DATAVISOR

CASE STUDY: PROMOTION ABUSE, BUYER-SELLER COLLUSION

Food Delivery Unicorn Uses DataVisor For Fraud-Free Rapid Expansion

CLIENT

A global online food ordering and delivery platform with 100 million+ monthly active users and services in 20+ countries.

CHALLENGES

- The business was rapidly expanding, and encountering unique and evolving fraud problems in each new region, including promotion abuse and buyer-seller collusion.
- The client needed a modern infrastructure solution to support real-time decisioning and handle massive data volumes.
- Existing solutions could not keep pace with the fast-growing business, were incapable of capturing unknown fraud in new markets, and created friction for good customers.

SOLUTIONS

- Leveraged unsupervised machine learning to capture bot-registered malicious accounts early at the registration stage and uncover buyer-seller collusion.
- Provided a proactive solution to ensure the business could get immediate results without the need for historical data and labels, and deliver frictionless experience for good users.
- Provided real-time detection and supported high QPS with low latency.

RESULTS

300%
Detection uplift

60%
Fraudsters caught at registration

$6M
Annual savings in fraud losses in USD

CLIENT CHALLENGES

The client is a fast-growing food tech unicorn that is reshaping the search, order, and delivery experience for over 100 million online users. The business has been rapidly expanding into new countries over the past two years, and now provides services in 10,000+ cities worldwide.

While growth was skyrocketing, the company was continuing to lose millions of dollars annually to fraud, and the problems were worsening as the business scaled. Attackers were continuing to evolve their attacks to evade existing detection systems, and the business was confronted by unique and previously unseen attacks types every time they expanded into a new region.

New Risks for New Markets

To penetrate new markets and maintain an aggressive growth trajectory, the client needed to move rapidly. This agenda, however, was at odds with the reality that their fraud team needed time to create new rules and train new models to address the new risks in each new market. With the company not able to build adequate defenses, their fraud losses increased accordingly and their good customers were impacted by the false positives. It quickly became apparent that to support their expansions, they needed a solution that could provide immediate protection and deliver accurate detection on day one.

Promotion Abuse

The client's aggressive promotion campaigns attracted both customers and fraudsters, and the fraudsters were creating fake accounts at a massive scale to take advantage of the promotions— sign-on and referral bonuses, discounts, and more. They were using a combination of botnets and human farms to attack with high frequency at large scale, and this led to substantial financial losses for the business.

Buyer-Seller Collusion

Collusion among merchants, customers, and delivery riders was happening under the radar. "Customers" were making thousands of fake orders online, the "merchants" were pretending to prepare food, and the "riders" were acting as if they had delivered the food. However, while all of the parties received a vast number of subsidies from the platform, no actual food delivery ever took place.

Lack of Real-Time Capability

The client needed to monitor activities in real time to block fake users and orders immediately, without creating any friction for good users. However, their existing solutions were not able to process the vast data volumes in real time, which slowed their decision processes, and left their detection efforts unable to scale on pace with the growth of the business.

FRAUD PATTERNS DETECTED

Buyer-Seller Collusion

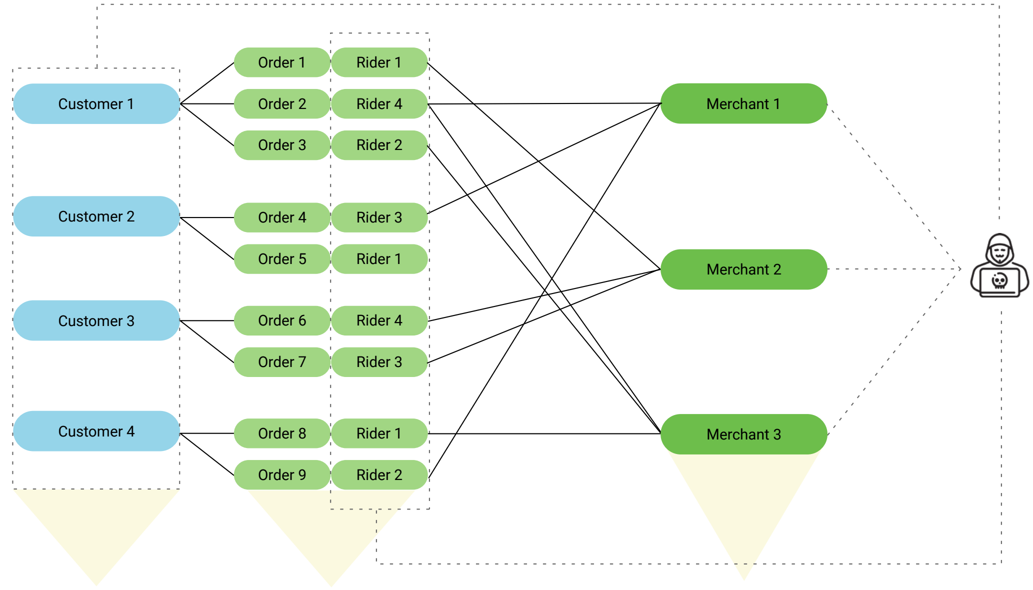
DataVisor uncovered an extensive collusion network containing over 50 customers, merchants, and riders, who conspired to place over 200 fake orders to fraudulently claim subsidies from the client.

Evasion Techniques

The fraud group used different delivery addresses for the orders. Most of the “customers” placed more than one order during lunchtime to mimic normal user behavior to evade simple detection rules.

Fraud Patterns DataVisor Detected

All of the “customers” shared similar email patterns, device models, and GPS coordinates. All the suspicious orders originated only from these “customers.” The intervals between order times and order deliveries were consistently between 5 and 10 minutes—a range not actually possible.



Mass-registered “customers” with different addresses but similar email patterns, device models, and GPS coordinates

5-10 minute intervals between food ordering and food delivery

Large numbers of fake orders pointing to only a few merchants, whose orders only came from those “customers”

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

DataVisor's best-in-class AI and machine learning solutions empowered the client to expand rapidly into new global markets with the confidence that they could successfully manage risk, neutralize fraud, and secure their platform. The DataVisor solutions adapted rapidly to new and unknown fraud in each new region, detected large-scale attacks in real time before any damage was done, and exposed under-the-radar, coordinated collusion.

The client chose DataVisor as their strategic partner for international expansion, knowing that DataVisor's proactive, scalable, and intelligent solutions provided exactly what they needed to meet their audacious goals.

Fast Onboarding and Accurate Detection for New Markets

The client rapidly onboarded DataVisor's solutions within two weeks, and the new systems immediately began to detect unknown and fast-evolving fraud with extremely low false positive rates. By eliminating their reliance on out-of-date, legacy rules written for previous regions, the client was able to accurately and proactively detect new fraud on day one in each new region, without impacting good users' legitimate activities. Instead of losing time to exploring and testing rules, collecting data and labels, and building and training models, DataVisor's scalable and adaptive solutions enabled the business to save more than $6M annually in fraud losses, and deliver superior experience to both new and existing customers.

Detecting Promotion Abuse at the Gateway

DataVisor's solutions preemptively detected the majority of promotion abusers at the registration stage, before they could launch any new attacks. Using unsupervised machine learning and big data analysis, the new solutions stopped highly damaging activities at scale, including malicious bot-scripted and human-operated attacks. In addition to providing significant detection uplift, DataVisor's solutions also delivered accurate results that enabled the business to consistently distinguish between good customers and fraudsters, ensuring optimal execution of promotion strategies.

Uncovering Hidden Collusion with Holistic Data Analysis

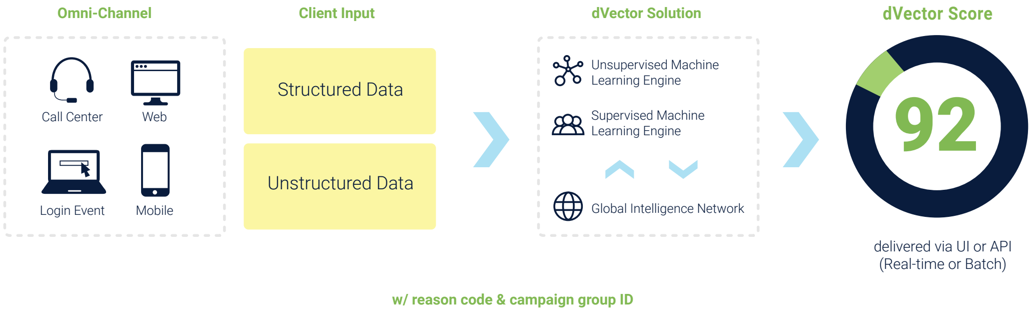
DataVisor's solutions discovered buyer-seller collusion by holistically analyzing activities, accounts, addresses, digital fingerprints, and more, to expose suspicious patterns and coordinated activities. While the malicious merchants, customers, and riders stealthy hid their behaviors and kept changing patterns, they nonetheless left subtle traces, and DataVisor's unsupervised machine learning technologies were able to connect the dots and expose the buyer-seller collusion.

Real-Time Detection and Big Data Capability

The client benefited greatly from DataVisor's modern infrastructure, which can handle massive data volumes and support real-time detection with high QPS. With DataVisor's highly scalable solution, the client was able to expand rapidly while defeating fraud, exposing collusion, and stopping promotion abuse in real time.

HOW DATAVISOR DVECTOR WORKS

DataVisor's dVector provides proactive fraud protection for clients. While conventional rules or supervised machine learning solutions require "pre-knowledge" of how attacks work to be effective, DataVisor's systems are architected to detect fraud attacks without requiring any historical labels, large datasets, or training time. Drawing on a proprietary unsupervised machine learning engine, DataVisor's solutions accelerate detection by analyzing all accounts and events simultaneously and identifying suspicious clusters of malicious activity—even at the point of account registration. In this way, DataVisor solutions can expose even new and unknown attack types.



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 4.2 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.

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
- Mobile & Gaming
- E-Commerce
- Telecom & Travel
- Social Platform
- 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