



Leading US-based Card Issuer Reduces False Positives by 40% and Increases Detection

SUMMARY

One of the largest U.S.-based card Issuers with \$1.4 billion in annual revenue. The client’s consumer banking division was launching digital banking services to offer online checking, savings, ACH, check deposits and wire transfers through online and mobile applications. The issuer considered multiple solution vendors to enable multiple layers of protection. With DataVisor, the client implemented fraud protection in two phases.

PHASE 1

The clients’ immediate need was to protect its new digital channel and address the challenges with existing rules-based systems.

CHALLENGES

- » The client’s legacy fraud solution was unable to detect fraud rings in real time with its reactive rules-based approach.
- » High false positive rates caused by the rules-based detection system were impacting customer experience and wasting the fraud operations team’s resources.
- » Fraud reviewers were spending too much time—up to 10 minutes or more per case—reviewing individual transactions.

SOLUTION

- » Combined rules-based detection with machine learning for proactive detection to defeat fraud before damage occurs.
- » Overhauled case management system to meet the needs of the client’s fraud operations team.
- » Delivered reporting and insights to gauge and improve fraud analyst performance.

RESULTS



Reduced false positives by 40% with a holistic, AI-powered approach to fraud detection.



Increased fraud capture rate by 50% without needing to hire more reviewers.



Reduced review time per case to < 1 min with easy-to-use yet powerful case review tools.

CHALLENGES



Reactive, rules-only solutions could not detect fast-evolving fraud.

The client's legacy fraud platform was a rigid rules-based solution that was unable to detect new and emerging fraud patterns or connect the dots between fraud signals across the customer account lifecycle with accuracy and, as a result, fraud rings were going undetected.



High rates of false positives were impacting customer experience while fraud slipped through the cracks.

Cracking down on fraud rings using a rules-only approach created too much friction for good customers, as legitimate transactions were denied due to outdated rules. The client was looking to reduce false positives by 40% while taking a more proactive approach using AI-driven models to augment its rules-based detection system.



The case review process was slow, inefficient and ineffective.

The client's fraud analysts were spending the majority of their time reviewing individual cases – sometimes thousands per day – and were unable to keep pace with the volume when in the middle of large, coordinated attacks. This resulted in fraud attacks infiltrating the system using basic obfuscation techniques, leading to fraud loss. Not only was the labor-intensive, time-consuming case review process ineffective and costly, analysts lacked the ability to visualize key data and connect the dots between fraud signals across the account lifecycle to make accurate, data-driven decisions.

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

DataVisor's comprehensive ML models detect fraud with high precision, reducing false positives by 40% while capturing 50% more fraud.

Instead of relying on rules alone, DataVisor took an integrated, holistic approach, leveraging Unsupervised Machine Learning (UML) and Supervised Machine Learning (SML), alongside rules-based detection.

The UML model discerns patterns in large unstructured data sets in real time, enabling early detection and adaptive response to new and evolving fraud attacks, without relying on historic fraud labels. Combined with graphing techniques and advanced feature engineering, UML eliminates false positives while detecting additional fraud – such as mule accounts and ACH-based fraud that can signify fraud rings – that would be missed by a simple rules-based approach. The SML model targets specific types of known attack patterns and can defeat the fraudsters by tracking down their techniques for spoofing the digital signals, such as device and IP, and mimicking good users' behaviors. It compliments the UML model by precisely detecting incubation-type behaviors, such as making a couple of small testing transactions first before bursting out with a large withdrawal.

The DataVisor Rules Engine takes the rule-based fraud operations experience to another level, with its easy-to-use, drag-and-drop style GUI for essential tasks such as velocity feature creation, rule suggestions, rule simulation and A/B testing. It lowers the technical bar for fraud analysts, who can adjust detection logic on the fly with confidence and agility.

Rules Engine > Rule Details > Update Rule

Update Rule

Rule Name: Seller Location > 100 miles from reg loc

Rule Description: This rules checks if a seller's location is more than 100 miles from the reg location

Tags: _____

Rule Score: Null Set Score

ADD CONDITIONS

Conditions are evaluated based on feature values available within the same event.

Not Constant Values Feature

SPECIFY ACTIONS

Action: SEND SMS VERIFICATION

Advanced Options

Action: REVIEW QUEUE

Advanced Options

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

Phase 2:

In phase 2 of the engagement, the issuer replaced their existing orchestration hub with DataVisor to integrate multiple data sources and apply advanced fraud intelligence to take action from a single platform.

DataVisor helped the client's fraud operations team customize the DataVisor Case Management system, bringing in efficiency-oriented configurations around review queue setup, case auto-assigning, "next case" smart auto-advancing and "smart layouts" of the case details page. These features enabled viewers to see the most relevant risk data based on the fraud patterns detected by DataVisor systems, and helped to accelerate case reviews and decisioning by 72%.

Working with the client, DataVisor customized and streamlined the case management dashboard in three ways:

» **Data stitching:**

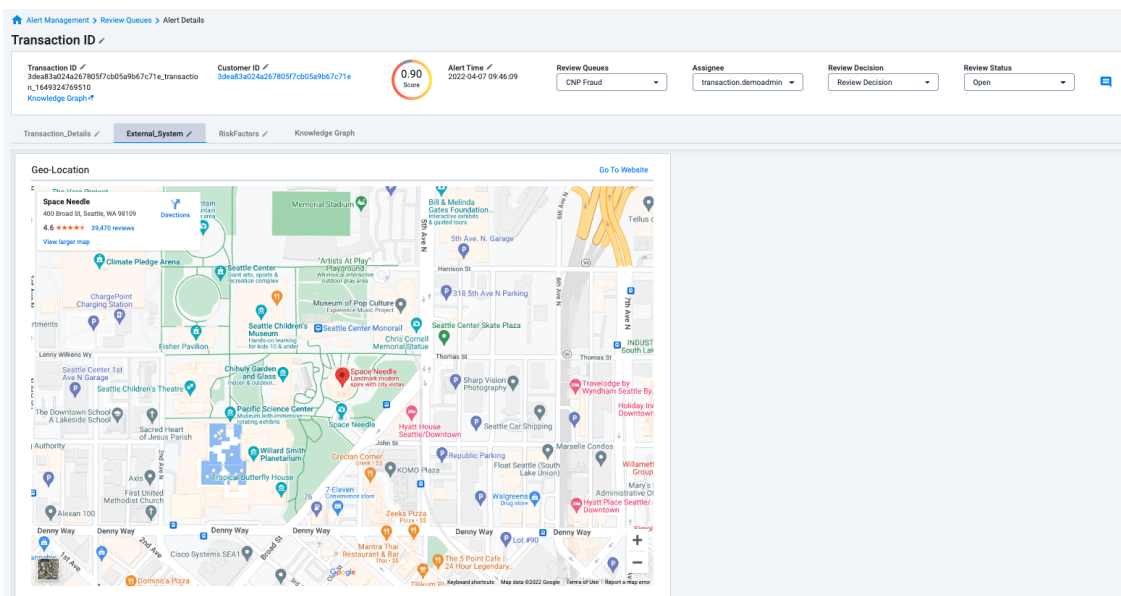
Previously, the client had no way to organize the various sources of data in a centralized place. For example, an analyst had to investigate multiple segregated databases – transaction history tables, customer profile tables and customer device usage logs – to review a single transaction. DataVisor's Case Management System comes with a Data Studio that intelligently joins data together accurately and renders all the relevant information onto a single review page, enabling analysts to make more informed decisions.

» **Enhanced intelligence:**

DataVisor's Case Management system integrates with other third-party data sources and tools that the client uses, bringing all the enhanced intelligence that a reviewer would ever need to review everything in one centralized system. Manual review decisions can also be sent to any other systems or microservices via API calls, so the downstream steps can benefit from a holistic view of the data and enhanced intelligence.

» **Ultimate flexibility and configurability:**

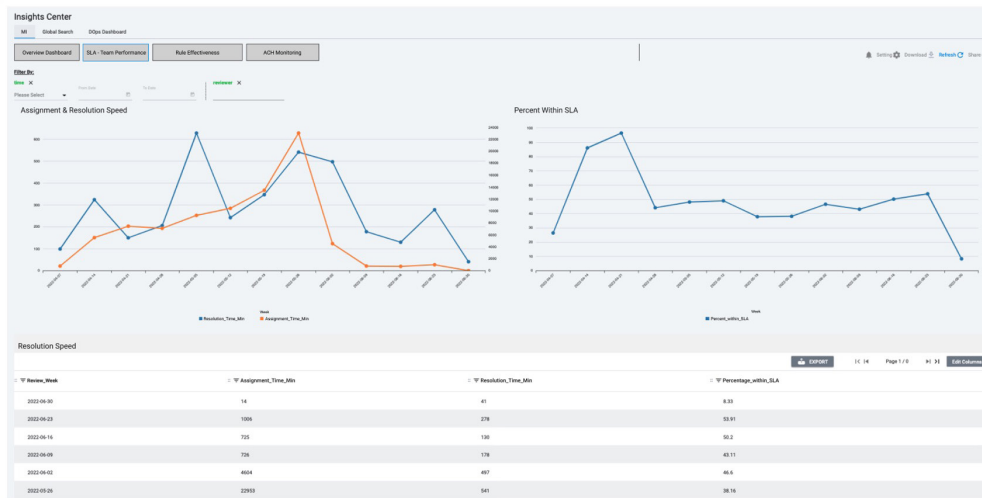
As a consumer banking service provider, the client's fraud operations team is responsible for reviewing risk in multiple types of transactions, where data schema, fraud patterns and review steps differ (i.e. ACH transfers, wire transfers and check deposits). With DataVisor's Case Management system, each transaction type has its own case review template, case details layout, case investigation workflow and review decision options. This boosts the fraud operations team's efficiency and helps them meet their goal of spending less than one minute per case, while achieving more than 95% review accuracy.



Additionally, DataVisor's Identity Graph enhances the review experience, enabling analysts to visualize hidden linkages from the transaction in question to other known risky entities in the ecosystem, such as blacklisted IP, frozen users, known mule accounts, risky devices and more. It gives the investigator a holistic but not overwhelming view of the case and helps them make a much more confident decision.

DataVisor Insights Center provides intelligence into analyst performance, driving efficiency and productivity.

The client uses DataVisor Insights Center to monitor analyst performance. An intuitive dashboard and detailed reports provide insight into the performance of all analysts, with complete visibility into how many transactions have been assigned to each analyst, which transactions are outstanding, and how quickly cases are reviewed and closed. Timestamps enable managers to generate reports by week or month, gauge analyst performance over time, and ensure nothing slips through the cracks. These insights help fraud teams improve speed and efficiency, and consistently meet the company's 24-hour SLA for reviewing transactions.



The client began to see results immediately, with DataVisor detecting fraud that had bypassed the client's legacy solution, providing real-time, highly accurate scores. Just as DataVisor has pioneered the application of transformational technologies to the challenges of modern digital threat attacks, our clients are now leading the way in embracing future-facing solutions that empower them to protect their customers, their data, and their businesses, so they can continue to grow and prosper over the next decade and beyond.

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