1st National Bank of Scotia
Main Office: [redacted] • [redacted] • www.firstscotia.com

September 12, 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

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

We respectfully submit the thoughts below in response to the request for comments regarding payments fraud. As a financial institution, we are on the front lines of this issue and appreciate the opportunity to provide our perspective. We believe that a multi-faceted approach, encompassing collaboration, education, regulation, and improved tools, is essential to effectively combat payments fraud.

Community banks face unique challenges and opportunities in this evolving landscape. While we possess deep, relationship-based knowledge of our customers and local markets, we often lack the scale and resources of larger institutions to develop and deploy proprietary and innovative fraud technology. Therefore, collaborative strategies are not merely a benefit to community banks, they are a necessity.

Collaboration – Combating fraud requires a collaborative, multi-layered defense. Information sharing initiatives currently exist in some communities among local/regional resources, but the scale and informal nature of these initiatives can limit the ability to effectively and broadly disseminate information. Banks also invest heavily in proprietary fraud detection systems; however, their utility is primarily reactive to existing trends and their effectiveness limited without broader information sharing around emerging threats. We support the creation of a centralized, secure platform or a formalized framework for real-time information sharing among all stakeholders. This would allow for the rapid dissemination of fraud trends, compromised account information, and threat intelligence.

For community banks, such a framework offers significant, tailored benefits:

- Access to broader intelligence – A shared consortium model would allow community level institutions to access anonymized and aggregated data on fraud patterns, mule accounts, bad actors, and high-risk entities, which have been identified by other financial institutions. This is especially critical for identifying emerging fraud threats or rings that operate across different banks and jurisdictions.

- Risk Mitigation – When one bank identifies a new fraud scheme, a collaborative network ensures that all participating banks benefit immediately, preventing others from becoming the next victim. This allows community banks to proactively defend against threats rather than react after a loss has occurred.

We believe the Federal Reserve, acting as a central coordinator, could facilitate this. The Fed's role in providing a secure, neutral ground for this collaboration is paramount for building trust and ensuring a consistent approach across the industry.

Education – Fraud prevention is not solely a bank's responsibility. It requires vigilance from all parties. While some fraud awareness resources and publications exist, they are segmented among various agencies and parties. We believe designing a national, coordinated public awareness campaign on payments fraud is the best approach to ensure successful and extensive dissemination of the information. The Federal Reserve, in partnership with other agencies, banks, and industry groups, is well resource-positioned to lead this effort. This campaign should focus on cohesive messaging for:

- Consumers – Simple, actionable advice on recognizing phishing attempts, avoiding imposter/impersonation scams and elder financial exploitation, and understanding the risks and schemes associated with growing and emerging payment technologies (P2P, instant payments, digital/crypto assets). Community banks can serve as trusted local partners in this effort, using our strong customer relationships to deliver cohesive educational content directly and personally.

- Businesses – Guidance on implementing and utilizing available controls which are designed to combat payments fraud (check/payee/ACH positive pay), employee training on payments monitoring and security best practices, and understanding risks associated with business-specific operations such as business email compromise (BEC) and invoice fraud.

- Industry – A unified approach to fraud training for bank employees, consistent messaging to customers, and sharing of best practices for fraud detection and response.

Regulation and Supervision – We support a balanced approach to regulation that fosters innovation while mitigating risk. Clear, consistent regulatory guidance on fraud prevention and loss allocation is vital. The current environment, with its varying interpretations and liabilities, creates

uncertainty. We recommend the Federal Reserve, and other regulatory bodies, consider the following:

- Harmonized regulations – Develop a unified set of regulations and guidance that apply consistently across different payment types (e.g., checks, ACH, wire, instant payments) to close loopholes and mitigate the ability of fraudsters to exploit gaps and inconsistencies in laws and regulations or different geographical jurisdictions.

- Clear Liability Framework – Establish clear, well-defined rules for liability. The varying regulations governing different payment types and the absence of a uniform set of consumer disclosures, error resolution procedures, and liability allocation structures (e.g., "unauthorized" transactions versus "fraudulently induced" transactions) for retail payments complicates liability determination. The current environment often places the burden on the consumer or bank, even when both parties have taken reasonable precautions. A more equitable framework would encourage all parties to invest in fraud prevention.

- Risk-Based Supervision – Understand that the availability and type of fraud resources can differ among institutions of varying sizes. Continue to tailor and support supervisory examinations to the specific risks faced by different institutions, recognizing that the fraud landscape is constantly evolving.

Data Collection and Information Sharing – Effective fraud prevention depends on data. The Federal Reserve Payments Study is a valuable tool but limited general awareness of its existence and the frequency of issuance minimizes its effectiveness. We support more granular and frequent data collection. A standardized reporting framework would allow for better analysis of fraud trends by type, payment channel, and geographic location. This data, anonymized and aggregated, could be shared with institutions to help them benchmark their own fraud performance and identify emerging threats. The Fed could also encourage the use of shared databases of confirmed fraudulent accounts and compromised credentials, similar to existing systems for other types of financial crime.

Fed Operator Tools and Services – As an operator of critical payment infrastructure, the Federal Reserve plays a unique role. We recommend consideration of the following enhancements to your operator tools and services:

- Enhanced Fraud Detection and Screening – Expand the fraud screening capabilities of the Fed-owned proprietary Fedwire and the FedNow services by establishing real-time anomaly detection within those tools.

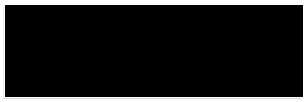
- API-Based Access – Continue to expand API access capabilities for banks to Fed-operated services to enable more seamless integration with proprietary fraud monitoring systems, allowing for faster response and mitigation. API-driven integration can enhance data exchange, reduce manual processes and improve efficiency in fraud monitoring and investigation, allowing financial institutions to respond more quickly to emerging threats. This is of particular relevance to

community banks that rely on third-party core processors and need to integrate new services efficiently.

- Education and Training Resources – Offer training and resources to help financial institutions understand what fraud mitigation tools and services the Fed offers and how to effectively utilize them.

We respectfully support a unified collaborative approach to build a safer and more resilient payments ecosystem for all. We appreciate your consideration of these comments.

Sincerely,



Kelly A. Gibbons
Sr. Vice President of Retail Banking
& Security Officer