address consumer and business concerns when supervised institutions hold customer funds due to suspected payments fraud? For example, should changes be considered with respect to permissible customer communications under SAR confidentiality rules?*

Response: Funds-availability holds are necessary but often misunderstood. Permit clearer customer explanations about suspected fraud within existing confidentiality requirements (preserving SAR confidentiality), using standardized disclosures and FAQs.

Question 13: *The Board, FDIC, and OCC have received complaints from supervised institutions regarding challenges in resolving disputes about liability for allegedly fraudulent checks. 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? 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?*

Response:

- Disputes are frequent and time-consuming; responses from larger institutions are often delayed, if not ignored.
- Establish time-bound response requirements, shared evidence standards, and structured escalation paths, with liability considerations when KYC deficiencies are present.

Question 14: *Regulation CC seeks to balance prompt funds availability with the risk of checks being returned unpaid for reasons that include fraud. What potential amendments to Regulation CC would support timely access to funds from check deposits while providing depository institutions with sufficient time to identify suspected payments fraud? (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? (b) What effects would shortening funds availability requirements have on payments fraud, consumers who rely on timely access to funds, and depository institutions? (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?*

Response:

- Technological advancements have improved detection speeds, but shortening hold times without other reforms would likely increase fraud exposure. Consider extending the return period for suspected fraud (with documentation and audit trails) and clarifying definitions for altered and counterfeit items.
- Do not shorten hold times; they remain essential for detecting and preventing check fraud.

Question 15: *Regulation CC provides six exceptions that allow depository institutions to extend deposit hold periods for certain types of deposits, including deposits for which the depository institution has reasonable cause to doubt the collectability of a check. Is this exception effective in allowing depository institutions to mitigate check fraud while also allowing timely access to funds? Would depository institutions benefit from further clarification on when it may be appropriate to invoke this exception? What are the experiences of businesses and consumers when depository institutions invoke this exception in order to delay the availability of depositors' funds?*

Response: The exception is useful but vague. Clarify criteria for invoking it and explicitly recognize data-driven flags (e.g., from a centralized fraud repository) as a valid basis. Require originator bank cooperation in fraud investigations.

Question 16: *Broadly, how could payments fraud data collection and information sharing be improved?*

Response: Create a centralized, privacy-protected fraud incident repository accessible to financial institutions and operators, with standardized data elements and common classification across payment types.

Question 17: *What barriers limit the collection and sharing of payments fraud data between industry stakeholders, and how could these barriers be alleviated? For example, have specific barriers limited development of solutions or participation in bilateral or multilateral payments fraud data collection and information sharing? What changes would address these barriers?*

Response: Privacy laws, liability concerns, and competitive dynamics hinder sharing. Provide safe-harbor protections for timely, good-faith reporting, promote anonymization where feasible, and set mandatory reporting thresholds for certain events.

Question 18: *What role should the Federal Reserve System, FDIC, or OCC take in supporting further standardization of payments fraud data? For instance, can the System better leverage or improve the FraudClassifier and ScamClassifier models?*

Response: Mandate consistent use of standardized classification models across institutions and payment types, publish implementation guides, and provide conformance testing and feedback loops.

Question 19: *What types of payments fraud data, if available, would have the largest impact on addressing payments fraud? If these data are not currently being collected or shared, what entities are best positioned to collect and share such data?*

Response: Most impactful fields include originating and depositary institutions, fraud typology, method of compromise, dollar amount, and resolution outcome. Payment processors and larger institutions are well positioned to collect and share this data.

Question 20: *Is there a need for centralized databases or repositories for the sharing of payments fraud data across entities? What legal, privacy, or practical risks and challenges could such a centralized database or repository pose? Which entities are best positioned to develop and participate in a centralized database or repository?*

Response: Yes. To mitigate risks, implement strong governance, access controls, audit trails, and independent oversight. Community banks would benefit from automated reporting tools integrated with existing services at no additional cost.

Question 21: *How can the Reserve Banks enhance their existing risk management tools and services, operations, rules, or procedures to better meet the needs of participating financial institutions in addressing payments fraud? For example, should the Reserve Banks consider requiring fraud reporting for payment rails (as they already do for the FedNow Service) or adopting any particular payment fraud standards?*

Response:

- Expand real-time anomaly alerts across rails; establish a fraud contact directory for rapid interbank escalation; and create a structured dispute-resolution mechanism for check-fraud breach-of-warranty claims.
- Prioritize low-friction integrations with third-party and core platforms used by community banks and adopt pricing scaled to size and complexity.

Question 22: *Are there risk management tools or services that the Reserve Banks should consider offering or expanding, such as (a) developing a payment fraud contact directory for financial institutions, (b) offering tools that can provide notification of atypical payment activity, or (c) introducing confirmation of payee services to help mitigate fraudulent payment origination?*

Response: Yes. In addition to the tools listed, community banks would benefit from: (1) a fraud information-sharing repository with analytics and trend dashboards; (2) check image analysis and verification leveraging image forensics; (3) cross-channel behavioral analytics for atypical payments; and (4) confirmation of payee services for ACH and wires.

Question 23: *What types of payments fraud have most impacted your organization and its stakeholders? What tactics have criminals employed when perpetrating these types of payments fraud*

Response: Check fraud—counterfeit and altered checks—has been most impactful, often linked to mail theft and social-engineering schemes, with items deposited at institutions where mule or identity-theft accounts have been opened.

Question 24: *What measures, including technological solutions or services, have been most effective in identifying, preventing, and mitigating payments fraud at your institution? Are there actions that consumers can take that help institutions? For example, do financial institutions find it helpful when consumers alert the institution in advance when making large purchases, transferring large amounts of money, and traveling abroad?*

Response: Positive Pay with payee match, dual authorization, transaction alerts, and advance notice on large or atypical transactions have been particularly effective.

Question 25: *To the extent not already addressed, are there other actions that would support stakeholders in identifying, preventing, and mitigating payments fraud?*

Response: Require or facilitate payee identity validation prior to check issuance and promote secure digital alternatives where appropriate. Encourage collaborative education campaigns and expand safe-harbor protections for data sharing.

Question 26: *Are there specific actions that commenters believe could encourage the use of payment methods with strong security features?*

Response: Offer pricing incentives or fee reductions for utilizing rails and tools with strong security features (including instant payments) combined with targeted education for consumers and small businesses.

Conclusion

Payment fraud continues to pose a significant threat to our community financial institution. In many of these cases, these check fraud losses are directly linked to the bank of first deposit failing to meet their obligations under current UCC regulations. We urge federal agencies to hold these institutions accountable for their inaction. Check fraud is a major issue for community banks, and we urge regulatory agencies to establish a system that allows us to report these incidents and compel larger banks to fulfill their obligations.

First Bank of Alabama appreciates the Agencies' leadership in confronting payments fraud. The recommendations above aim to improve prevention, accelerate detection, clarify liability, and streamline resolution—while ensuring that community banks can participate effectively without disproportionate burden. I welcome the opportunity to discuss these ideas further or provide additional details.

Respectfully,

J. Chad Jones
President & CEO
First Bank of Alabama