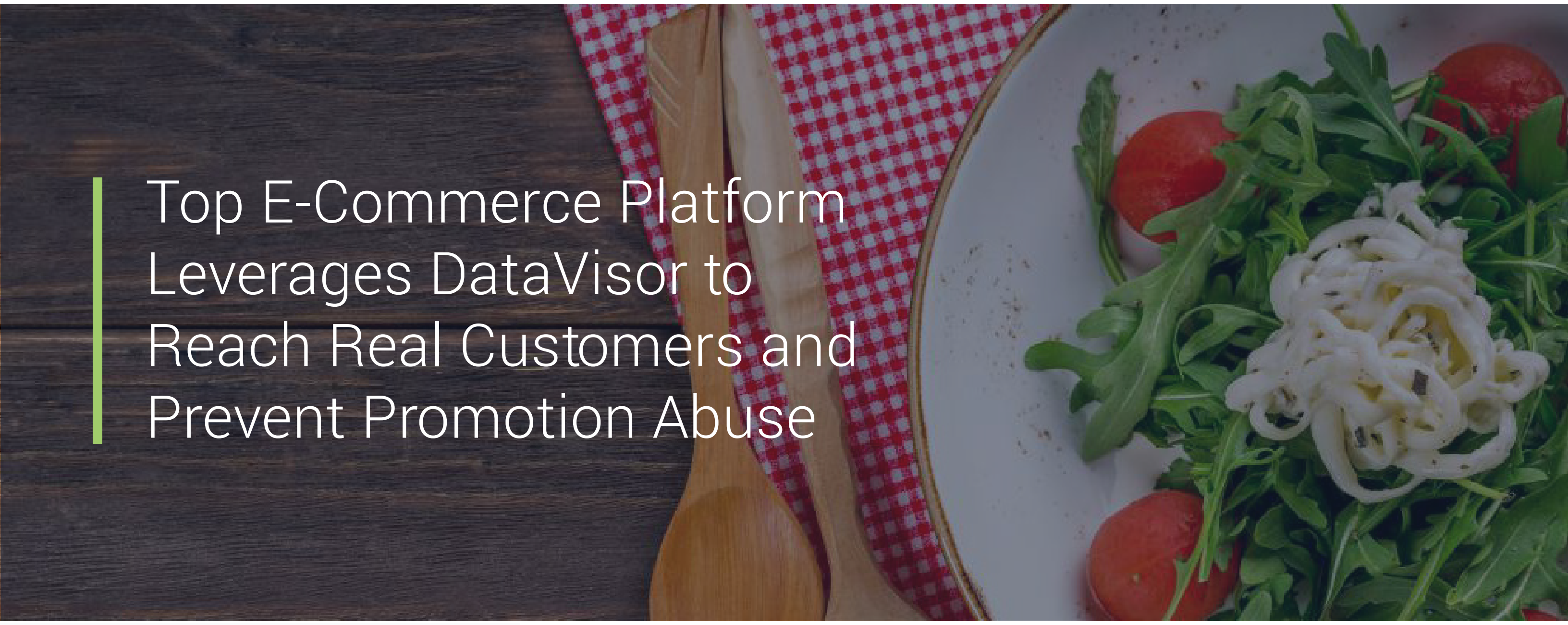


Top E-Commerce Platform Leverages DataVisor to Reach Real Customers and Prevent Promotion Abuse

Client Challenges

To compete in new markets, the client would launch large promotional campaigns, but fraudsters took advantage of the promotions by making large-scale fake orders, and merchants colluded with buyers to receive promotional subsidies. The client needed to better target real customers and simultaneously block fraud attacks.

DataVisor Results:

99.5%
detection accuracy

23%
detection uplift

90%
of fraudulent accounts detected in real time, at the point of registration

About the Client

DataVisor partnered with a large e-commerce platform in Asia that specializes in food delivery services and has over 50 million monthly active users. As they grow to serve new regions and extend their services to millions of merchants and consumers, the platform's mission is to digitize the catering and retail industry.

Client Challenges

The platform's market-entry strategies were fast, agile and aggressive, but their fraud prevention solutions were slow to adapt to new markets, unable to keep pace with growth, and ill-equipped to capture quickly-evolving attack patterns.

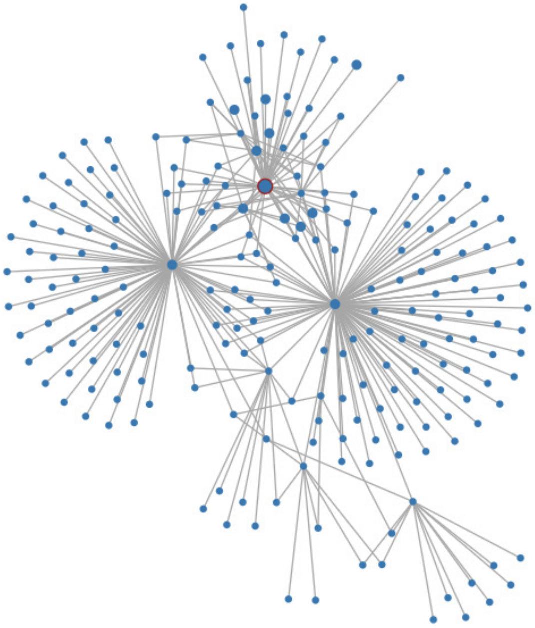
The platform was struggling with customers abusing its sign-up bonus offer to acquire more users. Newly registered users receive a discount towards their first purchase. Fraudsters would generate fake accounts to take advantage of the bonus and place orders for customers at a lower price while taking a cut. Another way fraudsters game this system involves merchants receiving promo subsidies from the platform by having fake users place orders on lower cost items or simply not shipping these fake orders.

To catch these promotion abuses, the platform deployed a rules-based system to detect fake account registration. Unfortunately, the rules decayed quickly due to constantly evolving attacks that rendered the rules outdated. Promo abuse was costing the growing platform millions of dollars of its marketing budget every year. The platform was in urgent need of a solution that could not only keep up with the latest techniques in promotion abuse, but also scale as the platform grows to new regions and provides new services.

How DataVisor Helped

DataVisor's solution rapidly and accurately identified all fraudulent activity, no matter how often or how quickly fraudsters changed their patterns, by seamlessly adapting to new markets starting on day one.

DataVisor's fraud protection solution was implemented to detect suspicious account activity including fake account registration. With its proprietary unsupervised machine learning (UML technology, DataVisor's systers were able to capture 90% of fraudulent accounts early at the point of registration, and detect 23% more fake accounts than what the internal teamwas previous detecting, at 99.5% accuracy. These actions blocked million dollars worth of fraudulent transactions in real-time.



DataVisor captures evolving frauds by finding links among accounts, behavioral data, metadata, digital footprints, and more.

Fraud Rings Detected

Mass Fake Orders

DataVisor identified a massive group of over 130K fraudulent accounts placing orders to over 30K merchants.

- **Evasion techniques**
  The fraud group utilized device emulators to create unique device IDs for all of the accounts. The accounts all have different GPS coordinates and IP addresses as well.

- **Patterns DataVisor detected**
  All of the orders are under $5, and all of the accounts are registered using a set of devices with hundreds of accounts tied to the same IMEI number. The fake accounts all share the same older OS version (Android Kitkat 4.4.2).

Merchant Subsidy Abuse

DataVisor uncovered a case where a single merchant used over 50 fake accounts to receive the promotion subsidy.

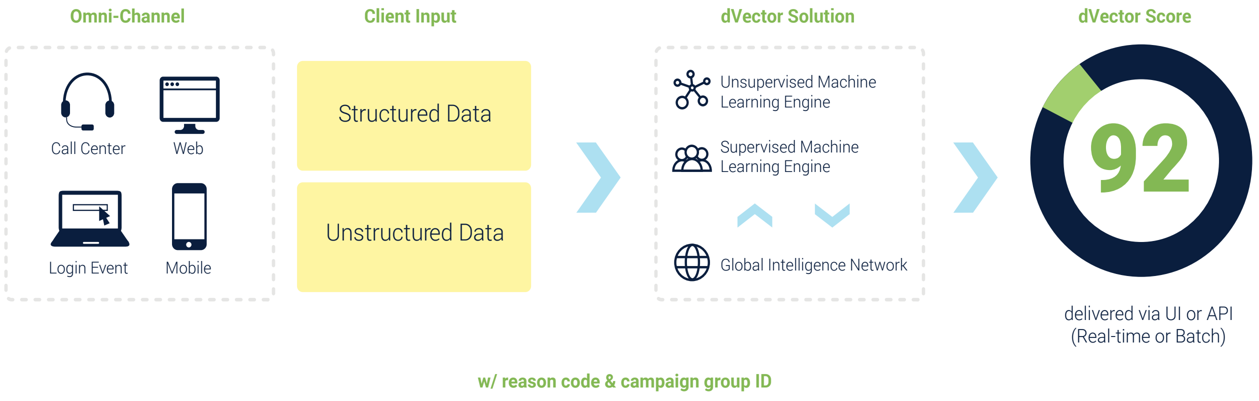
- **Evasion techniques**
  The fraud group used different delivery addresses for the orders. Most of the accounts placed more than one order to mimic normal user behavior to evade simple detection rules.

- **Patterns DataVisor detected**
  The merchants only orders came from these suspicious accounts. All of the accounts used iOS devices and had the same user agent strings, which is extremely rare in the global distribution of user agent strings. While all of the orders have different delivery addresses, all of the accounts point to the same GPS coordinates.

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, 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.


Omni-Channel
Call Center
Web
Login Event
Mobile
Client Input
Structured Data
Unstructured Data
dVector Solution
Unsupervised Machine Learning Engine
Supervised Machine Learning Engine
Global Intelligence Network
dVector Score
92
delivered via UI or API (Real-time or Batch)
w/ reason code & campaign group ID

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