A Top Payment Network Relies on DataVisor's AI Solutions to Boost Transaction Fraud Detection

CLIENT

A leading global payment solutions provider handling more than $8 trillion 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 Enterprise ML —an 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Outdated fraud models were decaying upon deployment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

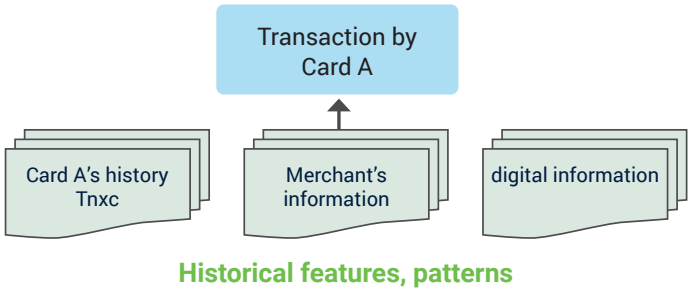
Unsupervised Machine Learning helped to fill in gaps in the client's existing fraud detection methods by analyzing all user behaviors and data without labels in real time and identifying suspicious patterns.This allowed fraud teams to detect attacks early and prevent them instead of doing damage control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

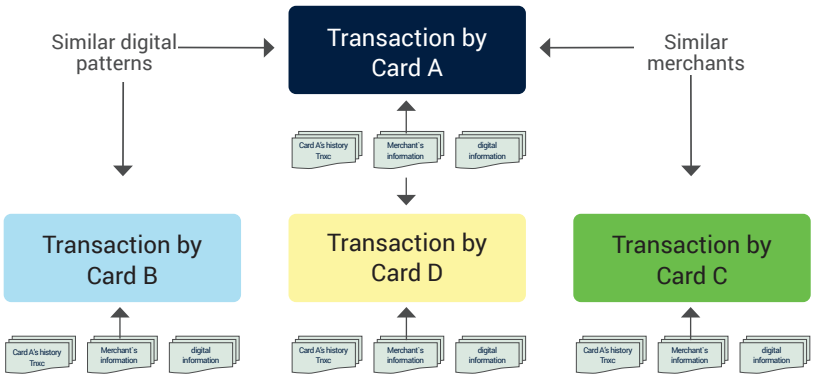
Traditional Rules or Supervised Learning

Decision based on the current event itself



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.

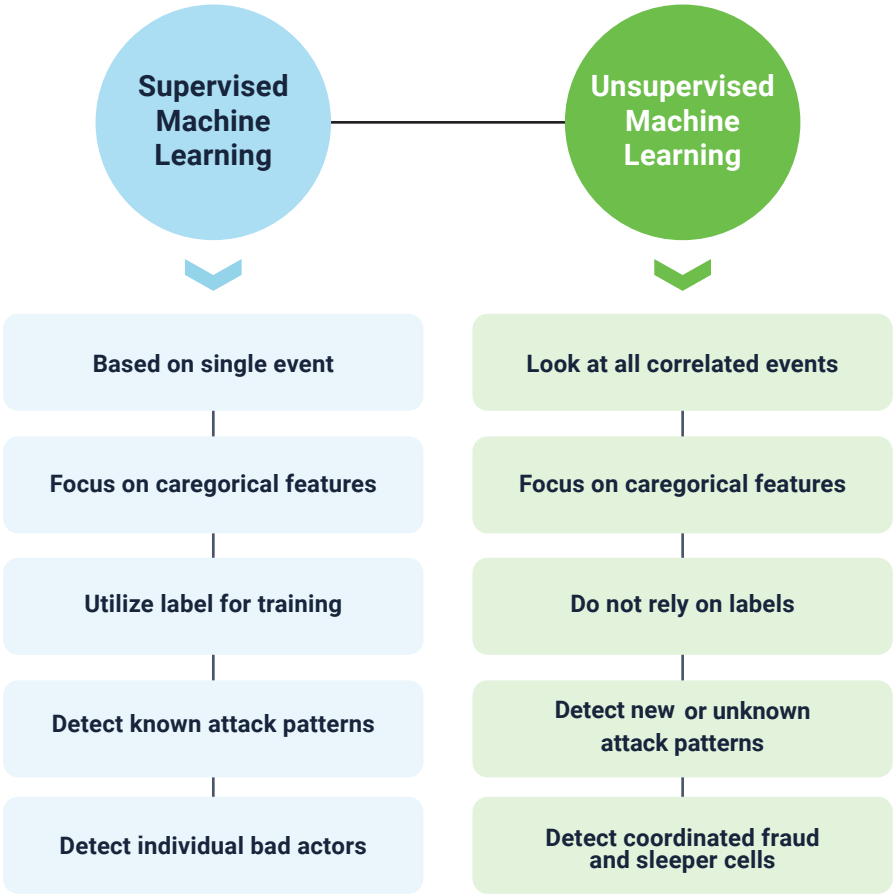
See the below chart: when the client was only using a supervised machine learning model, its model performance decayed significantly after 6 months. When the client added DataVisor's unsupervised machine learning solution to its supervised machine learning models, the fraud detection rate was still exceptional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



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

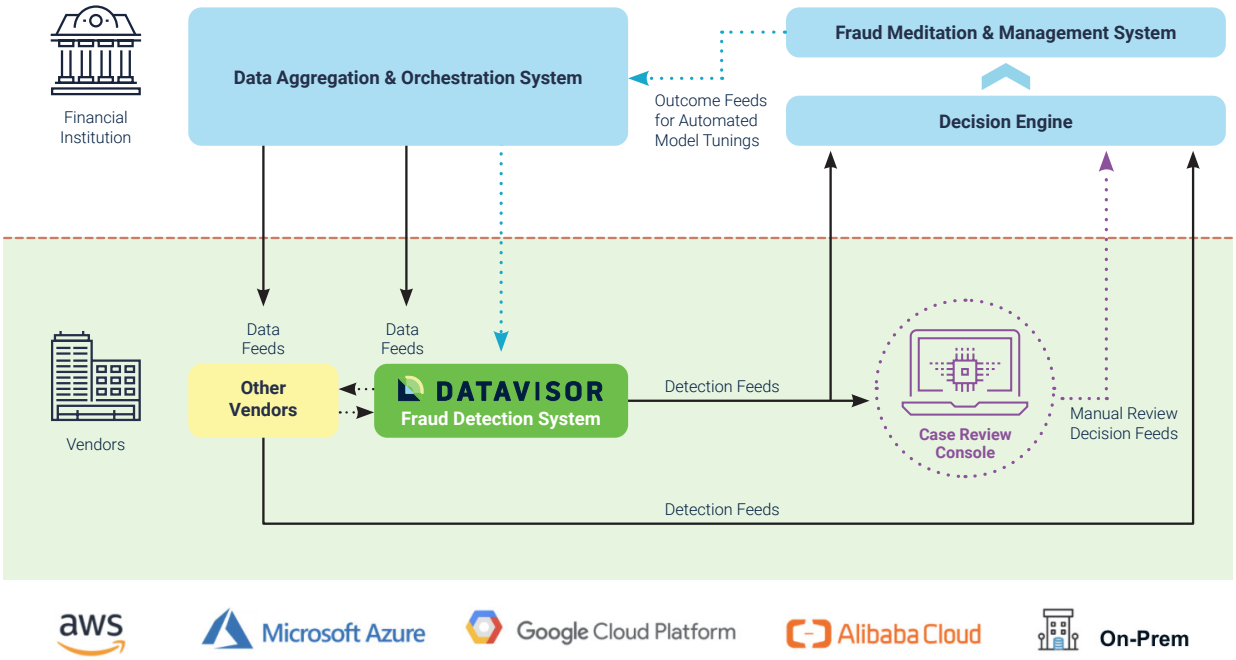
INTEGRATION

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



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

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