

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)

Docket No. OP-1866

September 11, 2025

Docket ID OCC-2025-0009 400 7th Street SW, Suite 3E-218

OFFICE OF THE COMPTROLLER OF THE CURRENCY

Washington, DC 20219 **BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM**

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.Al

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.

CUBE3.AI is a fraud prevention company focused on early interdiction of scam-related

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

Executive Summary Current payments fraud reporting is fragmented and delayed, with most data arising

We are not disclosing proprietary methods in this public filing and are available to

scammer accounts and related data elements, providing a substantial foundation for

disputes between institutions.

more targeted and effective.

increased investigative efficiency.

brief agency staff privately if helpful.

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.

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

collaboration channels would enable earlier interdiction and reduce downstream

tokens, and other payment endpoints used to receive fraud proceeds. Formal

Modern fraud schemes span multiple institutions and payment methods, often crossing traditional regulatory boundaries. Apex has demonstrated success in

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

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.

III. Regulation and Supervision (Questions 9-15)

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

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.

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

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 postincident. Pre-victim fraud signals, particularly account-level identifiers reused by scammers across different scams and platforms, could fill this gap. We support

providing forward-looking threat indicators alongside traditional incident documentation. CUBE3.Al Contribution: Apex generates standardized, actionable indicators of active scam endpoints that enable earlier interdiction and reduce repeated losses across

data elements already in our system, our data could enhance this repository

V. Federal Reserve Banks' Operator Tools and

Services (Questions 21–22)

ACH, and check services.

institutions. With hundreds of thousands of verified scammer accounts and associated

creating a shared utility where such intelligence could enhance fraud prevention by

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.Al 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.

Recommendation: Focus systemic improvements in fraud prevention on proactive

The fraud types most impacting financial institution partners include romance scams,

"authorized" losses by victims to scam-controlled endpoints. We believe that systemic

downstream accounts used to receive these funds before consumer harm occurs.

providing the type of proactive scam infrastructure intelligence needed for systemic

detection of scam infrastructure, with emphasis on detecting and sharing mule

investment fraud, and impersonation schemes, all of which typically result in

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

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

VI. General Questions (Questions 23–26)

accounts and payment endpoints before funds move.

CUBE3.AI supports the agencies' goals to reduce payments fraud across check,

improvements in fraud prevention.

practice. Respectfully submitted,

Founder and CEO

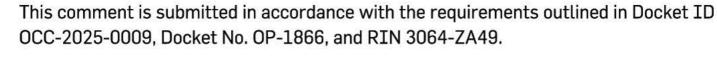
Conclusion

significantly.

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

Einaras von Gravrock

discuss data-sharing partnerships that demonstrate these approaches in



CUBE³

CUBE3.AI e@cuhe3.ai