

Top Cryptocurrency Exchange Defeats Account, ACH, and Card Fraud with DataVisor

CLIENT One of the world's best established cryptocurrency exchanges spearheading the next generation of decentralized finance. Present in over 150 countries, this company is truly a global leader enabling hundreds of thousands of users to perform trading and exchange activities with all the major digital assets, including Bitcoin, Bitcoin Cash, Ethereum, Ethereum Classic, and Litecoin.

CHALLENGES As part of an aggressive growth strategy, the client implemented a multi-channel approach that allowed users to fund their digital wallets through various means. Unfortunately, malicious actors were exploiting these channels by committing ACH fraud and by funding their accounts with stolen credit cards..

The client's growth strategy also relied on a promotion plan that provided economic incentives to new users. Some of these funds were being misappropriated by fraudsters who were serially registering new accounts that were later left dormant, raising concerns about their potential future use to commit financial crimes.

To retain its existing user base and maintain a high level of customer satisfaction, the client also decided to double down on its ATO protection measures. In sum, to ensure long-term business sustainability, the client needed to migrate from a rules-only detection system to a wholesome fraud solution.

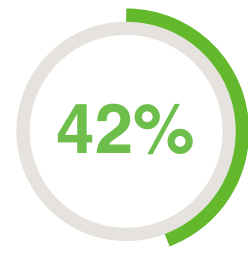
RESULTS



of fraudulent account openings detected before the disbursement of promotions



Auto-action on over 83% of detected fraud cases



detection accuracy improvement over existing in-house system

CLIENT CHALLENGES



Suppressing ACH and Credit Card Fraud to Reduce Losses

As part of its growth strategy, the client wanted to allow its clients to fund their accounts through as many means as possible; however, criminals were using stolen credit cards and fraudulent ACH transactions for these purposes. Therefore, the client needed to mitigate such fraud attacks early (i.e. before the respective funds were credited to the fraudulent accounts).



Efficiently Deploying High-ROI Promotions to Drive Growth

The client was experiencing an increase in the creation of fake accounts with the intention of abusing its promotion policies. Fraudsters were mass-registering accounts using synthetic or stolen identities, claiming the economic incentives, draining the funds, and leaving behind thousands of dormant accounts.



Eliminating ATOs and Improving the Customer Experience to Retain Users

The client needed to stop account takeover attempts before any losses materialized (e.g. before fiat and crypto balances were stolen). While the market offered several solutions, the client's team did not want to rely on high-friction verification measures.



Ensuring Scalability by Improving Review Efficiency

The client needed to migrate from its in-house rules-based fraud prevention system because it was no longer sustainable to allocate valuable resources (i.e. talented employees) to performing manual account opening and transaction reviews and maintaining in-house software that was becoming more and more obsolete with time.



Centralizing Risk Decisions to Simplify Internal Processes

The client needed a solution that could go beyond fraud detection to serve as a hub for managing its entire risk exposure in order to fight disparate systems and centralize decision-making with insights from several risk signals and systems.

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

DATA INTEGRATION

To lay the groundwork for a robust and scalable fraud prevention strategy, the client and DataVisor implemented a solution that could ingest the former's data by the terabytes. This data was then processed and enriched in a cloud-based system to automate the feature engineering process and extract meaningful insights in the form of multi-dimensional features that would later be ingested by machine learning models.

RULES ENGINE

The client's outdated architecture was replaced with a solution that allowed it to create and manage rules and continuously track and validate their performance with advanced capabilities such as back-and-forward testing. This allowed the client's team to manage complex rules at scale with maximum flexibility and a streamlined workflow, drastically reducing the number of cases that required human review and freeing up key employees to work on high value-add projects.

MACHINE LEARNING ENSEMBLE

To build an additional level of defense, DataVisor implemented a layer of supervised machine learning. This enabled the client to generalize patterns from historical attacks and to expand the number of features that were used to discern good and bad events. These supervised machine learning models also enabled the client to more accurately weigh those features.

On top of that, the client benefited from bespoke unsupervised machine learning algorithms that were fine-tuned by DataVisor's engineering team to deliver value right from the start. The UML component of the new solution was implemented to allow the client to identify fraud patterns without requiring prior labels on the data, which means that the client can now launch existing products in new countries with certainty from day one, leaving behind the expensive trial-and-error method of legacy fraud solutions.

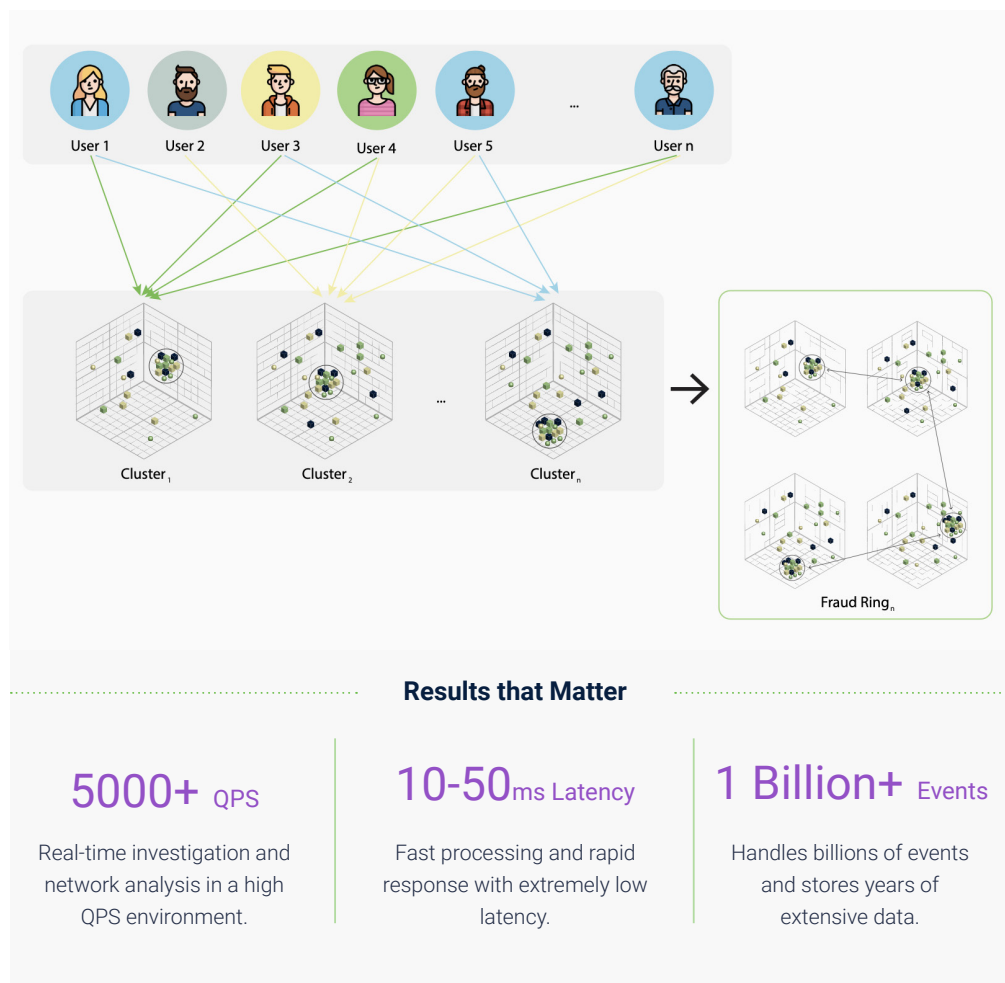
Furthermore, this machine learning ensemble enabled the client to leave behind transaction-level only approaches at fraud investigations and move towards a holistic-view strategy that evaluates every event in the context of the universe of transactions performed by all the users in existing records.

Insight: With DataVisor's true 360° view of events, the client was able to evaluate every application, account opening, transaction, or other action as part of a vast context composed of the totality of events available for scrutiny.

KNOWLEDGE GRAPH

As a final step to ensure the cohesion and usability of its new fraud prevention architecture, the client began using DataVisor's linkage-based fraud investigation solution. The many avant-garde investigation capabilities that the client benefited from include one-click investigations, intelligent searches based on advanced criteria, bulk decisions for similar cases, and dynamically-updated blacklists and whitelists.

In sum, Knowledge Graph enabled the client's team to connect data, analyze linkages, and uncover patterns among seemingly unrelated events and user profiles to uncover new fraud patterns in real-time. It also provided the client with the investigation tools it needed to ensure scalability by improving review efficiency.

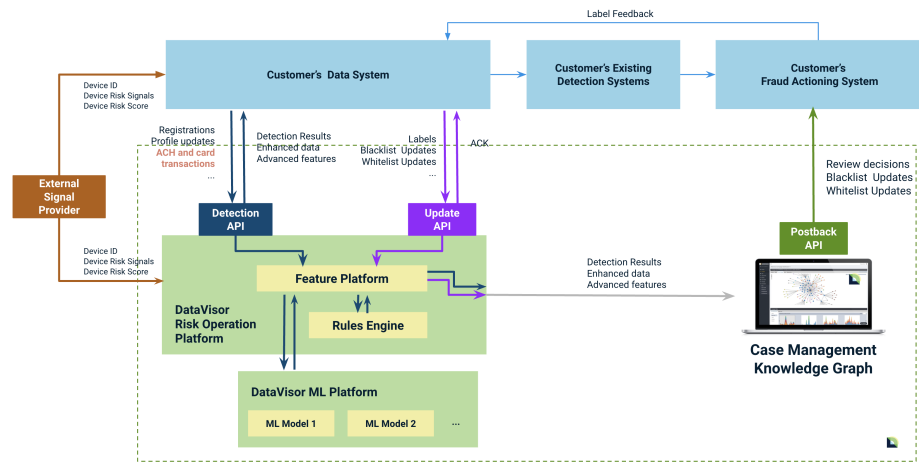


INTEGRATION AND LAUNCH

To meet the client’s requirements, it was paramount that the solutions described above were deployed with a minimal time-to-value lapse, ensuring zero service downtime during the implementation process, and enabling a straightforward integration with existing KYC system, technology stack, and other vendors. To set up the new fraud prevention architecture, DataVisor provided the client with a dedicated team of engineers that oversaw the integration and launch of the new fraud prevention architecture.

In parallel, a team of data scientists carried out the implementation of the machine learning ensemble model described above. To this purpose, the client provided its available historical data, which was used by DataVisor to train the supervised machine learning algorithm and test the unsupervised model to ensure that the results would deliver value from day one. Within days, the resulting algorithms were integrated to the new fraud architecture and the project’s launch was complete.

INTEGRATION DIAGRAM



Comprehensive Fraud Intelligence that Provides Fine-Grained Signals and Risk Scores

- 410 Million+ IP addresses
- 3.6 Million+ Email domains
- 300,000+ OS versions
- 5.3 Million+ User agent strings
- 160,000+ Device types
- 700,000+ Phone prefixes

Insight from 4.2 Billion+ Users and 800 Billion+ Events

- Financial Services
- E-Commerce
- Social Platform
- Mobile & Gaming
- Telecom & Travel
- Insurance

CONTACT US

If you are interested in learning how DataVisor can help bring your fraud detection to the next level or wish to start a trial to assess your current fraud exposure level, please contact us at: info@datavisor.com or visit us at www.datavisor.com

DATAVISOR

967 N. Shoreline Blvd.
Mountain View | CA 94043