DATAVISOR

CASE STUDY: PROMOTION ABUSE

Global Travel Platform Uses DataVisor to Defeat Promo Abuse and Fraud Attacks

CLIENT

A global travel platform connecting users to hotels, flights, car rentals, tours, airport transfers, and more, operating in over 200 countries and territories.

CHALLENGES

- Fraudsters were abusing promotion codes, making massive numbers of reservations, then reselling those reservations at a profit (especially in Asia), causing enormous fraud losses for both the client and its affiliates and partners.
- The client was forced to limit market-entry promotions due to hard-to-control promotion abuse, and this hampered new market growth and competitiveness.
- Financial losses resulting from promotion abuse were damaging partner relationships.

SOLUTIONS

- Reduced fraud losses, restored promotional campaigns, and enhanced partner relationships by boosting detection and stopping fraud before any damage occurred.
- Provided advanced case management to deliver deeper insights and enhanced operational efficiency with automatic actions, linkage analysis, and bulk decisions.
- Provided comprehensive defenses by using unsupervised machine learning, deep learning, and natural language processing.

RESULTS

40%
detection uplift

93%
detection precision

70%
of promotion abuse blocked early

$20M
savings in fraud losses

CLIENT CHALLENGES

The client is a global travel fare aggregator and travel metasearch engine providing lodging, flights, car rentals, airport transfer reservation services, and more, for many million monthly active users. The client supports over 40 languages and has a presence in more than 200 countries and territories.

When the client expanded their business in Asia, they launched large-scale promotion campaigns to compete with local providers and acquire new customers. However, the promotions attracted not only good customers but also fraudsters.

Financial Loss Due To Promotion Abuse

Fraudsters took advantage of promo codes, discounts, and bonuses to make massive numbers of fraudulent hotel reservations, and then later resold these reservations at inflated prices to make illicit profits. To do this, they leveraged sophisticated tools–botnets, VPNs, device emulators, cloud services, and more–to not only automate and scale attacks but also obfuscate their actions and hide their footprints.

The client's existing rules-based detection solutions were incapable of capturing these fast-evolving and stealthy attack patterns. Their fraud team could only update rules after attacks happened, and, by that time, it was already too late. Even with the most up-to-date rules, they continued to let damaging attacks slip through.

Slow Business Growth

Massive-scale promotion abuse not only caused significant financial losses for the client, but also slowed down their market growth in new regions. Since the majority of promotions went to fraudsters, real customers did not benefit from the promotions. In a competitive market where other travel platforms frequently launched promotions, the client's under-performing promotion campaigns were holding back their customer acquisition and retention.

Negatively Impacted Partner Relationships

A large number of their hotel partners were also suffering from promotion abuse losses when running promotions through the client's platform. The lack of effective fraud detection was damaging the client's partner relationships and reputation, subverting growth and competitiveness in the new market.

FRAUD PATTERNS DETECTED

DataVisor uncovered an extensive group of 230 malicious customer accounts that leveraged Christmas promotion codes to make over 400 hotel reservations in 2 hours, with the intention of reselling them to real customers.

DataVisor Detected A Group of 230+ Promotion Abusers

	different emails but with similar naming patterns	different IPs but within the same IP subnets		hotels in New York	Christmas promo code		similar check-in date	reservation in 2 hours
Transaction ID	Email	IP Address	Hotel Reserved	Hotel Location	Promo Code	Reward Amount	Check-in Date	Reservation Time
1235	dnnzna***224@dr.com	212.25.***.8	Hilton	New York	Special20	$45	12/30/20	13:01 12/10/18
1256	dnnzna***234@gmail.com	212.25.***.92	Westin	New York	Special20	$70	12/30/20	13:04 12/10/18
1346	mlxbc***09@workemail.com	212.25.***.121	Marriott	New York	Special20	$52	12/29/20	13:06 12/10/18
1438	dnnzna***284@dr.com	212.25.***.66	IHG	New York	Special20	$50	12/30/20	13:08 12/10/18
2594	mlxde***05@workemail.com	177.24.***.2	Ritz Carlton	New York	Special20	$80	12/31/20	13:56 12/10/18
3744	dnnzna***244@graduate.org	177.24.***.75	Four Seasons	New York	Special20	$60	12/30/20	13:58 12/10/18
5809	mlxfg***11@webname.com	177.24.***.154	Waldorf	New York	Special20	$75	12/29/20	14/02 12/10/18
6124	mlxhi***45@gmail.com	177.24.***.91	Westin	New York	Special20	$70	12/31/20	14.08 12/10/18
...	...	...	...	...	...	...	...	...

* Data shown above is for illustration purposes only and does not pertain to any of DataVisor's clients

Evasion Techniques

The group of fraudsters used different IP addresses and email addresses from various domains to make bookings at different hotels. All the transactions appeared legitimate when reviewed individually.

Patterns DataVisor Detected

Email Naming Patterns

DataVisor's deep learning and natural language processing models detected that the account emails shared similar naming patterns even though the domains and prefixes were different.

IP Subnets

Though fraudsters used different IP addresses to obfuscate their traces, DataVisor's unsupervised machine learning algorithms detected that all the IP addresses were from the same IP subnets.

Behaviors

By taking a holistic approach, DataVisor's solutions revealed that fraudsters were using Christmas promotion codes to book hotels in New York in bulk, all with check-in dates right around New Year's Eve.

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

Fast Integration and Immediate Protection For New Markets

The client integrated DataVisor's solutions within two weeks, and the new systems began to detect both known and unknown promotion abuse immediately. Especially for the recently-entered regions where the client's existing detection systems had low coverage, DataVisor's solutions boosted detection by 40% and significantly reduced false positive rates. The adaptive and accurate solutions helped the client save $20 million in fraud losses and enabled them to launch new large-scale promotions with the confidence that only real customers would receive benefits from the platform and its partners.

Real-Time and Early Detection For Ever-Evolving Fraud Patterns

After implementing DataVisor's solutions in production, the client was able to detect 70% of promotion abusers early, before any damage could occur. DataVisor's solutions leveraged unsupervised machine learning, deep learning, and big data analysis to proactively stop highly damaging activities at scale, even for new fraud patterns that had not been seen before. The rapid and real-time detection helped the client stay ahead of any new fraud in new regions–usually one-to-three months earlier than existing rules engine and supervised machine learning models were capable of.

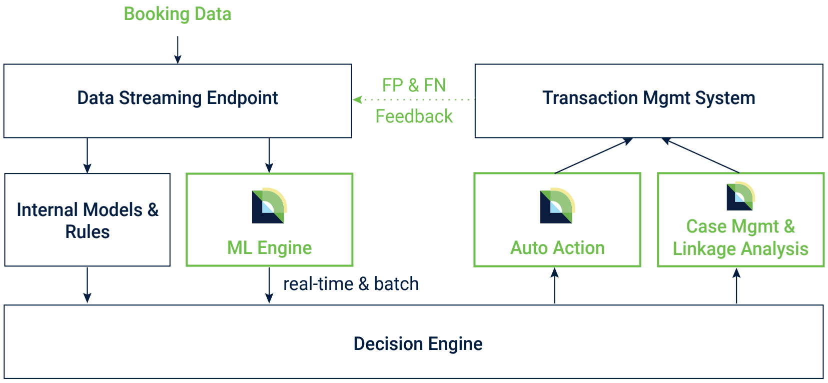
Auto Actions, Linkage Analysis, and Boosted Operational Efficiency

The client's fraud team significantly improved their efficiency and reduced overhead with DataVisor's automatic action capability and linkage analysis dashboard. They streamlined their workflow by automatically blocking highly risky accounts and activities based on DataVisor scores. For less-suspicious accounts that required manual review, the client used DataVisor's linkage analysis dashboard to gain deeper insights and expedite review, by uncovering hidden connections among the linked entities and making bulk decisions for all the cases.

INTEGRATION

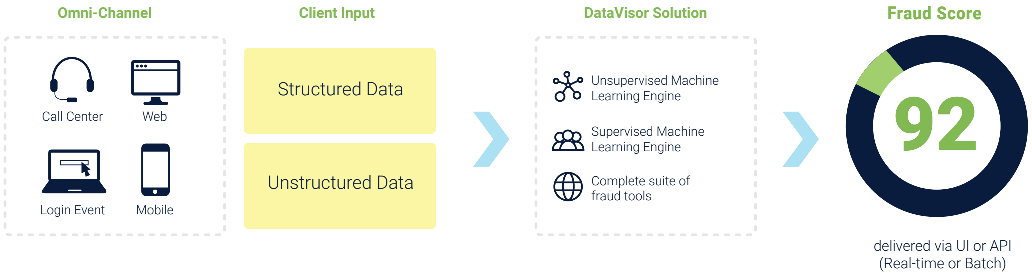
DataVisor's solutions integrated seamlessly with the client's existing data orchestration modules, detection modules, management systems, and decision engines.

The client onboarded DataVisor's solutions within two weeks and benefited from immediate protection.



HOW DATAVISOR DETECTION WORKS

DataVisor's solutions provide 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.



w r eason code campaign gr oup 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.

Results that Matter

$15 Million+

Annual Savings

Reduce financial losses and manual review costs with accurate detection.

5x -20x

Efficiency Uplift

Boost review and decision with link analysis, smart investigations, auto decisions and bulk actions.

1-2 Weeks

Fast Integration

Provide rapid and flexible integration with your systems and support real time and batch processing.

ABOUT DATAVISOR

DataVisor is the world's leading fraud and risk management platform that enables organizations to respond to fast-evolving fraud attacks and mitigate risks as they happen in real time. Its comprehensive solution suite combines patented machine learning technology with native device intelligence and a powerful decision engine to provide protection for the entire customer lifecycle across industries and use cases. DataVisor is recognized as an industry leader and has been adopted by many Fortune 500 companies across the globe.

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