Large Mobile C2C Marketplace Uses DataVisor to Create a Trustworthy and Safe Platform

Client Challenges

A large marketplace's existing rules-based detection system was not able to capture sophisticated and constantly evolving fraud attacks. The business was incurring significant operational costs from having to review large volumes of false positive alerts generated by the static rules.

DataVisor Results

<2 weeks
Solution integration time

10x
Increase in detection as compared with existing rules

20x
Improvement in manual review efficiency

90%
Of fake listings detected right after they are posted

60%
Of spammers flagged within 2 days of sign-up

About the Client

DataVisor partnered with a large mobile customer-to-customer marketplace to protect against various fraud and abuse activities such as fake listings, spam, and account takeovers. As the Marketplace expanded its service to more regions and customer segments, it was struggling to maintain a safe and trusted platform where consumers could trade goods and enjoy a seamless customer experience.

Client Challenges

The rapid growth of the marketplace attracted not only more users, but more fraudsters as well. Fake listings, spam, and account takeovers were becoming a growing problem, derailing the marketplace's efforts to maintain a safe and trusted platform and a seamless customer experience. Operational costs were increasing at unsustainable rates and the high level of false positive alerts generated by existing systems were driving away good users.

The marketplace did have an existing rules-based fraud detection system in place. However, those rules were not able to capture increasingly sophisticated and coordinated fraud and abuse attacks. At a certain point the platform suffered a massive spike of fake listings and spam, which led to a drop in active users. At the same time, there were significant operational costs to review the high volume of false positive alerts generated by the static rules. The Trust & Safety team was overwhelmed with a backlog of cases to review.

The marketplace was in urgent need of a solution that could not only keep up with the latest techniques in fraud and abuse detection but also produce actionable results with high accuracy and low false positives, saving time and cost spent on manual review.

Fraud Rings Detected

Coordinated Listing Spam

A fraud ring identified by DataVisor comprised over 1,700 accounts that posted used cars for sale with abnormally low prices to attract buyers first and later spam them with in-app messages.

- **Evasion techniques**
  Fraudsters bypassed existing rules-based detection by using legitimate-seeming email addresses and devices, but were still detected by DataVisor through identification of common patterns in digital fingerprints and activities.

- **Patterns detected**
  All of the email addresses on the profiles used "first name + last name + year" as the email prefix and yahoo.com as the email provider. In-app messages were sent from the same IP subnet, which further confirmed that these listings were from a group of coordinated fraudsters.

Large-Scale ATO Attacks Followed by Scams

DataVisor detected 5,000+ compromised accounts from a single country that were used to post suspicious luxury watch listings. All of the affected accounts were registered pre-2015 and had good buyer review ratings, making them seem legitimate.

- **Evasion techniques**
  The attackers were using legitimate-seeming ISP IPs from the same country and were not active immediately after ATOs—they were incubating the accounts before posting the scam content.

- **Patterns detected**
  All 5,000+ accounts had 10 to 20 login events within a 3-minute window on the same day, where the time interval between consecutive logins was always the same. In addition, those accounts each made at least one luxury watch listing on the next day, with a particular brand mentioned in each listing description.

The DataVisor Solution

DataVisor's fraud detection platform was customized and integrated within two weeks. In addition to focusing on fixing known issues the marketplace was facing, DataVisor was able to perform an end-to-end risk assessment. Using its proprietary unsupervised machine learning (UML) technology as part of its fraud detection platform, DataVisor detected unknown fraud attacks. By examining all activity holistically across all users instead of evaluating user events one-by-one as a traditional system would, DataVisor uncovered hidden patterns of fraud and abuse common to fraudsters. Having identified the patterns, DataVisor's systems flagged malicious accounts earlier and blocked them before damage happened.

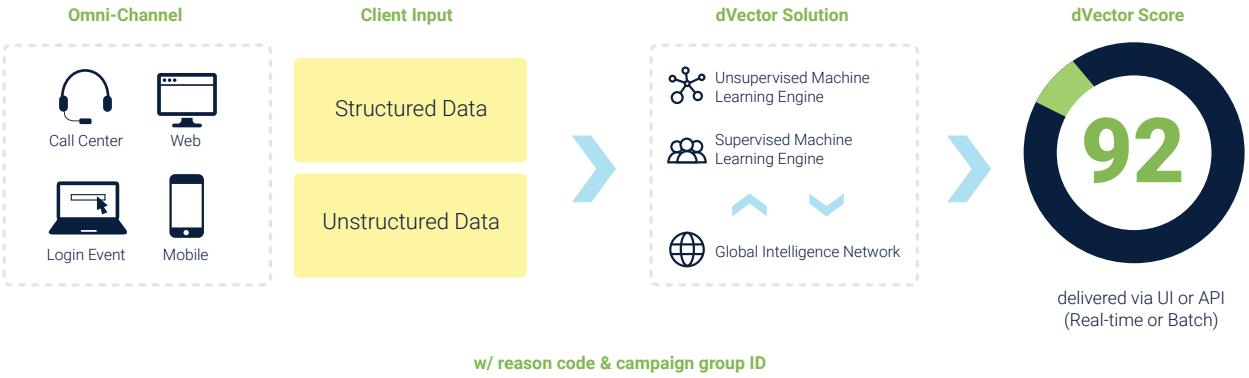
Additionally, it addressed the source of these issues —mass fraudulent account registrations and account takeovers. DataVisor's apporach increased detection by 10x compared to the existing rules-based system.

The Trust & Safety team maintained its headcount even as the marketplace expanded rapidly. With the high accuracy of DataVisor's solution, the team was able to act faster to prevent fraud and abuse activities. Instead of spending time on false positive alerts, they focused on truly fraudulent cases and adjusted strategy accordingly, maintaining a safe and trustworthy platform for its users.

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.



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