

[REDACTED]

From: Ravindran Loganathan <[REDACTED]>
Sent: Wednesday, August 27, 2025 5:54 PM
To: Comments
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information on Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)

[REDACTED]

August 26, 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 on Potential Actions to Address Payments Fraud

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

On behalf of SardineAI Corp. and its subsidiary SonarAI LLC, which provide financial crime prevention infrastructure to banks, credit unions, and financial technology firms across the United States, I appreciate the opportunity to respond to the joint Request for Information on Potential Actions to Address Payments Fraud.

We commend the agencies for addressing the increasing threat of fraud across checks, ACH, wire transfers, and instant payments. Fraud in these channels is no longer a series of isolated events at the customer level; it has become a systemic risk that undermines confidence in the U.S. payment system.

I. Key Challenges

Fragmented Controls Across Payment Systems

-
-
- Each rail—ACH, wire, check, and RTP/FedNow—operates independently with distinct settlement
- rules and dispute processes. There is no industry-wide mechanism to assess counterparty risk prior to settlement.
-
-
-
-
-
- Fraudsters exploit these gaps by rapidly moving funds across rails (e.g., ACH credit
- followed by RTP withdrawal), outpacing dispute and recovery windows.
-
-
-

Funds Availability Misaligned with Fraud Risk

-
-
- Current Regulation CC funds availability requirements were designed for paper-based processes
- and are increasingly exploited in today's environment of remote deposit capture and near-instant withdrawals.
-
-
-
- This enables schemes in which fraudulent deposits are immediately made available and
- withdrawn through mule accounts.
-

Fraud–AML Disconnect

-

-
- Fraud, onboarding risk, and anti-money laundering obligations are supervised separately.
- Criminals exploit this separation by using fraudulent deposits and mule accounts both to defraud institutions and to launder proceeds.

-

-

-

Fragmented Intelligence and Delayed Attribution

-
-
- Fraud intelligence remains distributed across vendors, processors, and consortia. The
- absence of a unified, real-time system for flagging counterparties prevents early intervention and increases losses, particularly for smaller institutions.

-

-

-

Persistence of Check Fraud

-
-
- Altered and counterfeit checks remain a significant source of losses. Current Regulation
- CC deadlines are not aligned with the velocity of fraud when items are deposited via remote capture and withdrawn within hours.

-

-

-

II. Recommended Actions

1. Cross-System Counterparty Screening Utility

-
-
- Establish an industry-wide utility to provide real-time counterparty screening across
 - ACH, RTP, FedWire, and check clearing.
 -
 -
 -
 - Essential features should include device and behavioral biometrics, network graph analysis
 - linking counterparties across systems, and a fraud attribution ledger.
-
-
-
-
- Participation should be supported by privacy and compliance frameworks, including Gramm-Leach-Bliley
- Act safeguards and federated learning models.
-
-
-

2. Regulation CC Modernization and Risk-Based Funds Availability

-
-
- Permit a risk-based approach to funds availability, allowing hold times to be extended
 - when fraud signals are present.
 -
 -
 -
 - Clarify definitions of “alteration” and “reasonable cause to doubt collectability” to
 - ensure that community banks are not disproportionately burdened.
 -
 -
 -
- Require the use of check image analytics as part of a modernized risk framework.

-

-
-

3. Integration of Fraud and AML Oversight

-
-

- Encourage supervisory expectations that integrate fraud and AML obligations, particularly around mule accounts, scams, and authorized push payment fraud.

-

-
-

4. National Fraud Intelligence Framework

-
-

- Formalize public-private fraud intelligence hubs built on anonymized, privacy-compliant data.

-
-
-

- Expand and standardize frameworks such as FraudClassifierSM and ScamClassifierSM.

-
-
-

- Require participation from non-bank financial intermediaries, including fintechs, processors, and cryptocurrency platforms.

-

-
-

5. Federal Reserve Banks' Role in Operator-Level Tools

-
-
- Introduce confirmation-of-payee services for wires and instant payments.
-
-
-
- Create a centralized directory of fraud escalation contacts across institutions.
-
-
-
- Implement an electronic platform for breach-of-warranty claims to expedite resolution of check fraud.
-
-
-
- Explore development of an identity fraud classifier to create a baseline detection standard across the industry.
-
-
-

6. Encouragement of AI Innovation with Appropriate Safeguards

-
-
- Recognize that smaller institutions may lack internal resources to adopt advanced technologies.
-
-
-
- Establish safe harbors and regulatory sandboxes for supervised use of AI in fraud detection.
-
-
-
- Provide supervisory clarity to reduce regulatory uncertainty that discourages innovation.
-
-

-

III. Conclusion

Fraud has become a systemic infrastructure challenge that cannot be addressed by individual institutions in isolation. A national response built on cross-rail counterparty screening, risk-based funds availability, integrated fraud–AML oversight, standardized data sharing, and enhanced operator-level tools is required.

SardineAI and SonarAI are actively developing these capabilities and would welcome the opportunity to collaborate with regulators, financial institutions, and non-bank providers to advance pilot projects in these areas.

Thank you for the opportunity to provide these comments. We look forward to supporting the agencies' efforts to strengthen the security and integrity of the U.S. payment system.

Respectfully submitted,

Ravi Loganathan
Head of Banking and Policy, SardineAI Corp.
President, SonarAI LLC