LexisNexis®
RISK SOLUTIONS

Ken Meiser
LexisNexis Risk Solutions

[redacted]

September 18, 2025

Via Electronic Submission

Office of the Comptroller of the Currency (OCC)
Chief Counsel's Office
400 7th Street, SW, Suite 3E-218
Washington, D.C. 20219
Attn: Comment Processing

Board of Governors of the Federal Reserve System (FRS)
20th Street and Constitution Avenue NW
Washington, D.C. 20551
Attention: Ann E. Misback, Secretary

Jennifer M. Jones, Deputy Executive Secretary
Federal Deposit Insurance Corporation (FDIC)
550 17th Street NW
Washington, D.C. 20429
Attention: Comments RIN 3064-ZA49

Re: Response to Request for Information on Payments Fraud (RFI)
Docket IDs: OCC-2025-0009, FRS OP-1866, and FDIC RIN3064-ZA49

LexisNexis Risk Solutions Inc. ("LNRS") appreciates the opportunity to comment on the Request for Information ("RFI") on Payments Fraud. LNRS submits this comment letter in support of the OCC, FRS, and FDIC proactive stance on anti-fraud activities and to share insight on the use of consumer data to support consumer identity verification, fraud detection and investigation that protect consumers and the financial system as a whole.

LNRS provides information solutions to help predict and manage risk; and to protect consumers and institutions from cyber risks, such as identity theft. LNRS solutions help our customers underwrite and manage risks, detect and prevent fraud, positively identify individuals, and verify that individuals are who they say they are. Consumers benefit from the use of data solutions as

[redacted]

those tools make it harder for fraudsters to steal identities to get credit, services or benefits they are not entitled to obtain.

LNRS's corporate customers comprise over 75% of Fortune 500 companies, including major retail businesses and all of the top 50 U.S. banks. LNRS also serves tens of thousands of small- and medium-size businesses, insurance companies, online retailers, manufacturers, healthcare providers, non-profits, and federal, state, and local government law enforcement and other agencies. The LexisNexis® Digital Identity Network analyzes more than 345 million transactions daily, and over 121 billion transactions annually. Additionally our network-driven solutions detected around 690m human initiated fraud attacks and more than 2bn automated bot attacks for customers in 2024

As an example of payment-specific fraud tools operating in other jurisdictions, LexisNexis Risk Solutions operates ThreatMetrix® Payment Defense in the UK which provides risk assessment of both outbound and inbound payments. This solution utilizes cross party event data and machine learning to address Authorized Push Payment scams.

Our comments fall into four areas:

I. The Evolving Threat Landscape in New Payment Systems

- While traditional payments fraud persists, new and alternative payment systems have introduced novel vulnerabilities.
    - Crypto, non-bank payments, faster payments, p2p apps, etc. have added additional variables and increased fraud attack surface for businesses and consumers alike. The speed and irreversibility of payments create a unique risk, compounded by an increased attack surface.
    - Traditional sources of payment processing, including checks are able to access authoritative verification of sending and receiving entity data and account association. The ability of newer payment methodologies to leverage similar data is constrained.
- The decentralized and often cross-platform nature of these systems makes it difficult for a single entity to detect and prevent sophisticated fraud rings. Pseudonymity and anonymity are frequently core tenets of many emerging payment systems. Fraudsters often use chain-hopping techniques to obscure the trail of stolen funds, and the lack of established regulatory authority and jurisdictional challenges create further complexity.
    - According to FTC's Sentinel Report, imposter and investment scams accounted for $8.8b in fraud losses in 2024.
    - The 2025 LexisNexis Risk Solutions True Cost of Fraud study indicates that Financial Institutions report an average additional cost of $5.75 for every $1 lost to fraud. Additionally, the impact to customer experience of fraud prevention techniques results in additional losses due to friction.
- Existing data-sharing safe harbors, which allow controlled exchange of information on the parties to a transaction for the purposes of fraud prevention, were largely designed for

[redacted]

traditional banking relationships and do not adequately address the unique needs of these new systems and new participants in the transaction stream.

II. The Critical Role of Enhanced Data Sharing to Prevent and Detect Fraud.

- Real-time, cross-platform data sharing is essential for moving from a reactive to a proactive fraud prevention model that leverages network intelligence.
    - Based on LNRS research, the following types of data would be most useful for inclusion in a network fraud solution:
        - transaction patterns
        - sending and beneficiary account details including social alias for P2P powered payment apps
        - behavioral indicators
        - known fraudulent indicators.
        - for crypto, consider the impact of on-chain and off-chain data while respecting the inherent non-identifying nature of crypto wallets
- Safe harbors would enable non-traditional payment system operators to securely share aggregated fraud signals with its partner banks and other e-commerce platforms, creating a network effect that benefits all participants and customers.

III. The Need for Regulatory Clarity and Safe Harbors

- Companies are hesitant to share data for the following reasons:
    - Legal and compliance uncertainty related to fear of violating privacy provisions of the GLBA, FCRA, or EFTA.
    - Antitrust concerns regarding information sharing between competitors.
    - Unclear liability for data breaches or misuse of shared information.
- Without explicit regulatory safe harbors, industry participants will remain cautious, allowing fraudulent activity to flourish in the seams between systems.

IV. Specific Recommendations for the OCC, FRS and FDIC

- Issue Guidance: The OCC, FRS and FDIC should solicit best practices and publish guidance that defines the specific conditions under which data sharing for payments fraud prevention is permissible, and which types of data are considered safe to share. Additionally, continue to leverage and improve the Federal Reserve fraud/scam classifier models to ensure uniformity and ease of implementation
- Establish a formal Safe Harbor provision: Create a new, payments-specific safe harbor provision that explicitly protects firms collaborating on fraud prevention
- Examine current private sector best practices and convene a public-private sector working group: OCC, FRS and FDIC should lead an industry-wide task force to examine current consortia and discuss best practices for data exchange, ensuring all stakeholders (banks, fintechs, payment providers, risk mitigation providers) have a voice.

[redacted]

Conclusion

We look forward to partnering with you to create an updated framework that protects consumers and encourages innovation. For additional information, you can reach me at [redacted]

Sincerely

Ken Meiser
Vice President, Public Policy
LexisNexis Risk Solutions