Early Detection of Payments Fraud Through Scam Infrastructure Intelligence:

A CUBE3.AI Response to the Federal Banking Agencies' RFI

CUBE SECURITY INC (DBA CUBE3.AI)
[redacted]

September 11, 2025

OFFICE OF THE COMPTROLLER OF THE CURRENCY
Docket ID OCC–2025–0009
400 7th Street SW, Suite 3E–218
Washington, DC 20219

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
Docket No. OP–1866
20th Street and Constitution Avenue NW
Washington, DC 20551

FEDERAL DEPOSIT INSURANCE CORPORATION
RIN 3064–ZA49
550 17th Street NW
Washington, DC 20429

Re: Request for Information on Potential Actions to Address Payments Fraud
Docket ID OCC-2025-0009, Docket No. OP-1866, RIN 3064-ZA49

To Whom It May Concern:

CUBE3.AI appreciates the opportunity to submit comments in response to the joint Request for Information on Potential Actions to Address Payments Fraud issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation.

About CUBE3.AI

CUBE3.AI is a fraud prevention company focused on early interdiction of scam-related financial infrastructure. Our flagship product, Apex, identifies active money mule accounts, including Zelle tokens, U.S. bank accounts, and other payment endpoints used to receive stolen funds across multiple payment rails. We deliver verified, actionable intelligence to financial institutions enabling intervention before funds are irretrievably lost. This intelligence is uniquely positioned to address the types of authorized fraud and scams referenced throughout this RFI.

We are not disclosing proprietary methods in this public filing and are available to brief agency staff privately if helpful.

Executive Summary

Current payments fraud reporting is fragmented and delayed, with most data arising post-incident. CUBE3.AI's Apex system fills this gap by generating pre-victim fraud signals, particularly account-level identifiers reused by scammers across platforms and payment methods. Our platform has already cataloged hundreds of thousands of scammer accounts and related data elements, providing a substantial foundation for fraud prevention efforts. We recommend the agencies focus on practical steps that leverage early intelligence on scam recipient endpoints to reduce consumer losses, interbank disputes, and operational burden.

I. External Collaboration (Questions 1–4)

Recommendation: Establish formal collaboration with specialized intelligence providers that detect scam infrastructure in real-time.

Modern fraud schemes span multiple institutions and payment methods, often crossing traditional regulatory boundaries. Apex has demonstrated success in identifying high-risk accounts before financial institutions or consumers are aware of fraudulent activity. We recommend creating a joint working group between public and private stakeholders to integrate this early-warning intelligence into fraud prevention protocols.

CUBE3.AI Contribution: Our system identifies active U.S. bank accounts, Zelle tokens, and other payment endpoints used to receive fraud proceeds. Formal collaboration channels would enable earlier interdiction and reduce downstream disputes between institutions.

II. Consumer, Business, and Industry Education (Questions 5–8)

Recommendation: Enhance existing federal educational initiatives by incorporating real-world insights from active scam operations to make fraud awareness campaigns more targeted and effective.

Apex collects real-world scammer tactics and narratives through interactive intelligence gathering. These insights can support education efforts by informing targeted fraud awareness campaigns, particularly around emerging scam trends including pig butchering, refund scams, and romance fraud. We propose aggregated and anonymized sharing of scam interaction patterns to strengthen federal educational initiatives such as OCC's Safe Money series and the Federal Reserve's consumer alerts.

CUBE3.AI Contribution: Anonymized examples of current scammer narratives and payment instructions help make federal education resources more timely and specific, improving consumer and business recognition of evolving fraud tactics.

III. Regulation and Supervision (Questions 9–15)

Recommendation: Encourage supervised institutions to adopt tools that focus on intent detection, not just transaction monitoring, to address the growing threat of authorized payment fraud and integrate such intelligence into SAR workflows for increased investigative efficiency.

The growing threat of authorized payment fraud requires the adoption of tools that focus on intent detection, not just transaction monitoring.

CUBE3.AI Contribution: Apex helps financial institutions identify scam recipient accounts before funds are transferred, providing verified intelligence that can be integrated into fraud risk management systems and SAR workflows.

IV. Payments Fraud Data Collection and Information Sharing (Questions 16–20)

Recommendation: Support development of a centralized, privacy-safe repository for fraud recipient accounts using hashed identifiers and standardized fraud typologies.

Current fraud reporting is fragmented and delayed, with most data arising post-incident. Pre-victim fraud signals, particularly account-level identifiers reused by scammers across different scams and platforms, could fill this gap. We support creating a shared utility where such intelligence could enhance fraud prevention by providing forward-looking threat indicators alongside traditional incident documentation.

CUBE3.AI Contribution: Apex generates standardized, actionable indicators of active scam endpoints that enable earlier interdiction and reduce repeated losses across institutions. With hundreds of thousands of verified scammer accounts and associated data elements already in our system, our data could enhance this repository significantly.

V. Federal Reserve Banks' Operator Tools and Services (Questions 21–22)

Recommendation: Expand the use of real-time fraud detection capabilities such as confirmation of payee, risk scoring overlays, and negative list lookups for FedNow, ACH, and check services.

These operator-level tools would provide an additional layer of security to real-time payment rails by allowing participants to identify high-risk endpoints before transaction completion.

CUBE3.AI Contribution: Apex maintains dynamic watchlists of mule accounts and scammer-preferred endpoints. This data could inform such tools, offering an additional layer of security to real-time rails.

VI. General Questions (Questions 23–26)

Recommendation: Focus systemic improvements in fraud prevention on proactive detection of scam infrastructure, with emphasis on detecting and sharing mule accounts and payment endpoints before funds move.

The fraud types most impacting financial institution partners include romance scams, investment fraud, and impersonation schemes, all of which typically result in "authorized" losses by victims to scam-controlled endpoints. We believe that systemic improvements in fraud prevention will require proactive detection of scam infrastructure, and CUBE3.AI is ready to support this shift.

CUBE3.AI Contribution: Apex has proven highly effective in detecting the downstream accounts used to receive these funds before consumer harm occurs, providing the type of proactive scam infrastructure intelligence needed for systemic improvements in fraud prevention.

Conclusion

CUBE3.AI supports the agencies' goals to reduce payments fraud across check, ACH, wire, and instant payment systems. Our approach provides verified recipient-endpoint intelligence that complements existing fraud detection systems by identifying threats during their operational phase rather than after consumer harm occurs.

We appreciate the opportunity to contribute to this important initiative and are available to provide additional information, participate in pilot programs, or discuss data-sharing partnerships that demonstrate these approaches in practice.

Respectfully submitted,

Einaras von Gravrock
Founder and CEO
CUBE3.AI
e@cube3.ai
[redacted]

This comment is submitted in accordance with the requirements outlined in Docket ID OCC-2025-0009, Docket No. OP-1866, and RIN 3064-ZA49.