DATAVISOR

CASE STUDY: SHIPPING FRAUD, FAKE ACCOUNTS

# DataVisor Empowers Top Delivery Company to Detect Shipping Fraud Fast and Early

**CLIENT**

Top delivery services company  processing over 6 billion packages annually.

**CHALLENGE**

Fraudsters were committing identity theft and using the stolen information to mass register fraudulent new accounts. They were then using these fake accounts to reroute packages, scam good users with malicious emails, and track criminal shipments.

**SOLUTIONS**

- Proactively detected fraudulent reroute and hold requests; avoided financial loss resulting from stolen packages.
- Identified and blocked mass-registered fake accounts at the point of signup, before any damage could occur.
- Improved operational efficiency with automatic blocking and quarantine functions, and enabled faster manual review and bulk decisioning.

**RESULTS**

**60%**

**Detection uplift**

**40%**

**Increase in review efficiency using holistic analysis**

**>$4M**

**Fraud loss savings in USD**

## CLIENT CHALLENGES

DataVisor recently partnered with a top delivery services company to detect shipping-related fraud and fake account openings to ensure trust and safety for their digital platform.

The client was experiencing an increase in malicious users stealing good customer credentials to register fake online accounts at large scale. These fake accounts were being used to reship packages to different locations, issue package holds for delayed pick-ups, and spam good users with malicious advertising. Fraudsters were additionally taking advantage of the client's online portal to track thousands of fraudulent shipping actions. The massive volume of fake account registrations and spamming activities were causing financial and reputational damage for the client, and negatively impacting customer experience for their good customers.

The client needed an advanced fraud solution to detect the sophisticated attacks that were bypassing their existing prevention systems. They also needed to capture fraudsters as early as possible, to minimize potential losses starting on day one. They needed to achieve this at scale. They were impressed by DataVisor's advanced data analysis capabilities, and the ability to draw insights from large datasets in different formats and structures, without the need for historical labels. They chose DataVisor's solution—powered by proprietary unsupervised machine learning—for its fast and comprehensive protection, and its ability to stop fraud before damage happens.

## CLIENT SUCCESS WITH DATAVISOR'S DVECTOR

The client began using DataVisor's dVector solution—an advanced AI-powered solution leveraging advanced unsupervised machine learning algorithms and vast global intelligence—to expose shipping fraud and uncover fake accounts at the time of registration. DataVisor's solution proactively protected the client from sophisticated new and emerging fraud types, no matter how fast fraudsters changed their attack patterns and technologies. The client leveraged DataVisor's advanced machine learning technologies, holistic data analysis, and advanced contextual detection capabilities to preserve trust and safety on their platform, and prevent fraudsters from hijacking their services for criminal purposes.

### Holistic Data Analysis

DataVisor's dVector solution found hidden connections between seemingly isolated incidents, exposed new attack patterns, and unmasked highly sophisticated fraud attacks. dVector's advanced data analysis capabilities produced actionable insights from large volumes of data and took a holistic approach to reviewing and analyzing a wide variety of event types, digital fingerprints and profile information related to accounts, shipments, and deliveries. By performing contextual detection and pattern analysis, DataVisor's machine learning solutions captured 60% more fraud beyond what the existing systems were able to detect— saving the client more than $4 million (USD) in a single year.

### Early Detection

By drawing on the power of DataVisor's unsupervised machine learning technology, the client was able to detect a significant majority of malicious accounts at the point of registration, with the remainder caught while trying to perform a first attacking action. On average, dVector was able to catch fraudulent accounts approximately 30 days earlier when compared to known client labels in a cross-validated training set. Unlike other anti-fraud services which focus on behavior monitoring at the attack event level, DataVisor's emphasis on early detection means that these malicious entities are neutralized before they can cause any damage.

### Accelerated Review Efficiency

The client's fraud analyst team was able to significantly improve efficiency with automated actions and bulk decisioning. Because dVector was able to discover clusters of linked accounts and group the results, fraud analysts needed only to review a handful of sample cases before confidently making bulk decisions applicable to all cases within the same fraud ring. Using this approach, the client experienced a 40% increase in review efficiency.

## FRAUD PATTERNS AND VULNERABILITIES DETECTED

By taking a holistic approach to analyzing user profiles, digital fingerprints, registration and tracking events, and package shipping and rerouting activities, dVector enabled the client to detect the following fraud patterns and vulnerabilities:

### ▶ Online Shipping Portal Abuse

The online shipping portal is typically used when an original order has an error; for example, when a wrong item is included in the shipment, or the destination address is incorrect. However, dVector revealed that malicious users could leverage stolen customer information to create fake online accounts that could be used to modify these orders to include higher-value items, or to reship them to different destinations.

### ▶ Call Service Fraud

Any order that passed a fraud screening phase could still be modified via phone calls to customer service. While this service was useful for customers, it also represented a vulnerability that could be exploited by fraudsters, who could call in, impersonate a good customer, and make changes to accounts, including shipping details, credit card information, and more.

### Tracking Malicious Delivery

Shipping tracker services were used by good customers to keep track of their legitimate orders. However, dVector revealed that fraudsters were also using these services to keep track of hundreds, even thousands, of fraudulent rerouting and shipping actions. By analyzing the tracking events and digital signals, dVector was able to capture coordinated groups of fraudulent users who were taking advantage of the online platform to manage their illicit activities.

### Ad Scam

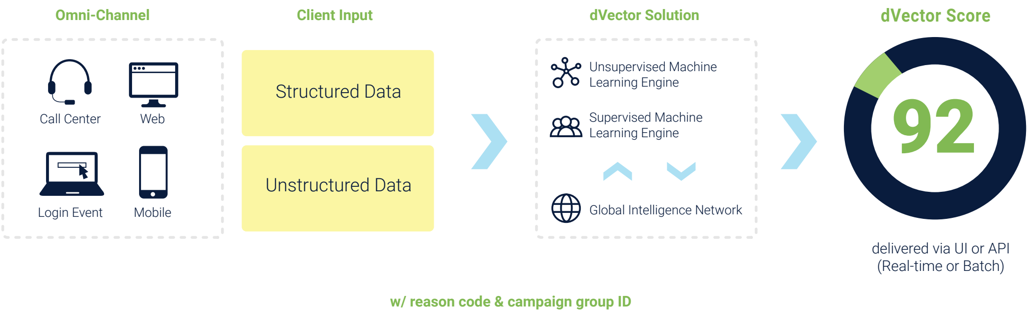
Fraudsters were registering large numbers of online accounts to send enormous quantities of scam mails and packages. dVector quickly found large clusters of mass registered users, which, after short incubation periods, were shipping scam mails at high frequency to harass victims, and deceptively entice them to fall prey to advertising frauds.

dVector detected one such campaign that contained over 200 users, all of whom shared the following properties:

| | |
|---|---|
| **Email Address** | ampenergyXXX@XYZ.com |
| **Registration Time** | 2018-08-22 to 2018-09-20 |
| **IP Addresses** | All shared in the 105.112.26.xxx or 105.112.28.xxx block. 43% were associated with Nigerian providers, and 7% came from known data-centers. Based on Datavisor's Global Intelligence Network, these IP CIDR blocks were "associated" with known bad users from other clients. |
| **Phone Numbers** | All from (069) 037-XXXX, (700) 140-XXXX, and (800) 461-XXXX. Note that area codes (069) does not exist. (700) is reserved for corporate use only or for voice over IP networks (VoIP). |
| **Package Weights** | Either 1lb or 0.5lbs |
| **Shipping Address** | XX Street, Houston, Texas. Some were rerouted to other locations. |

## HOW DVECTOR WORKS

dVector provides proactive fraud protection for clients. While conventional rules or model-based 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.


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

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