DATAVISOR

Financial Firms Fight Back

Financial Services Case Study Booklet

Banks, credit unions, lenders, fintechs, and other financial firms of all kinds are expected to grow, optimize their costs, and increase revenue regardless of any external challenges and competitive business environments. They need all the allies they can find, and artificial intelligence can make a big difference.

Among all disruptive forms of technology, AI has perhaps been the most heralded as an ally for financial firms. Teams that see its value and cut through the hype by understanding it as a means to achieve the truly consequential (yet relatively simple!) end of automation are poised to emerge as true leaders in their fields.

The power of automation lies precisely in its ability to help solve the most pervasive problems facing organizations—those that affect virtually every operational component. Among these problems, digital fraud is perhaps the most widespread in modern financial services:

> *A recent survey of more than 250 respondents found that 81% of banks see digital fraud as the top concern with respect to the global economy.*[1]

In this case study booklet, you'll find first-hand accounts of how five key financial services companies partnered with DataVisor to gain full control of their fraud exposure and protect their business and their clients by leveraging AI-powered automation coupled with the most advanced fraud and risk management platform.

By doing so, they were able to directly impact the three goals they care most about:

Growing sustainably by controlling fraud. Through AI-powered automation and advanced fraud management tools, financial firms can grow their business operations without increasing the size of their fraud teams. It's all about empowering fraud professionals of all levels to do more and work smarter.

Reducing costs by preventing fraud attacks. Proactively detecting and acting on fraud before losses materializes directly translates into a healthier cost structure. On top of this, the right fraud management platform can reduce total costs of ownership for financial firms.

Increasing revenue by managing risk exposure. By coupling AI with advanced analytics and decisioning tools, financial firms can launch new products, enter new markets, and attract new customers while remaining protected against fraud from day one.

And these are just a few examples…

DataVisor's secret is a comprehensive approach that delivers all the tools financial firms need to fight fraud in a single, flexible, and self-serve solution. Powered by machine learning at its core and extensible across use cases, it seamlessly integrates any data source (incl. 3rd party data) and combines rules engine, device intelligence, decision engine and case management to boost detection and minimize fraud losses.

[1] 2021 Treasury Perspectives Survey Report, Strategic Treasurer, page 9.

Case Studies

Product Sheet - Platform

Global Card Network Relies on DataVisor's AI Solutions to Boost Transaction Fraud Detection

CLIENT A global payment solutions provider handling several trillion dollars in payments each year.

CHALLENGES

- Limited ability to keep up with the rapidly changing tactics used by fraudsters due to fast model decay and long model-build time
- Low fraud detection capability due to limited insights from digital data, incomplete data labels and missing information in client data fields
- Lack of a modern infrastructure to handle massive-scale data sets across multiple channels resulting in real-time fraud detection

SOLUTIONS

- Leveraged DataVisor's open machine learning modeling platform that includes unsupervised learning combined with supervised learning to capture fast-evolving new fraud patterns
- Provided a feature engineering platform that works with imperfect or partially filled data so the client can utilize digital signals even when some fields are missing
- Provided a big data platform that can compute digital data with QPS and low latency, ensuring streamlined model development and production deployment

RESULTS

20%
transaction fraud detection uplift

94%
detection accuracy

5x
faster to build a new model, from 4-6 months to weeks

CLIENT CHALLENGES

Outdated fraud models were decaying upon deployment

Rules-based and supervised machine learning are commonly used to detect known fraud patterns. However, because fraud tactics evolve so quickly, these tools cannot effectively touch unknown fraud. Therefore, the client's machine learning models could mostly detect known fraud patterns but not unknown threats. This reactive fraud detection method led to financial losses over time.

Building a machine learning model was a time-consuming process for this global payment solution provider. The company needed to wait 3 months for the label to mature and needed to take another 2-3 months to build and validate the model. By the time it went into production, it had already started to decay.

Incomplete data limited client insights

The client mostly used non-PII data but no digital data because its existing models could only incorporate limited values from digital data.Therefore, the company was not able to derive useful intelligence to build good models, making fraud detection inefficient and leading to monetary losses.

Real-time functionality across channels was increasingly complex

Running real-time machine learning in production was challenging for the client because it is not easily parallelizable. For example, one transaction needs to be compared to many other potentially related transactions in many subspaces. Real-time clustering is the key to detect new patterns as fraudsters are moving fast.

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

DataVisor's Unsupervised Machine Learning augmented the client's rules and supervised machine learning to help detect more fraud

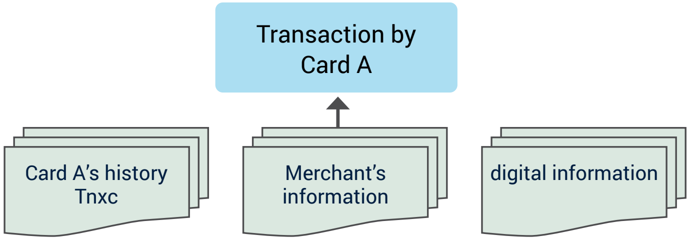
Unsupervised Machine Learning helped to fill in gaps in the client's existing fraud detection methods by analyzing all user behaviors and data without labels in real time and identifying suspicious patterns.This allowed fraud teams to detect attacks early and prevent them instead of doing damage control after the fact.

To illustrate, supervised machine learning may review single transactions, such as a canceled ACH transfer. On the surface, this cancellation might appear legitimate. But by reviewing data on a holistic level, FIs might find that many similar transactions are occurring from a single user or IP address in a short span, which could indicate fraud.

> DataVisor's unique capability of checking many other potentially related transactions in many subspaces and making real-time decisions helped the client detect fraud more accurately and much earlier than traditional solutions.

Traditional Rules or Supervised Learning

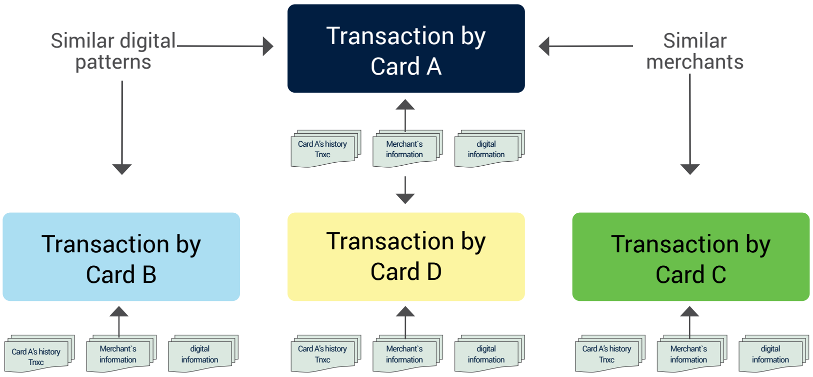
Decision based on the current event itself



Historical features, patterns

DataVisor Unsupervised Learning

Decision based on correlation with other events

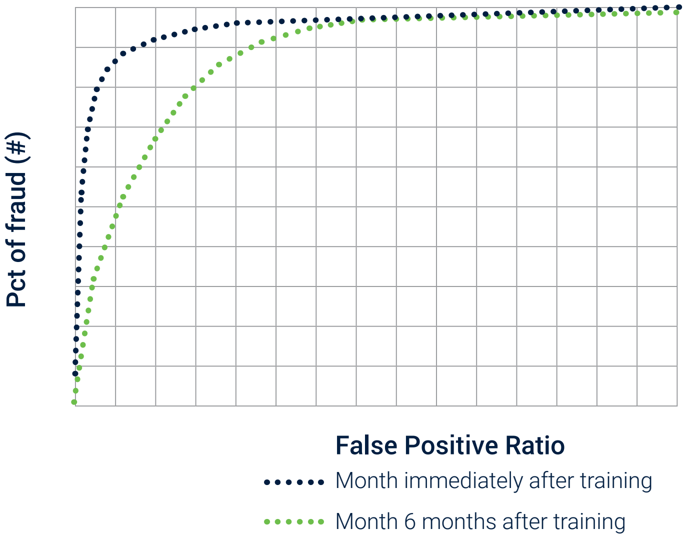


> Adding unsupervised machine learning to existing supervised machine learning models can capture more unknown fraud and help reduce model decay significantly.

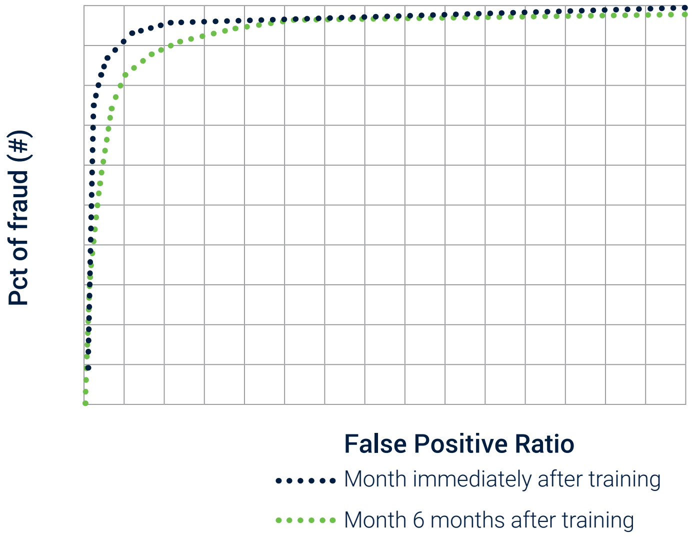
Because the unsupervised machine learning model does not rely on historical labels, it was fast to build and by nature adapted quickly to evolving fraud patterns. It did not require constant model retuning.

See the below chart: when the client was only using a supervised machine learning model, its model performance decayed significantly after 6 months. When the client added DataVisor's unsupervised machine learning solution to its supervised machine learning models, the fraud detection rate was still exceptional even after 6 months.

Supervised ML Only: Models Decayed Fast

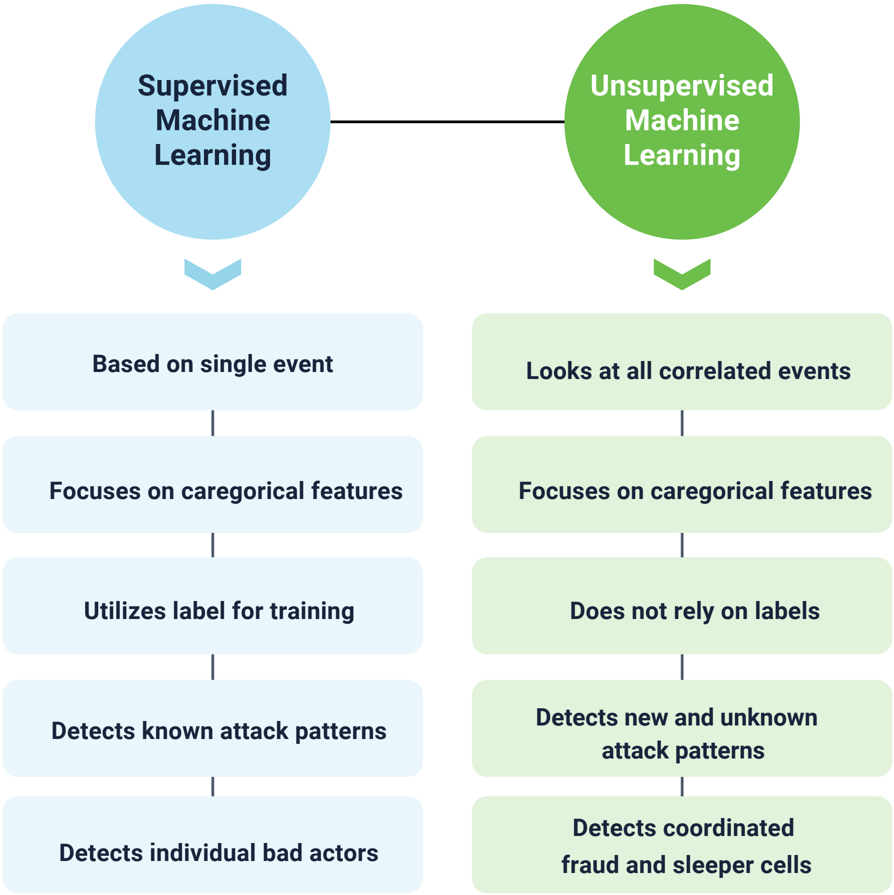


Unsupervised ML+ Supervised ML: Exceptional Detection Rate Even After 6 Months



DataVisor combined the power of supervised machine learning and unsupervised machine learning to achieve best-in-class protection

The client leveraged supervised machine learning to detect known fraud patterns, getting the best from its existing data. Then, DataVisor helped the company go a step further, using unsupervised machine learning to detect unknown and emerging fraud patterns in real time with no need for data labels and constant model retuning. This allowed the client to evolve alongside threats and take a proactive approach to fraud detection. Leveraging both types of machine learning, DataVisor provided comprehensive, best-in-class protection.



Supervised Machine Learning	Unsupervised Machine Learning
Based on single event	Looks at all correlated events
Focuses on caregorical features	Focuses on caregorical features
Utilizes label for training	Does not rely on labels
Detects known attack patterns	Detects new and unknown attack patterns
Detects individual bad actors	Detects coordinated fraud and sleeper cells

DataVisor facilitated real-time machine learning in production

DataVisor helped the client's fraud detection system scale and process massive-scale transaction data and user data with high QPS and only 50-100 ms latency. The system is highly distributed so that it can process and index all recent transactions in different subspaces. All fraud features are updated in real time and stored in memory.

DataVisor enabled bespoke fraud models with black-and-white insight

The client got complete control to build its own models using DataVisor's open platform and got full explainability of the generated results. This made it easy to:

- Build and tune unsupervised machine learning models in the easy-to-use platform
- Create customized features
- Use pre-built fraud solution packages for different fraud scenarios
- Review results with linkage analysis and get in-depth explanations with the detailed reason code
- Streamline transaction fraud detection using integrated model development and production deployment features

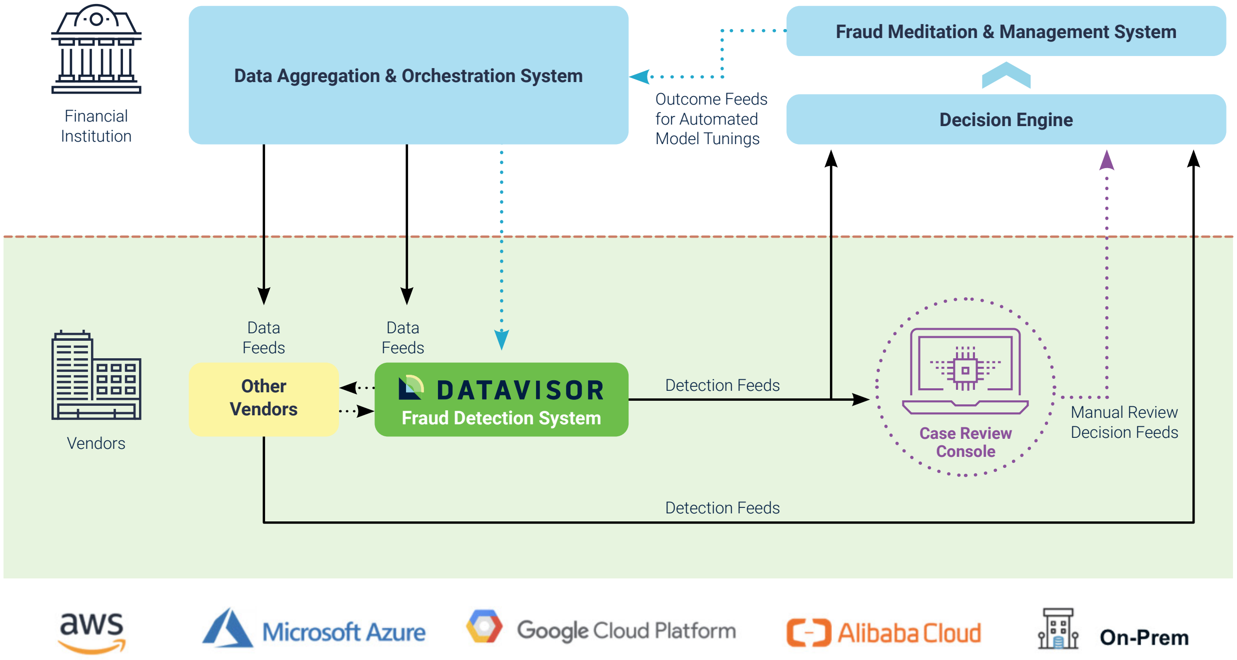
INTEGRATION

Our client enjoyed seamless integration with the client's existing systems and vendors. DataVisor's comprehensive fraud solution provided rapid and flexible integration with the client's systems in two weeks, and it supported:

- Real-time and batch processing
- Asynchronous and synchronous modes
- Structured and unstructured data
- Cloud and on-prem deployment

DataVisor's solution works seamlessly with the client's current data architecture, orchestration solutions, and third-party vendors. The client only needed to provide basic data fields and user events to get started.

INTEGRATION WITH THE CLIENT’S INTERNAL SYSTEM



Results that Matter

$15 Million+

Annual Savings

Reduce financial losses and manual review costs with accurate detection.

5x -20x

Efficiency Uplift

Boost review and decision with link analysis, smart investigations, auto decisions and bulk actions.

1-2 Weeks

Fast Integration

Provide rapid and flexible integration with your systems and support real time and batch processing.

Global Financial Institution Uses DataVisor to Fight Fraudulent Transactions in Real Time

Challenges

Millions in chargebacks resulting from fraudulent transactions continued to slip through existing detection systems. Meanwhile, the client's customers were having negative experiences due to high false positives that led to rejections of good customer transactions.

Results:

20%
Increase in detection

94%
Detection accuracy

0.9%
False positive rate

$12M+
Annual chargeback savings

About the Client

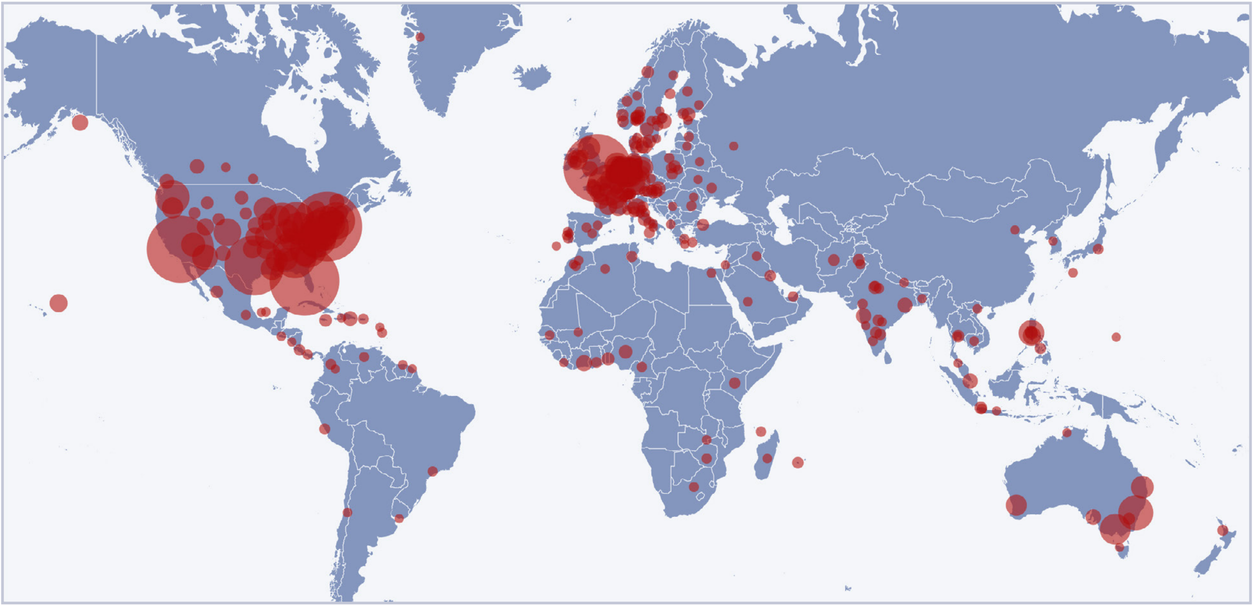
DataVisor partnered with a financial institution that services over 200 countries and has been in the financial services industry for more than 100 years.

The client had been relying on a large number of third-party fraud solutions that offered machine learning capabilities, and was employing an experienced internal fraud team. However, the organization was continuing to lose millions of dollars to fraudulent transactions.

Client Challenges

While the organization had existing systems in place to try and detect and deter fraudulent transactions, it struggled with the increasing sophistication and scale of the attacks that plagued its defenses. Its supervised machine learning fraud models, which worked incredibly well on training and testing data, were unable to detect new and emerging fraud attacks that were unknown before and during model production. As a result, significant numbers of fraudulent transactions were successfully eluding the client's systems, and fraudsters were making handsome profits in the process. Both the company and its customers were suffering.

Fraudulent transactions are extremely difficult to catch because the decision to block a transaction needs to occur within seconds. Failure to do so can mean serious financial loss. Yet unintentionally rejecting a good user's transaction will negatively impact their experience, and this has a downstream effect on the company's top line. As attacks continued to come, the company's concerns became more dire. The company's fraud team—while both large and competent—simply couldn't keep up, let alone get ahead. The attacks were too numerous, evolved too fast, and were too sophisticated.



Geo view of malicious accounts detected by DataVisor's solution

How DataVisor Helped

Boosted Fraud Detection

DataVisor's proprietary unsupervised machine learning (UML) algorithms detected 20% more fraudulent transactions on top of what the company's existing solutions were able to identify, with 94% accuracy. By capturing new and fast-evolving fraud patterns without the need for historic labels, large datasets, or training time, the impact was immediate, and significant—more than $12M in savings.

Real-Time Decisioning

Upon deploying the DataVisor solution, the client began receiving stable, accurate, and failure-free fraud signals, with results returned within 10 milliseconds. They were able to make decisions in real time, with complete confidence.

Early Detection

DataVisor's solution detected fraudulent accounts before they could conduct transactions that would have resulted in financial loss. DataVisor prevented over 90% of the fraudulent transactions attempted by the bad accounts, at least 3 hours in advance.

Frictionless Customer Experience

In addition to delivering high-accuracy detection results, DataVisor's systems produced a strikingly low false positive rate of only 0.9%. By preventing good customers from being incorrectly rejected, overall customer experience improved substantially.

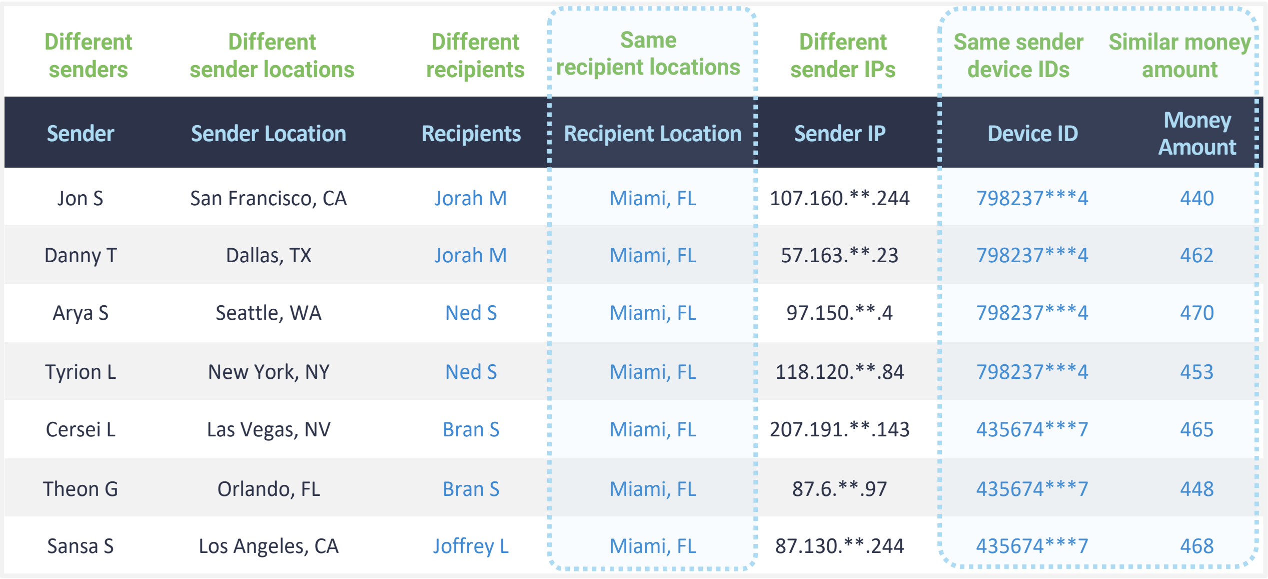
Fraud Pattern Detected

Mass-registered accounts

A large fraud ring included 500+ fraudulent accounts that were created to transfer money to different recipients. Relying on DataVisor's fraud solutions, the client was able to detect these accounts in real time by uncovering telltale patterns.

- **Evasion techniques**
  All the sender's accounts had different IP addresses and names and they sent money to different recipients. This seemingly-legitimate attack patterns made it hard for the client's existing solutions to detect them.

- **Patterns DataVisor detected**
  Similar patterns were discovered within the fraud ring–the sender's accounts were all registered from data center IP subnets, and the senders all used the same device IDs to transfer the same amount of currency ($440-$470) to the same locations, as shown in the table. DataVisor's contextual detection strategies and holistic data analysis brought these coordinated activities to light.



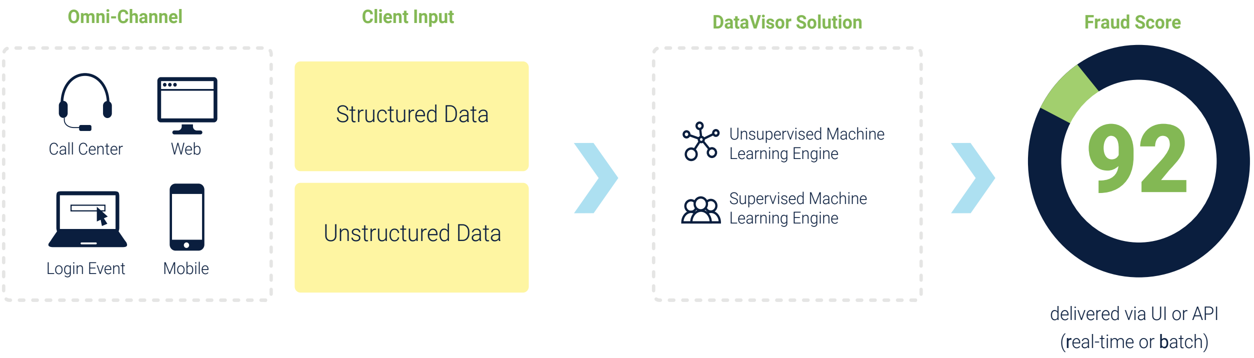
Different senders	Different sender locations	Different recipients	Same recipient locations	Different sender IPs	Same sender device IDs	Similar money amount
Sender	**Sender Location**	**Recipients**	**Recipient Location**	**Sender IP**	**Device ID**	**Money Amount**
Jon S	San Francisco, CA	Jorah M	Miami, FL	107.160.**.244	798237***4	440
Danny T	Dallas, TX	Jorah M	Miami, FL	57.163.**.23	798237***4	462
Arya S	Seattle, WA	Ned S	Miami, FL	97.150.**.4	798237***4	470
Tyrion L	New York, NY	Ned S	Miami, FL	118.120.**.84	798237***4	453
Cersei L	Las Vegas, NV	Bran S	Miami, FL	207.191.**.143	435674***7	465
Theon G	Orlando, FL	Bran S	Miami, FL	87.6.**.97	435674***7	448
Sansa S	Los Angeles, CA	Joffrey L	Miami, FL	87.130.**.244	435674***7	468

** Data shown above is for illustration purposes only and does not pertain to any of DataVisor's clients*

Insight: DataVisor detected mass-registered accounts that utilized sophisticated techniques to make fraudulent money transactions.

How DataVisor Detection Works

DataVisor combines adaptive machine learning technology and powerful investigative workflows to deliver real-time fraud analytics. While conventional rules or model-based solutions require “pre-knowledge” of how attacks work to be effective, DataVisor is **designed** to detect fraud attacks without any historic labels, large datasets, or training time. Drawing on a proprietary UML engine, **DataVisor** accelerates detection by analyzing all accounts and events simultaneously and identifying suspicious clusters of malicious activity—even at the point of account registration. **In addition, DataVisor combines UML with** supervised machine learning solutions **and therefore** excels at finding both known and unknown attacks.



Omni-Channel

Call Center

Web

Login Event

Mobile

Client Input

Structured Data

Unstructured Data

DataVisor Solution

Unsupervised Machine Learning Engine

Supervised Machine Learning Engine

Fraud Score

92

delivered via UI or API
(real-time or batch)

Results that Matter

$15 Million+

Annual Savings

Reduce financial losses and manual review costs with accurate detection.

5x -20x

Efficiency Uplift

Boost review and decision with link analysis, smart investigations, auto decisions and bulk actions.

1-2 Weeks

Fast Integration

Provide rapid and flexible integration with your systems and support real time and batch processing.

Top 5 Crypto Exchange Defeats Account, ACH, and Card Fraud with DataVisor

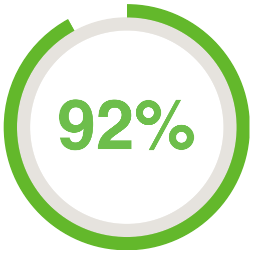
CLIENT One of the world's best-established cryptocurrency exchanges spearheading the next generation of decentralized finance. Present in several dozen countries, this company is truly a global leader enabling hundreds of thousands of users to perform trading and exchange activities with all the major 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..

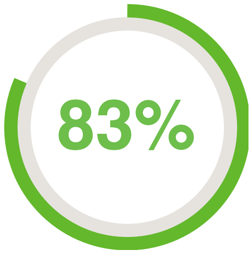
The client's growth strategy also relied on a promotion plan that provided economic incentives to new users. Some of these funds were being misappropriated by fraudsters who were serially registering new accounts that were later left dormant, raising concerns about their potential future use to commit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

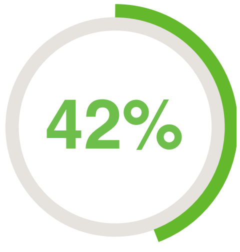
RESULTS



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.

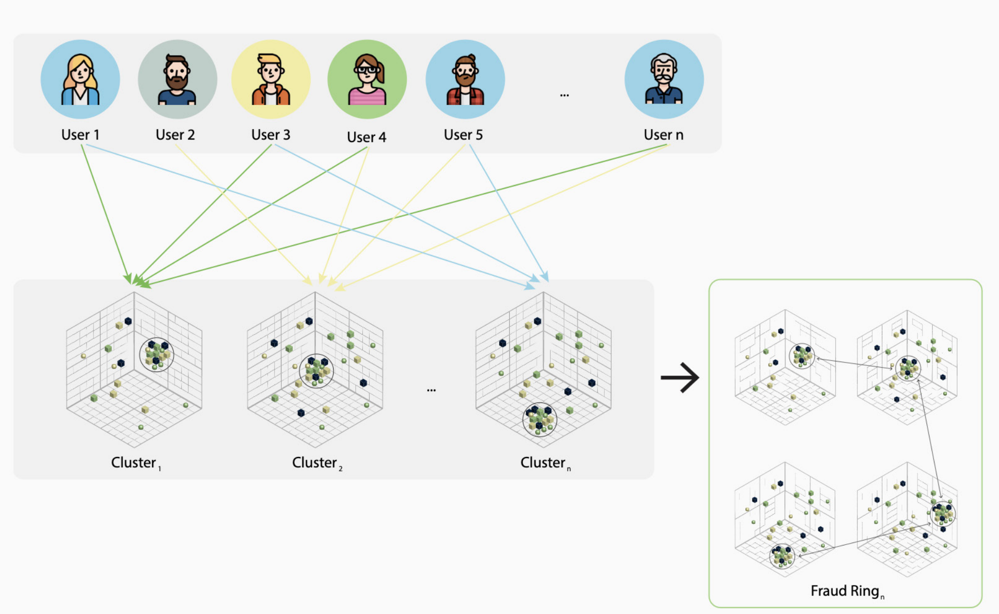
Furthermore, this machine learning ensemble enabled the client to leave behind transaction-level only approaches at fraud investigations and move towards a holistic-view strategy that evaluates every event in the context of the universe of transactions performed by all the users in existing records.

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.



Results that Matter

5000+ QPS

Real-time investigation and network analysis in a high QPS environment.

10-50ms Latency

Fast processing and rapid response with extremely low latency.

1 Billion+ Events

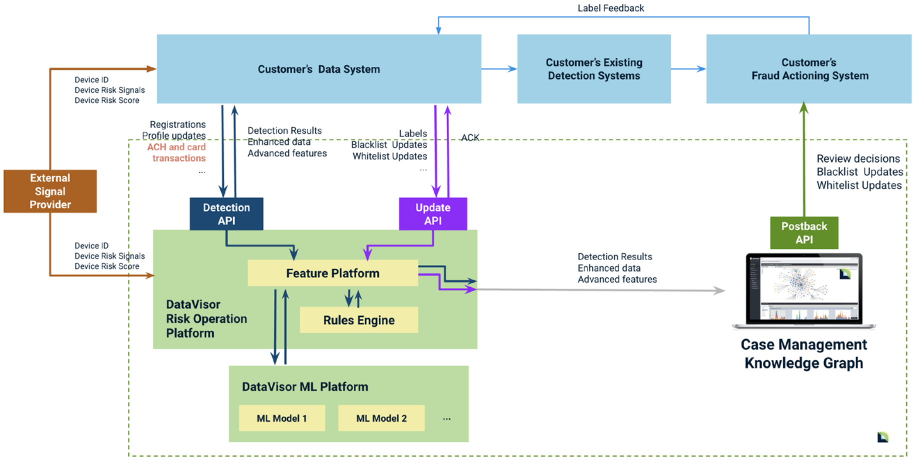
Handles billions of events and stores years of extensive data.

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



Results that Matter

$15 Million+

Annual Savings

Reduce financial losses and manual review costs with accurate detection.

5x -20x

Efficiency Uplift

Boost review and decision with link analysis, smart investigations, auto decisions and bulk actions.

1-2 Weeks

Fast Integration

Provide rapid and flexible integration with your systems and support real time and batch processing.

BNPL Case Study - Raising the Bar for Customer Experience and Reducing Fraud with Machine Learning

CLIENT

An innovative American financial technology company that pioneered the point of sale finance industry by providing a fast, transparent, and more inclusive loans to consumers.

CHALLENGE

Fraudsters were using synthetic identities to mass register fraudulent new accounts and then requesting loans that were never paid back.

Solving the well-known industry trade-off between customer experience and fraud prevention.

High rates of account takeovers and promotion/benefit abuse indicated that the client had outgrown its insourced fraud model.

SOLUTIONS

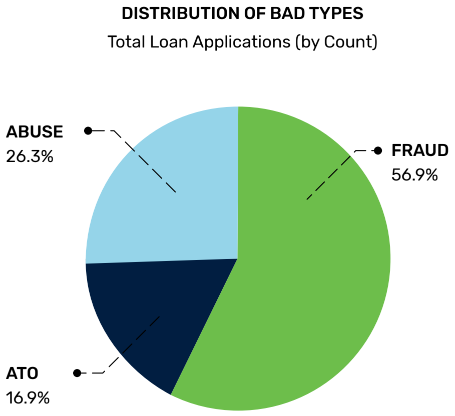
- Processed vast amounts of proprietary data with Feature Platform and enriched it with insights from 4.5B third-party accounts and 1T events.
- Leveraged the Rules Engine tool to create and manage commands with heightened efficiency and accuracy.
- Gained a 360° view of fraud data and its connections using DataVisor's Knowledge Graph.
- Leveraged the Case Management toolset to take fast, efficient, and informed decisions in real-time.

RESULTS

41%	320+	5x
reduction in hurt ratio, a measure of false positives.	**fraud rings detected, some of them related to over $80k in losses per attack.**	**estimated review efficiency improvement.**

CLIENT CHALLENGES

The client was experiencing three different types of fraud, distributed as follows:



In this context it approached DataVisor with the following top-of-mind goals:

- Reducing Friction for Good Borrowers

Reducing the hurt ratio was determined as a top priority because the client expressed that a high-quality customer experience was paramount to success in a highly competitive market.

The hurt ratio measures false positives by indicating how many non-fraudulent events (i.e. credit applications) are flagged for review for every fraudulent one. The client experienced a hurt ratio of five (5/1), which means that its fraud detection system was flagging five good credit applications for review for every fraudulent one. A low hurt ratio means a smoother customer experience where good borrowers are not subject to unnecessary identification measures.

- Increasing the Percent of Fraudulent Applications Detected

A low rate of fraud detection ultimately resulted in first payment defaults, which reduced the client's profits.

- Uncovering Coordinated Fraud Attacks

Since it operates in a highly dynamic environment where thousands of consumers request small to medium-sized loans every day, the client needed a solution that could handle and make sense of vast amounts of data to stop organized cybercriminals.

- Improving Review Efficiency

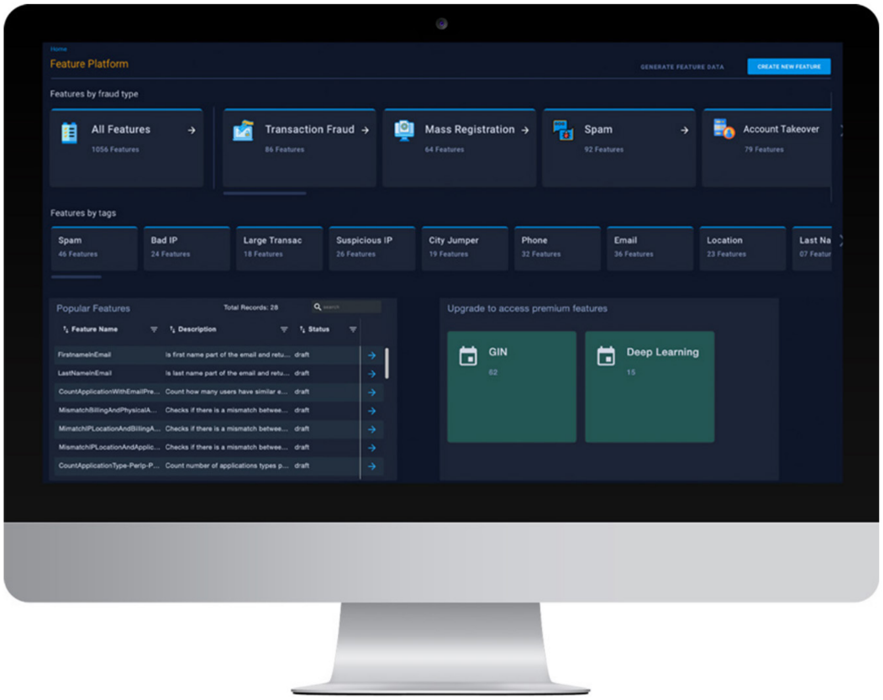
A high review time per application resulted in an increase in operational costs for the client because it had to hire more employees, which reduced the scalability of its business model.

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

FEATURE PLATFORM

The solution starts with data and DataVisor's Feature Platform. Here, the Client's data was ingested and processed by our cloud-based system and leveraged by the client to automate the feature engineering process and produce thousands of auto-derived multidimensional features. These features are then used to develop artificial intelligence models using DataVisor's unique unsupervised machine learning algorithm as well as open-source machine learning frameworks such as XGBoost.

Led to savings in the tens of thousands of dollars in in-house feature creation costs and machine learning model development and enabled the client to bypass the time-to-market cycle of developing its own features and model, which can last up to five years for comparable financial technology companies.



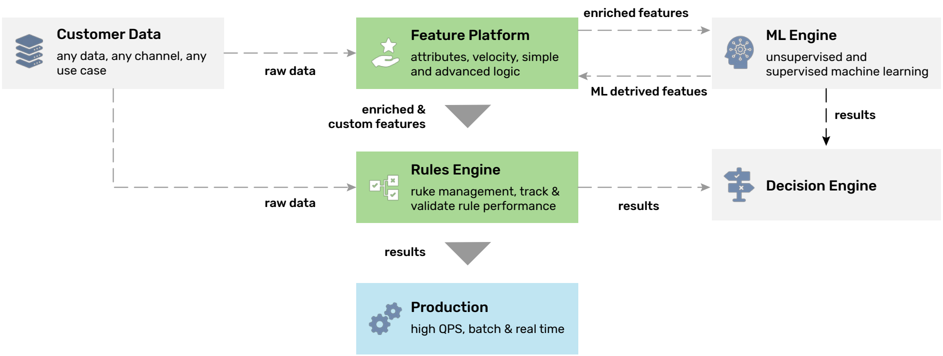
Feature Name	Description	Status
FirstnameInEmail	Is first name part of the email and retu...	draft
LastNameInEmail	Is last name part of the email and retu...	draft
CountApplicationWithEmailPre...	Count how many users have similar e...	draft
MismatchBillingAndPhysicalA...	Checks if there is a mismatch betwee...	draft
MimatchIPLocationAndBillingA...	Checks if there is a mismatch betwee...	draft
MismatchIPLocationAndApplic...	Checks if there is a mismatch betwee...	draft
CountApplicationType-Perlp-P...	Count number of applications types p...	draft

Improving the customer experience:
More and cleaner data means smarter decisions that thwart fraud but do not tag good users as bad.

RULES ENGINE

With the data in the right place, the Rules Engine was the next step taken to build a holistic fraud protection approach.

The client leveraged DataVisor's Rules Engine to create and manage command sets and to systematically organize rules and track and validate their performance with advanced capabilities such as backtesting and forward testing. The client also combined the results from the Rules Engine with the results from the machine learning model in a centralized decision-making process that promoted enhanced performance.


Customer Data
any data, any channel, any use case
raw data
Feature Platform
attributes, velocity, simple and advanced logic
enriched features
ML Engine
unsupervised and supervised machine learning
ML detrived featues
enriched & custom features
results
Rules Engine
ruke management, track & validate rule performance
raw data
results
Decision Engine
results
Production
high QPS, batch & real time

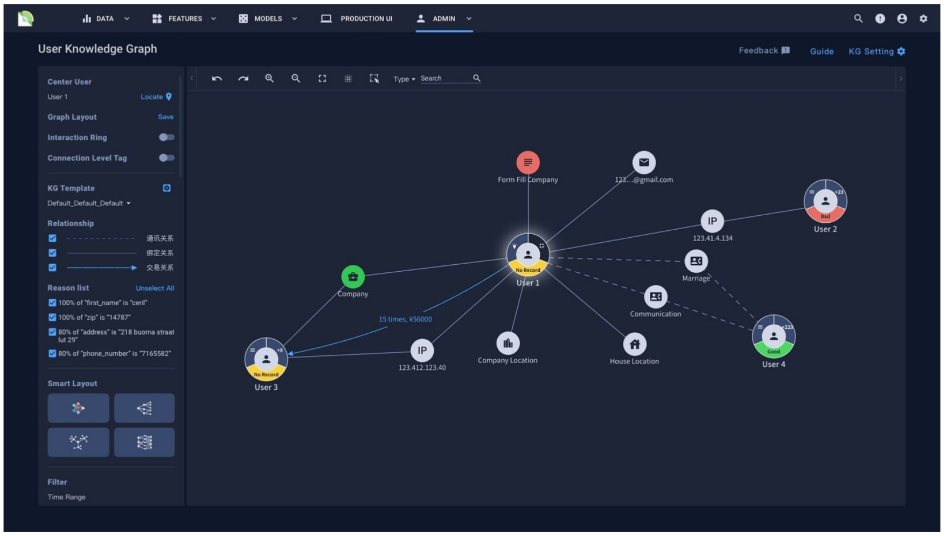
> *Improving the customer experience:*
> *Not all rules are created equal. The client built an auditable and testable rules policy that is in constant self-improvement with the Rules Engine.*

KNOWLEDGE GRAPH AND CASE MANAGEMENT

With a firm base in data and a robust approach to rules in place, the Client began using DataVisor's Knowledge Graph and Case Management tools to visualize fraud insights and take swift actions based on them.

The Knowledge Graph analyzes vast amounts of data to uncover connections between seemingly independent events that are invisible to the naked eye. These connections come in the form of shared entities, groups, money flows, IPs, emails, and other attributes between transactions and are presented in an easy-easy-to-use interface that powers data-driven decisions at the highest level.

Once a comprehensive and interactive view of the data was in place, DataVisor's Case Management tool enabled the client to take context-enriched decisions that stopped fraud with augmented accuracy and an estimated 5x review efficiency gain. Among other features, the client was able to take bulk decisions for groups of events and create custom blacklists and whitelists that simplified internal processes substantially.



Center User
User 1 Locate

Graph Layout Save

Interaction Ring

Connection Level Tag

KG Template

Default_Default_Default

Relationship

☑ 通讯关系
☑ 绑定关系
☑ 交易关系

Reason list Unselect All

☑ 100% of "first_name" is "ceril"
☑ 100% of "zip" is "14787"
☑ 80% of "address" is "218 buorna straat lut 29"
☑ 80% of "phone_number" is "7165582"

Smart Layout

Filter

Time Range

A noteworthy feature of DataVisor's platform is the One-Click Investigation, which reduces the amount of friction throughout the customer experience to help operational teams investigate faster and smarter and avoid keeping the customer waiting. Once it builds a linkage, it can automatically connect the new entities or events with previously detected fraud rings; therefore, if the client finds that some new users are strongly connected with known bad actors, the client can immediately mark new users as bad without spending extra time for manual searches or investigations from scratch.

Improving the customer experience:
By allowing its team to whitelist good customers and investigate cases with a single click, the client ensured that good borrowers returned and that applications that need review are promptly cleared without keeping the customer waiting.

LAUNCH AND INTEGRATION

To ensure that the client's needs were addressed promptly and in full, DataVisor implemented its proven deployment strategy. First, a bespoke model that combined the best of supervised and unsupervised machine learning was developed for the client. Then, this model was trained using data from several months' worth of credit applications and their performance. Then, the model was fine-tuned by a consortium of DataVisor engineers and data scientists to enable it to hit the ground running and begin detecting fraud from day one.

DataVisor tested the model and its results were then compared to the observed performance of the loans. Before launch, the client received a presentation that highlighted all the benefits of the DataVisor approach with clear and actionable insights on its own data.

All in all, DataVisor's solution is designed for seamless integration, and its trained team of professionals delivered value to the client within 2 weeks of the start of the process. Adding to this, DataVisor's Knowledge Graph and Case Management tools connect to data from the client's internal systems and third-party vendors in real-time and DataVisor ensured that its solution worked seamlessly with the client's current data architecture, orchestration solutions, and technology stack.

The client only needed to provide its dataset and review the results of the model to get the implementation in motion. From there, the DataVisor team followed a process that has been thoroughly proven across the financial industry.

Results that Matter

$15 Million+

Annual Savings

Reduce financial losses and manual review costs with accurate detection.

5x -20x

Efficiency Uplift

Boost review and decision with link analysis, smart investigations, auto decisions and bulk actions.

1-2 Weeks

Fast Integration

Provide rapid and flexible integration with your systems and support real time and batch processing.

Large Federal Credit Union Leverages Datavisor Unified Platform for Holistic Fraud Analysis

CLIENT A large federal credit union with thousands of members nationwide and more than $3 billion in assets.

CHALLENGES

» Keeping up with growing fraud resulted in the operations team doubling. Instead of expanding the ops team, the client wanted to invest in systems/tools so they are more scalable.

» Managing multiple disconnected systems resulted in high operational overhead and prevented holistic fraud analysis.

» Reactive, rules-based fraud solutions were unable to keep pace with fast-evolving fraud.

» Limited budget and operations resources made reviewing more risky cases difficult.

SOLUTION

» Enabled comprehensive protection across multiple use cases in a single, one-stop fraud and risk management platform.

» Combined rules-based detection with machine-learning models to enable a proactive approach.

» Leveraged Knowledge Graph to visualize patterns and connections between fraud signals, reducing false positives and simplifying decision-making.

» Used device risk signals provided by DataVisor to directly detect fraud from manipulated devices and bots.

» Reduced operational overhead resulting in strong ROI.

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

DataVisor delivered a unified platform for comprehensive fraud protection across multiple use cases.

With DataVisor's all-in-one platform, the credit union can detect multiple types of fraud effectively, including membership application fraud, loan application fraud, credit card fraud, ACH transaction fraud, wire transfer fraud and more. Instead of managing disparate systems for each type of fraud, the client benefits from reduced operational overhead and holistic analysis of all relevant transaction data and fraud signals in one centralized platform in DataVisor, which simplifes decision-making.

The client also brought in their existing, third-party data partners – credit bureau, dark web monitoring and ID verification. With DataVisor's out-of-the-box integrations and flexible microservice-based integration capabilities, the credit union do not have to rely on its IT team to perform complex integrations with data partners. Instead, DataVisor" microservice-based platform became the integration hub, enabling the credit union to leverage data partners to access enhanced signals for fraud detection in less than two weeks.

DataVisor's linkage graph-based review tools enable the client's fraud operations teams to review and resolve questionable transactions faster and more efficiently. Users can reference an intuitive dashboard to identify potential risks along with the context and data they need to complete their investigation rapidly. To date, the cusotmer has leveraged Datavisor to stop multiple coordinated loan application attacks using synthetic and stolen IDs, identify social security numbers and employment discrepancies, resolve address and geolocation disputes, and identify device-based fraud rings.

DataVisor Combines Machine Learning with Rules for Proactive Protection

Rigid rules-based fraud detection is incapable of detecting new and evolving fraud patterns with a high degree of accuracy, allowing fraud to slip through the cracks. By combining a rules-based approach with advanced machine-learning models, DataVisor provided the customer with a more proactive approach to detect more attacks early, before they cause damage. This greatly improved the member experience, while largely reducing the manual tasks involved in analyzing attack patterns and iterating rules.

DataVisor's Identity Graph visualizes sophisticated fraud patterns to help identify fraud rings.

The credit union relies on Datavisor's Identity Graph for reviewing loan applications and making connections between various fraud signals across transactions, enabling rapid identification of fraud patterns and crime rings with a high degree of accuracy. Identity Graph highlights suspicious relationships and supports one-click investigations that automatically connect new entities or events with identified fraud rings, such as those outlined in Figure 1:

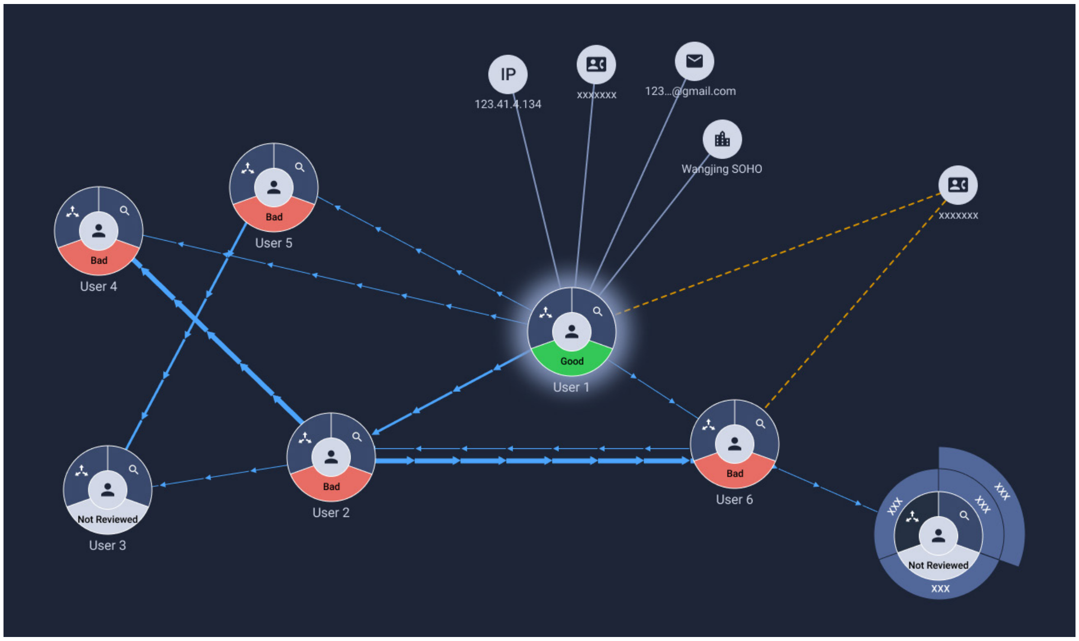


Figure 1

In the table above, each loan is unique and has a unique user ID. However, the IP address is the same for six of the loans, and originating from just two devices. Additionally, the email addresses follow the same pattern. By surfacing this information in a graph, DataVisor makes it easy for the client to spot suspicious patterns that could indicate a fraud ring or other malicious activity.

The client is using Identity Graph to detect and investigate multiple types of fraud, including application fraud, identity fraud, transaction fraud, and account takeovers (ATO) as well as fraud rings. Using this contextual approach that looks beyond isolated behaviors, the team can make quick data-driven decisions while dramatically increasing operational efficiency.

Device Intelligence helps prevent mobile fraud by detecting malicious devices.

DataVisor Device Intelligence not only provides an industry-leading device fingerprinting solution for mobile and web users, it leverages non-PII device data at the source to detect compromised devices resulting from device signal spoofing, emulators, hooked devices or repackaged apps. It enables the customer's fraud team to make accurate distinctions between legitimate human users and programmed bot-controlled users. Leveraging these risk signals, the customer can detect 36% of the risky transactions without having to use more sophisticated logics such as cross-dimensional velocities or ML algorithms.

DataVisor delivered customization and tailored reports to meet the client's specific needs.

Working directly with the client's fraud team, DataVisor created custom signals and data fields within the user interface to capture information and comments for auto-populating other mission-critical systems. This is made possible through a direct API integration between DataVisor's case management system and the customer's own case report systems. By leveraging the API, the customer saved 300+ hours in manual operations by eliminating the need to copy and paste information into Excel. Additionally, DataVisor provided a guided management dashboard tool for the customer to develop tailored fraud operations reports, to track and optimize the fraud team's performance and efficiency.

DataVisor AI-Powered Fraud and Risk Platform

DataVisor's unified platform integrates signals from heterogeneous data sources to deliver superior fraud detection and minimize financial loss.Powered by an extensive array of tools and machine learning algorithms that include unsupervised and supervised learning, rules engine, feature engineering, device intelligence and link analysis, our platform enables a holistic fraud prevention strategy for enterprises to proactively defeat fraud, grow business safely and create frictionless customer experience.

Capabilities

Data Integration

Integrate internal and third-party data from omni channels in real time or in batch. Accelerate data cleansing and ETL for rapid model development and decision making.

Feature Engineering

Get out-of-the-box fraud feature packages to jump start protection. Analyze years' of data to create production-ready features via UI or coding without IT dependency.

Machine Learning

Provide fraud signals from supervised and unsupervised models. Import external models or build, test and deploy your own models with our open platform.

Decision Management

Manage business rules and decision flows with built-in simulation and real-time rule performance analysis. Operationalize business rules with speed and governance.

Case Management

Get alerts, analyze cases and manage queues and user access. Support bulk actions on fraud rings and auto decisions. Get detailed reason codes and a full audit trail.

Analytical Insights

Monitor the performance of fraud strategies in real time. Extract insights from actioned results to improve the strategies with off-the-shelf reports and custom queries.

Add-On Modules

UML Modeling Studio

Build unsupervised machine learning models with an open platform to detect unknown fraud without waiting for historical data and labels. Have complete control when building models, get full transparency and explainability, and meet compliance requirements.

Knowledge Graph

Ingest internal and third-party data in real time to perform entity resolution and link analysis. Auto discover the most suspicious patterns, provide smart investigation to get granular insights, and support directly adding entities to blocklists and allowlists.

Device and Behavior Intelligence

Detect fraud by using the lightweight SDK to get device signals, behavior data and risk indicators. Uncover emulators, botnets, rooting and more. Generate unique device IDs, no matter how fraudsters manipulate the apps or devices.

Solutions for Every Team

For Fraud Leaders

Ensure safe and rapid business growth, reduce fraud losses and remove customer frictions with DataVisor's integrated AI approach that combines machine learning and rules for maximum, proactive detection with full transparency and explainability.

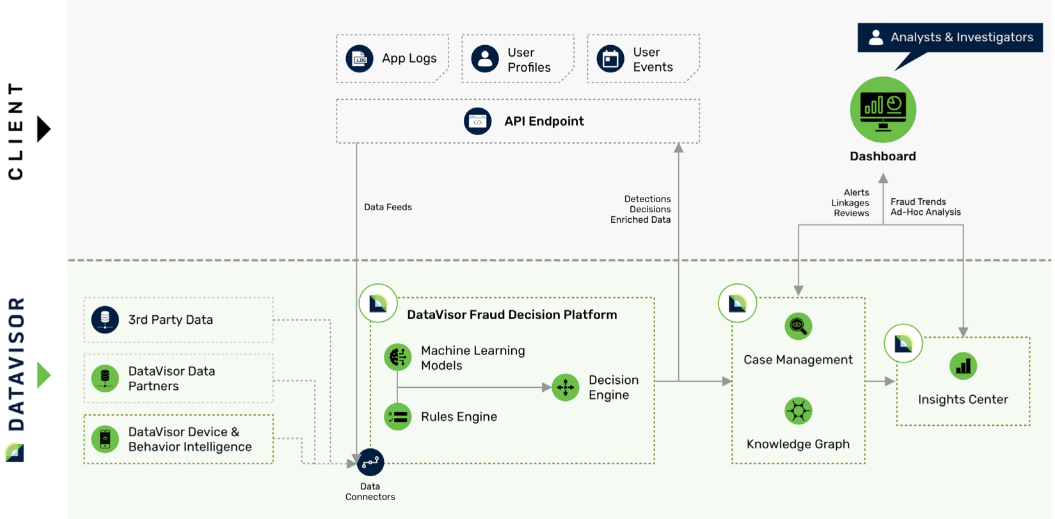
For Fraud Strategists

Devise new defense strategies, monitor fast-evolving fraud trends and run analysis on production data. DataVisor provides a 360° view of fraudsters and customer behavior to optimize strategies with guided analysis and validation steps.

For Operations Team

Boost operational efficiency by 5x-20x with auto decisions, bulk actions and smart investigation. DataVisor provides global, intelligent search and link analysis at multiple levels to uncover hidden patterns and empower contextual decisions.

Rapid and Flexible Integration



Results that Matter

$15 Million+

Annual Savings

Reduce financial losses and manual review costs with accurate detection.

5x -20x

Efficiency Uplift

Boost review and decision with link analysis, smart investigations, auto decisions and bulk actions.

1-2 Weeks

Fast Integration

Provide rapid and flexible integration with your systems and support real time and batch processing.

Conclusion

Just like these financial firms fought back, your team can tap into the power of a truly modern fraud detection strategy. Are you ready to experience the power of the most powerful fraud and risk management platform available today?

Schedule a Demo with Our Experts

ABOUT DATAVISOR

DataVisor is the world's leading AI-powered Fraud and Risk platform that delivers the best overall detection coverage in the industry. With an open SaaS platform that supports easy consolidation and enrichment of any data, DataVisor's solution scales infinitely, enabling organizations to act on fast-evolving fraud and money laundering activities as they happen in real-time. Its patented unsupervised machine learning technology, combined with its advanced device intelligence, powerful decision engine, and investigation tools provides a guaranteed performance lift from day one.

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