Top Airline Uses DataVisor to Defeat Ticketing Fraud, ATO, and Loyalty Program Fraud

CLIENT

- A leading airline in Asia with 160+ routes globally

CHALLENGES

- **Bot-Scripted Ticketing Fraud**
  Fraudsters were using scripted bots to purchase tickets in bulk and later resell or cancel the tickets. They fraudulently claimed seats and manipulated prices, causing revenue loss and negative customer experiences.

- **Account Takeover and Loyalty Program Fraud**
  Fraudsters were using sophisticated techniques to compromise good users' accounts to redeem loyalty points on loyalty program marketplaces, and use saved credit cards to purchase airline tickets.

SOLUTIONS

- **Leveraged DataVisor's dVector–An Advanced Machine Learning Solution**
  Proactively captured fast-evolving bot attacks by taking a holistic view to analyze orders in real time. Analyzed web session logs, cross-account linkages, digital fingerprints, profile info, and behaviors to surface even the most stealthy fraud patterns.

- **Leveraged DataVisor's dEdge–A Fraud Prevention SDK for Mobile and Web**
  Collected real-time intelligence from mobile apps and web browsers to uncover malicious activities targeting mobile devices and web pages. Generated accurate risk signals, device IDs, and device scores for enhanced fraud prevention.

RESULTS

additional fraud captured

detection accuracy

113K

hours saved per year (seat occupancy time)

FRAUD PATTERNS DETECTED

Bot-Scripted Ticket Reservation Fraud Patterns

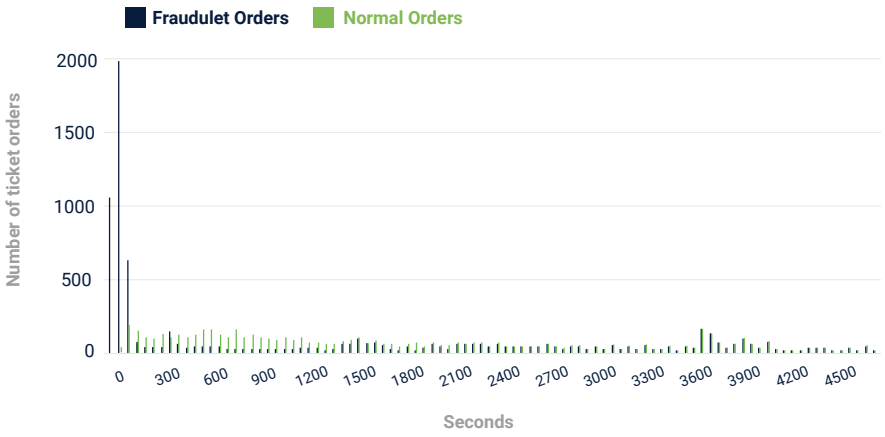
Passenger names were randomly generated, though the contact phone numbers were from the same area code. None of the fraudulent orders in this example had a web referrer, indicating that the bots were programmed to visit the airline booking webpage directly. These were sophisticated attacks. The fraudsters had detailed knowledge of the airline website's defenses, and they were able to specifically craft their bots to evade detection.

Same flight number	Randomly generated names	Phone numbers with same area code	Short session duration	Similar time interval	Same IP subnets	Direct visit without referral link
FLIGHT NUMBER	PASSENGER NAME	CONTACT PHONE	SESSION LENGTH (SEC)	AVERAGE TIME INTERVAL (SEC)	IP ADDRESS	REFERRER URL
BH283****	Destiny Compton	(235) 408-****	58	3.24	113.62.18.***	null
BH283****	Quincy Luna	(235) 408-****	52	2.87	113.62.18.***	null
BH283****	Moses Snow	(235) 408-****	63	3.06	113.62.18.***	null
BH283****	Cooper Zamora	(235) 408-****	57	2.95	113.62.18.***	null
BH283****	Cannon Lozano	(235) 408-****	48	3.13	113.62.18.***	null
BH283****	Sony Ramen	(235) 408-****	61	2.67	113.62.18.***	null
BH283****	White Jack	(235) 408-****	55	3.09	113.62.18.***	null

Fraudulent ticket reservations made by scripted bots.

How DataVisor Detected the Patterns

Even though fraudsters obfuscated malicious bot activity to try and evade detection, there were still behavioral patterns that set them apart from normal users. For example, all of those fraudulent orders went through the same sequences of webpages to search and book flights. The time it took the bots to fill out the booking information varied, but that distribution was significantly different from those of legitimate users. In this example, DataVisor's solutions detected that the fraudulent users consistently had very short session durations (often less than 100 seconds), whereas normal, manual orders were at least twice that duration, and could be as high as 5000 seconds.

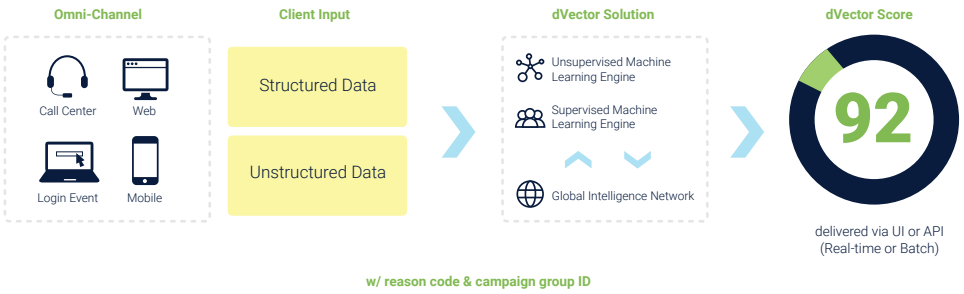


The distribution of web session duration from fraudulent orders is much shorter in duration than normal orders.

HOW DATAVISOR DETECTION WORKS

dVector–An Advanced Machine Learning Solution

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's systems are architected to detect fraud attacks without any historic labels, large datasets, or training time. Drawing on a proprietary UML engine, DataVisor's 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, DataVisor's dVector excels at finding both known and unknown attacks.



dEdge–A Fraud Prevention SDK For Mobile and Web

DataVisor's dEdge provides organizations with a transformational opportunity to move detection to a much earlier point along the timeline of a fraud attack—to the device and browser level. dEdge collects extensive device intelligence in real time from mobile applications and web pages, and delivers accurate signals, device IDs, and risk scores. When used in combination with DataVisor's dVector, dEdge empowers organizations to uncover known and unknown threats and attacks early, and to take action with confidence.

Global Intelligence Network

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.

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