Top 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

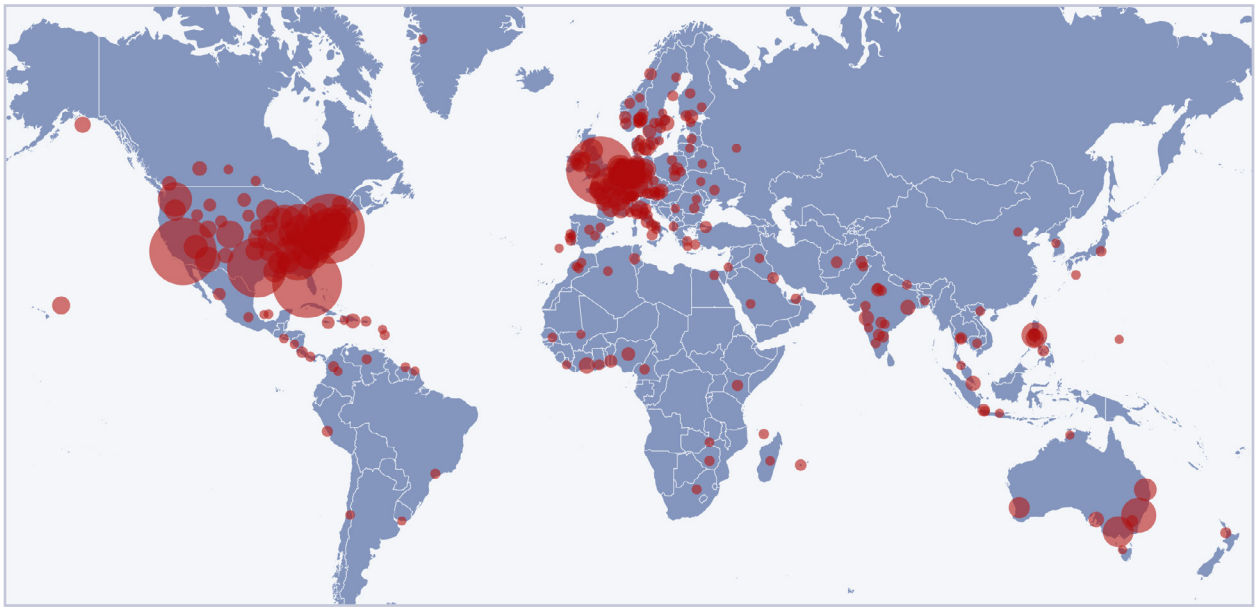
DataVisor recently partnered with a large global financial institution that services over 200 countries and has been in the financial services industry for over 100 years.

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, they were struggling with the increasing sophistication and scale of the attacks that were plaguing their defenses. Their 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 their 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.

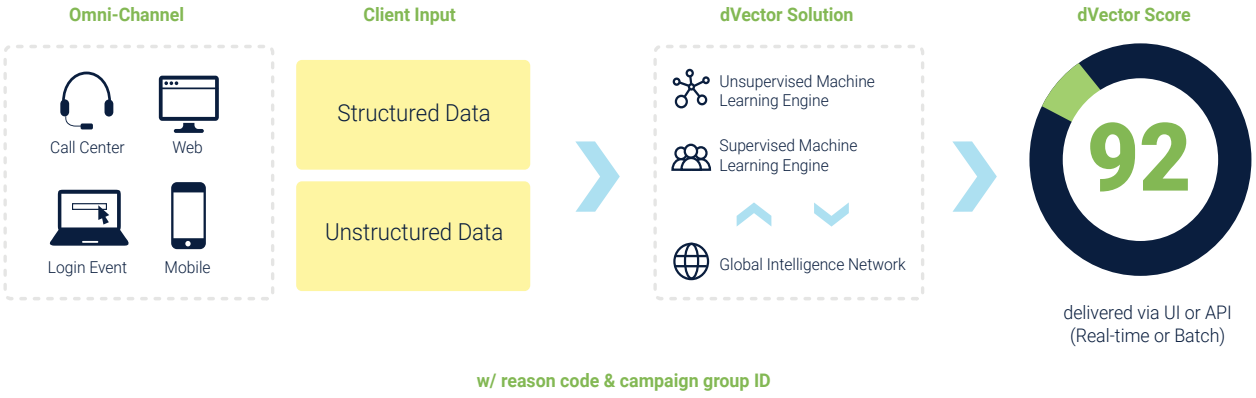
- **Patterns DataVisor detected**
  Similar patterns were discovered within the fraud ring–the sender's accounts were all registered from data center IP subnets, and the senders all used the same device IDs to transfer the same amount of currency ($440-$470) to the same locations, as shown in the table.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

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

How DataVisor Detection Works

DataVisor's dVector 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 dVector is architected to detect fraud attacks without any historic labels, large datasets, or training time. Drawing on a proprietary UML engine, dVector accelerates detection by analyzing all accounts and events simultaneously and identifying suspicious clusters of malicious activity—even at the point of account registration. Combined with supervised machine learning solutions, dVector excels at finding both known and unknown attacks.



To enhance detection efforts and enrich decision-making, DataVisor also leverages its Global Intelligence Network (GIN), which is comprised of anonymized non-PII data from over 4 billion protected accounts and 800 billion events across the globe. The GIN contains rich information on digital data such as IP address subnets, prefixes, proxies and data centers, user agent strings, device types and OS, email address domains, and more. Information from the GIN feeds into machine learning algorithms to further improve overall detection.

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