FNBB
First National Bankers Bank
[redacted] · www.BANKERS-BANK.com
OFFICE TOLL-FREE FAX
[redacted]

September 2, 2025

Jonathan V. Gould
Comptroller of the Currency
Office of the Comptroller of the Currency
400 7th Street, SW, Suite 3E-218
Washington, DC 20219

Ann Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Jennifer M. Jones
Deputy Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Re: Request for Information on Potential Actions to Address Payments Fraud
(OCC Docket ID OCC–2025–0009; Federal Reserve Docket No. OP–1866; FDIC RIN 3064–ZA49)

Dear Comptroller Gould, Secretary Misback, and Deputy Executive Secretary Jones,

On behalf of First National Bankers Bank (FNBB), we appreciate the opportunity to comment on the joint Request for Information on Potential Actions to address Payments Fraud. We applaud the agencies' initiative to address rising fraud concerns and seek input to mitigate the associated risks.

FNBB is a bankers' bank headquartered in Baton Rouge, Louisiana, with regional offices across Louisiana, Mississippi, Alabama, Arkansas, and Florida. We serve over 600 community bank customers throughout the Southeastern United States and are owned exclusively by those community financial institutions.

Community banks operate with smaller teams, leaner resources, and closer customer relationships than large institutions. They are often on the front lines of fraud prevention, yet face significant disadvantages when it comes to real-time data access, affordable technology, and cross-institution collaboration. The following comments reflect the operational realities of community banking and provide recommendations for addressing payments fraud effectively.

I. **External Collaboration**
Community banks urgently need industry-wide, real-time collaboration tools. FNBB recommends:

- Establishing a shared, real-time database of known scams, bad actors, and fraudulent accounts, accessible to all banks regardless of asset size. Bad actors deliberately target institutions they perceive as having weaker defenses; community banks are disproportionately at risk without equal access to intelligence.
- Creating a check verification system that enables all banks, regardless of size or core provider, to validate items before posting.
- Allowing information sharing of relevant SAR data in a manner consistent with legal and confidentiality requirements so banks can proactively identify and avoid opening accounts for known fraud participants.
- Providing easier access to vetted fraud detection vendors via a shared due diligence model supported by recognized standard-setting and certifying organizations to establish baseline security and performance criteria.
- Supporting development of a consolidated fraud detection platform with cross-system communication to connect ACH, check, wire, and instant payment fraud detection.

II. **Consumer, Business, and Industry Education**

From a community bank perspective, fraud education is most effective when it is personal, repeated, and relatable. We recommend:

- Direct customer engagement: branch conversations, targeted mailings, church and civic group presentations, and nursing home visits.
- Leveraging popular media platforms like YouTube and TikTok to deliver short, memorable fraud prevention messages, especially for younger audiences.
- Coordinating federal, state, and industry messaging so that consumers receive consistent, up-to-date guidance across channels.
- Ensuring fraud education resources reach non-digital populations, particularly seniors, through physical mail and in-person outreach.

III. **Regulation and Supervision**

The predominant check regulations have not been updated to reflect the current check processing environment. The last significant updates to Regulation CC were the addition of the Check 21 Act in 2003 and the presumption of alteration in 2018. UCC Articles 3 and 4 have not been updated since 1990, when transfer and presentment warranties were added. Both frameworks need significant changes to address today's fraud issues and processing methods, including mobile deposits and remote deposit capture. Community banks and bankers' banks would benefit from these regulatory and supervision changes:

- Uniform fraud claims standards across all institutions, with required timelines for acknowledgement, investigation, and resolution.
- Regulatory flexibility in placing holds on high-risk deposits, including government and cashier's checks, when fraud is suspected.
- Support for adoption of payee positive pay and other front-end verification tools for business customers.
- Greater oversight and accountability for institutions that originate a disproportionate share of fraudulent transactions, as fraud tends to cluster where criminals believe they can avoid detection.

- Holding depository banks responsible for their lack of due diligence in the mobile deposit of fraudulent checks. Mobile deposit has become a primary avenue for check fraud, and the depository institution, not the bank of first return, should bear clear accountability for performing appropriate verification before accepting these items.
- Regulatory review and violation process: Regulatory agencies should have a formal review process for claims that are not processed in accordance with existing rules and regulations, as well as a violation process for cases where the law is clearly ignored or disregarded. This accountability is necessary to ensure that institutions cannot avoid or delay claim resolution in hopes the claimant will abandon the process.

IV. **Payments Fraud Data Collection and Information Sharing**

The current approach to fraud data collection is fragmented. Community banks recommend:

- Standardized, centralized fraud databases with real-time updates, accessible to all financial institutions regardless of size.
- Cross-verification capabilities that flag duplicate presentments, altered items, and suspicious payee changes.
- Built-in payee validation for all government-issued checks, with Treasury-provided issued check lists integrated into Federal Reserve processing systems.
- Secure channels for SAR-derived intelligence sharing to prevent criminals from exploiting account openings at new institutions.
- Data systems that support cross-payment-rail communication, so that trends identified in one channel can inform controls in another.

V. **Reserve Banks' Operator Tools and Services**

We recommend the Federal Reserve Banks:

- Offer real-time fraud contact directories for participating institutions.
- Provide configurable payment velocity alerts and optional Confirmation of Payee APIs that are interoperable with existing core systems.
- Expand fraud dashboards and anomaly reporting capabilities for community banks, ensuring these tools are affordable and not cost-prohibitive.

VI. **General Observations**

For community banks, check fraud, particularly counterfeit checks created from stolen mail, remains one of the most frequent and damaging fraud types. Our experience shows that criminals often target institutions where they believe oversight is lighter and detection is slower. Equalizing fraud prevention capabilities across all asset sizes is essential to closing these gaps. Preventing losses for smaller banks is not just a matter of fairness; it is vital to maintaining access to safe, affordable banking in rural and underserved communities. We urge the agencies to consider mandatory adoption of stronger payment security methods to ensure consistent protection across the financial system.

FNBB
First National Bankers Bank
[redacted] · www.BANKERS-BANK.com
OFFICE TOLL-FREE FAX
[redacted]

Thank you for considering our perspective. FNBB and our community banks stand ready to work with the OCC, Federal Reserve, and FDIC to implement practical, scalable fraud prevention solutions. Equal access to data, tools, and vendor resources, combined with uniform claim-handling standards, stronger mobile deposit due diligence requirements, coordinated consumer education, and a robust regulatory review and violation process will substantially reduce fraud losses and strengthen the payments ecosystem.

Sincerely,

[redacted]

Jessica Johnson
SVP, Director of Bank Operations
First National Bankers Bank