



DATAVISOR

**Fighting Fraud With Machine Learning:
Stories from the Frontline**



Contents

Leading U.S. Credit Card Issuer Uses
DataVisor's Machine Learning Solution
to Reduce Application Fraud Losses3

DataVisor Enables Top Online
Marketplace to Defeat Mass
Registrations and Fake Listing Scams5

Leading Review Platform Relies on
DataVisor to Maintain a Trustworthy
and Safe Digital Environment7

DataVisor Empowers Global Social
Platform to Stop ATO and Spam
Before Damage Occurs9

Top E-Commerce Platform Leverages
DataVisor to Reach Real Customers
and Prevent Promotion Abuse11

How DataVisor Detection Works13

5 Critical Questions Fraud Analysts
Need to Ask14

About Us15

Leading U.S. Credit Card Issuer Uses DataVisor's Machine Learning Solution to Reduce Application Fraud Losses

CLIENT A top U.S. credit card issuer processing more than 20 million card applications every year.

CHALLENGES Sophisticated fraudsters were using stolen and synthetic identities to apply for hundreds of new cards at a time and the client could not capture the entire fraud group. Their operational team was simultaneously overwhelmed by fraud alerts that required intensive manual review. The client's existing solutions were reactive and could only capture known fraud. Adapting to new patterns meant delays of up to a year to refresh supervised machine learning models that required labeled data for intensive training, and which still failed to capture the coordinated application fraud group.

RESULTS



additional fraud captured



detection accuracy

0.17%

good user false positives

>\$15M

**fraud losses and
operational savings in USD**

FRAUD PATTERNS DETECTED

- ▶ Attackers used loopholes in the Gmail system to bypass the internal rule detection. Each application was associated with a unique email address, but all of them got directed to the same email account. For example:

tom.hanks@gmail.com

to.mhanks@gmail.com

tomh.anks@gmail.com

- ▶ All the above three emails would redirect to **tomhanks@gmail.com** because the character '.' is ignored in a Gmail address.
- ▶ Fraudsters kept changing patterns. To dodge detection, they applied for Card A in week 1 and then used different names and emails to apply for Card B in week 2, but DataVisor revealed that their IP subnets, devices, OS, and browsers remained unchanged.
- ▶ Fraudsters used real people's names and addresses in the U.S, but the email domains were 126.com—a China-exclusive domain—and their names and email addresses were not correlated. Their IPs were from a single data center in Los Angeles.

DataVisor took a holistic approach to detect sophisticated application fraud

Names and email addresses are not correlated		126.com domain is from China but the addresses are in U.S.		Different cards	Different incomes	Different IPs but from the same data center	DATAVISOR SCORE
NAME	EMAIL	ADDRESS	CARD	INCOME	IP ADDRESS		
Jon S	ZHOU12**@126.COM	34** Sa** Blvd, CA	Card A	133k	50.51.***.69		93%
Daenerys T	WANG23**@126.COM	22** Mi** Ave, CA	Card B	123k	50.51.***.202		93%
Arya S	CHEN34**@126.COM	68** Vi** Dr, CA	Card A	103k	50.51.***.129		93%
Tyron L	HUA15**@126.COM	43** Mi** Ave, TX	Card B	113k	50.51.***.19		93%
Cersei L	MO87**@126.COM	36** He** Dr, TX	Card A	93k	50.51.***.4		93%
Theon G	DAI65**@126.COM	12** Co** Road, TX	Card B	153k	50.51.***.23		93%
Sansa S	ZHAO90**@126.COM	56** Sh** St, NJ	Card A	128k	50.51.***.224		93%
Jaime L	QIN55**@126.COM	75** St** Blvd, NJ	Card C	139k	50.51.***.202		93%

HOW DATAVISOR HELPED

DataVisor's solution enhanced detection coverage and significantly improved operational efficiency. Its unsupervised machine learning solution proactively detected coordinated and unknown frauds with high accuracy, enabling the client's analysts to effectively make bulk decisions that could be applied to hundreds of cases in the same fraud ring.



DataVisor Enables Top Online Marketplace to Defeat Mass Registrations and Fake Listings

CLIENT A global online marketplace operating in 40+ countries with over 350 million monthly active users.

CHALLENGE The client was plagued by mass-registered accounts that would first incubate for weeks, then start launching fake listings to scam good users. The accounts were highly coordinated and shared similar patterns, but the client's current solutions could only capture a portion of the fraud rings due to an inability to identify the cross-account linkages among all of the accounts. The solutions were also not able to analyze unstructured data and metadata and therefore could not reliably detect large-scale fake listings.

RESULTS



of fraudulent accounts
caught before the first scam



Auto-action on over
65% of detections

68k+

accounts caught in
the largest fraud ring

>20%

detection accuracy improvement
over existing solutions

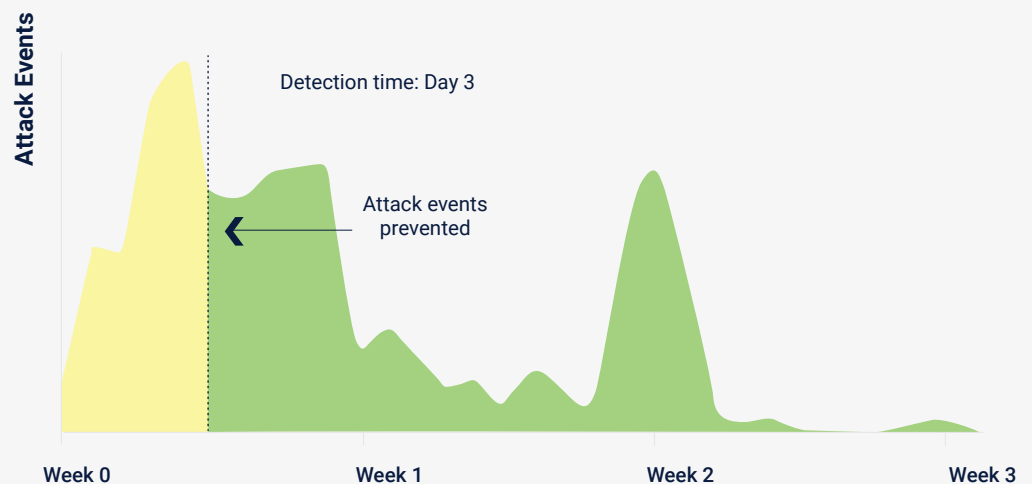
FRAUD PATTERNS DETECTED

- ▶ Disposable emails for registrations; bots for scripted logins from cloud hosting IPs.
- ▶ 2-minute intervals between login and attack; similar listing descriptions created from templates with shared URLs.
- ▶ “Hit-and-run” behavior: 60% of fraudulent accounts made the first attack within 2 hours of registration; 76% made the first attack within 24 hours of registration.
- ▶ Sleeper cells: some accounts logged in then remained dormant for weeks prior to a large-scale scam.
- ▶ Human-operated scam farms: a group of scam armies was highly correlated on behavioral patterns such as event sequences, event time, and intervals. They attacked weekdays and rested on public holidays and weekends.

HOW DATAVISOR HELPED

DataVisor’s solution uncovered suspicious accounts and coordinated fraudulent registrations early in the incubation stage, and flagged scam content by analyzing posts and images and spotting similar attributes and behaviors across accounts.

DataVisor’s solution detects sleeper cells early in the incubation





Leading Review Platform Relies on DataVisor to Maintain a Trustworthy and Safe Digital Environment

CLIENT A top U.S.-based online reviews platform that connects businesses and customers through over 170 million total reviews.

CHALLENGE The client was suffering from financial and reputational losses, and incurring increased compliance risk, due to massive amounts of fake reviews and spam activities. The client's content-based systems were struggling to identify fake reviews, particularly those that came at a large scale. By the time they were flagged as fraudulent, the damage had already been done, as they'd been up for weeks and viewed by thousands of customers.

RESULTS

10,000+

fake reviews/ratings
prevented per day

2,000+

Auto-action on over
65% of detections

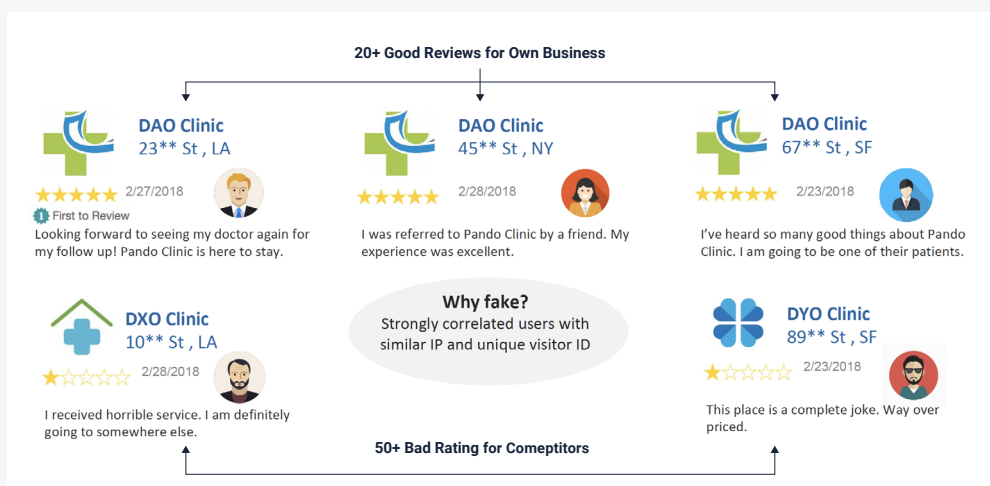
>80%

coverage of spam, capturing
both small and massive-scale
fraud rings

FRAUD PATTERNS DETECTED

- ▶ Professional campaigns: A large coordinated group of paid posters promoted specific businesses using legitimate-seeming accounts with profile photos, friends, and varying time zones.
- ▶ “Mom-and-Pop” reviews: Business owners endorsed their own services and degraded their competitor’s businesses.
- ▶ Meticulous strategies: Attackers “incubated” accounts before using them in attacks, consistently changed IPs/devices/locations, and wrote diverse reviews. For those attackers who only cared about ratings, they simply copied irrelevant reviews from good users to speed up their attacks.
- ▶ Engagement efforts: Attackers friended good users, then sent promotion spam and/or requested reviews for certain businesses.

Positive reviews for their own businesses and 50+ bad ratings for competitors



HOW DATAVISOR HELPED

DataVisor’s solutions identified patterns of fraudulent activity—through close analysis of digital signals and cross-account linkages—to detect even the most sophisticated fake reviewing rings. DataVisor’s solutions also captured groups of fraudsters at the time of registration, before any damage occurred.



DataVisor Empowers Global Social Platform to Stop ATO and Spam Before Damage Occurs

CLIENT A leading global social commerce platform with over 250 million monthly active users.

CHALLENGE Fraudsters were taking over user accounts in bulk and spamming legitimate users, thereby damaging the client's brand and accelerating their customer churn rate. The client's existing tools could not catch up with new and evolving account takeover (ATO) techniques or detect large groups of coordinated ATO. When fraudsters used legitimate accounts to spam good users, their solutions were not effective at capturing those events—the coverage was limited and the fraud alerts triggered weeks later.

RESULTS



of all spammers captured



of spammers stopped at sign-up

7x

increase in overall detection rates

FRAUD PATTERNS DETECTED

- ▶ Fraudsters took over inactive accounts and edited profile descriptions to include spam domains. They used these accounts to follow large number of users, and gained new followers who would then visit the spam links in their profiles.

Large-scale friend requests with spam links in the profile

Friend Request from Alex

Message

Follow

80 followers, 900 following

Followed a large number of users expecting them to see the profile

About me:

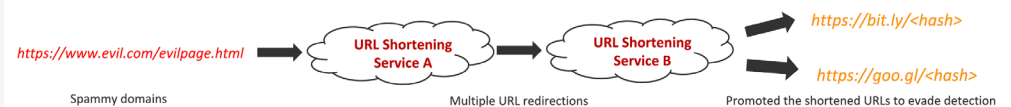
[https://bit.ly/\[hash\]](https://bit.ly/[hash])

Spammy links in the profile descriptions

The link has steal more of my sex photos and videos

- ▶ Attackers disguised spam domains with shortened URLs to avoid blacklisting and used multiple URL redirections to further evade detection.

URL shortener and multiple URL redirections to evade detection



- ▶ Fraudsters used VPN or cloud hosting sites to hide their true locations.
- ▶ Attackers used scripted bots to automate high-frequency events: 90% of observed inter-event intervals were 1-3 seconds.

HOW DATAVISOR HELPED

Using machine learning models to analyze user histories, behavior changes, and suspicious patterns, DataVisor's solutions captured sophisticated, large-scale, coordinated ATO attacks before damage could occur, and prevented spambot attacks by identifying correlations of digital patterns.

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

CLIENT A leading food delivery platform in Asia, with over 50 million monthly active users.

CHALLENGE 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. The client'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.

RESULTS



detection accuracy enabled client to
launch promotion campaigns to real
customers



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

23%

detection uplift

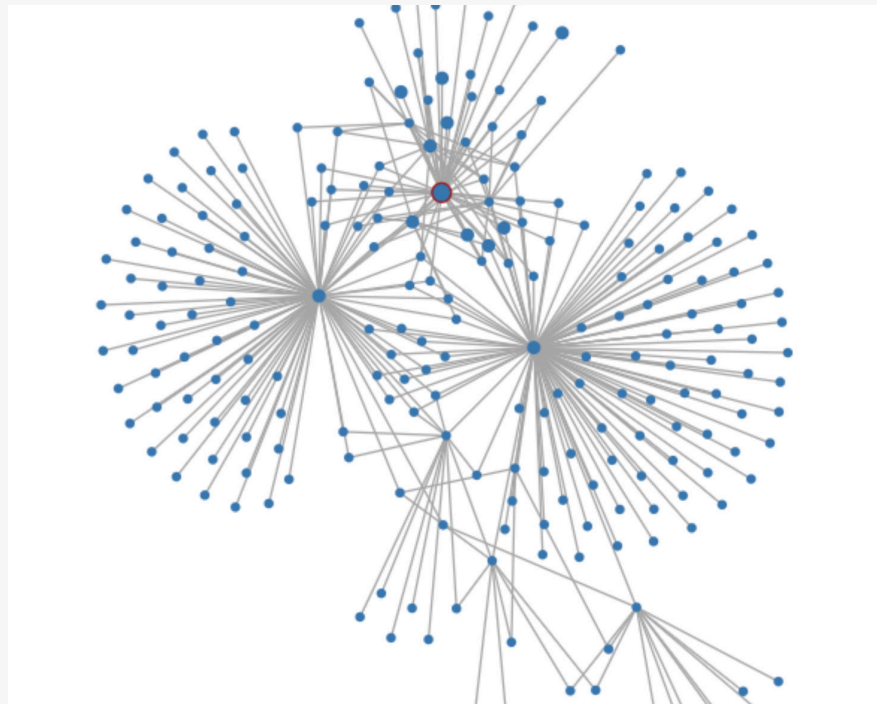
FRAUD PATTERNS DETECTED

- ▶ A group of over 130k fraudulent accounts with different IPs placing orders to over 30K merchants. Fraudsters utilized emulators to create unique device IDs for all accounts.
- ▶ A group of 1.2k+ attackers registering on the same day a promotion launched; the accounts used fake addresses, placed orders under \$5, and wrote “don’t deliver” in the comments.
- ▶ A merchant that used 50+ fake accounts with various delivery addresses to receive the promotion subsidy. Most of the accounts placed more than one order to try and mimic normal user behavior and evade detection rules.
- ▶ Mass registration of accounts using old Android devices, out-of-date OS versions, and disposable emails. Fraudsters attempted to hide their locations through IP obfuscation.

HOW DATAVISOR HELPED

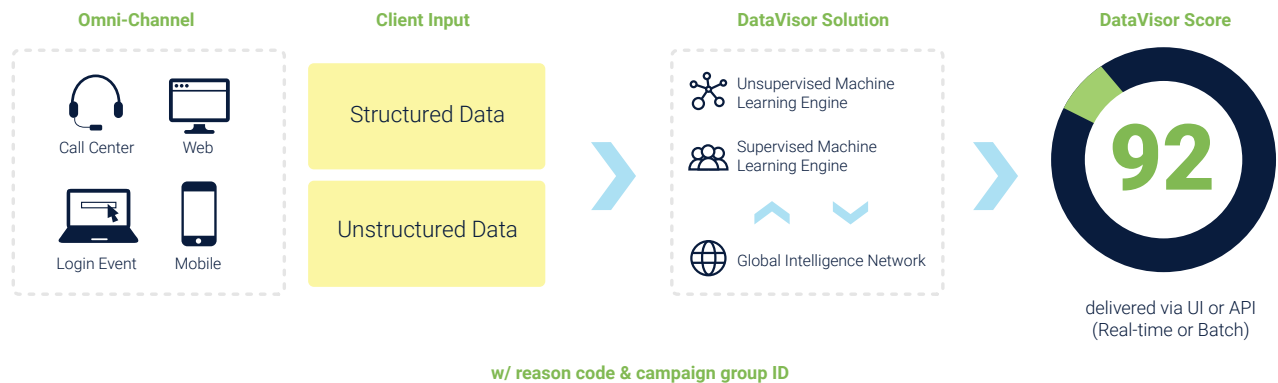
DataVisor’s solution rapidly and accurately identified all fraudulent activity no matter how often or how quickly fraudsters changed their patterns, seamlessly adapting to new markets on day one.

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







How DataVisor Detection Works

The DataVisor approach enables proactive fraud protection. 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 solutions accelerate detection by analyzing all accounts and events simultaneously and identifying suspicious clusters of malicious activity—even at the point of account registration. This approach is ideal for finding new and unknown attacks because it does not require historical data and constant retuning.









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.

Comprehensive Fraud Intelligence that Provides Fine-Grained Signals and Risk Scores

- | | |
|--|---|
|  410 Million+ IP addresses |  5.3 Million+ User agent strings |
|  3.6 Million+ Email domains |  160,000+ Device types |
|  300,000+ OS versions |  700,000+ Phone prefixes |

Insight from 4.1 Billion+ Users and 800 Billion+ Events

- | | | |
|--|--|---|
|  Financial Services |  E-Commerce |  Social Platform |
|  Mobile & Gaming |  Telecom & Travel |  Insurance |

5 Critical Questions Fraud Analysts Need to Ask

Q: How do I take advantage of next-gen fraud prevention solutions that are built on modern architecture, when their workflows aren't as mature as my legacy tools?

A: You can choose a solution that offers the best of both worlds. DataVisor's platform is built on the latest big data infrastructure to make real-time computations at big data scale. It also empowers all stakeholders to work collaboratively. Fraud teams can act with the benefit of mature case management and alert system capabilities, while data science teams can import and visualize data, explore recommended features, and run, validate, and deploy their models.

Q: How can I make the best use of my large, complex, and unstructured data sets?

A: The best way to handle data effectively is to rely on a solution that can extract valuable derived information such as digital footprints, user behaviors, and cross-account linkages, and structure them into consumable insights. DataVisor's solution empowers you to leverage digital data to enhance your decision-making efforts, and significantly improve your results.

Q: Is it possible to enrich my signals with global fraud intelligence?

A: Yes! DataVisor clients count on our DataVisor Global Intelligence Network (GIN) to enhance fraud

intelligence. The GIN is powered by over 4 billion protected accounts and 800 billion events and provides fine-grained signals and risk scores. Its digital data includes IPs, location, email domains, devices, OS, browser agents, phone prefixes, and more.

Q: Sophisticated fraudsters launch large-scale, coordinated attacks. What's the most effective way to capture and act on all of them?

A: The best approach is to analyze and process events and accounts holistically, instead of viewing them in isolation. DataVisor captures entire fraudulent groups by uncovering hidden links among accounts with correlated attributes. These accounts are then clustered together so that analysts can review all cases at one time and make bulk decisions, significantly improving their efficiency.

Q: Attackers keep changing their patterns. How can I catch them early, in real time, before damage occurs?

A: To do so, you'll need to embrace a proactive solution that can stay ahead of fraudsters at all times. DataVisor's unsupervised machine learning solution adapts rapidly to new frauds because it does not require labeled data, extensive training periods, or constant retuning. It captures fraudsters early at registration time and provides real-time scores at the speed of your business.

An isometric illustration of a vibrant city street scene. In the foreground, a large white sign with a rainbow arch over it sits on a sidewalk. People are walking around, some carrying bags. In the background, there are colorful buildings, a blue car, and a large yellow coin with a Bitcoin symbol. A sign on a building says "WELCOME".

About Us

DataVisor is the leading fraud detection platform powered by transformational AI technology. Using proprietary unsupervised machine learning algorithms, DataVisor restores trust in digital commerce by enabling organizations to proactively detect and act on fast-evolving fraud patterns, and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of more than 4B global user accounts, DataVisor protects against financial and reputational damage across a variety of industries, including financial services, marketplaces, e-commerce, and social platforms.

For more information on DataVisor solutions:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043