CASE STUDIES

Stories from the Frontline

E-COMMERCE & MARKETPLACE FRAUD

DATAVISOR

Introduction

Consider the experience from your customer's perspective. They're on a tight budget, and a new car just isn't an option. But they need reliable transportation to hold on to their job. It's a big investment, and they're worried about buying something used online. They're not an experienced online shopper, and they've heard about the scams out there. They've also heard your platform is trustworthy, so they give it a shot despite their misgivings. Before they know it, they're being victimized by fraudulent ads they don't recognize as malicious. They click on one wrong link too many, provide a little too much personal information, and end up getting hacked. Fake accounts set up in their name start posting more scams. Shipping orders start to go missing. They get charged for online orders they never made. It's a nightmare.

This kind of devastating experience happens far too often across today's digital marketplaces and e-commerce platforms. When fraudsters succeed, trust is eroded, and angry and frustrated customers churn out as businesses suffer both financial and reputational damage.

It doesn't have to be this way. Today, many organizations are successfully fighting back against increasingly sophisticated, large-scale threats by embracing cutting-edge, AI-powered fraud solutions capable of proactively detecting and preventing coordinated attacks in real time and at scale.

Let's look at four examples of marketplace and e-commerce clients who chose DataVisor as their fraud prevention partner, and who are now thriving accordingly.

Contents

PAGE NO. 11

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

- Client Challenges
- Client Success with DataVisor's Solutions
- Fraud Patterns and Vulnerabilities Detected

60%
detection uplift

40%
increase in review efficiency using holistic analysis

>$4M
fraud loss savings

PAGE NO. 15

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

- Fraud Patterns Detected
- How DataVisor Helped

90%
of fake listings detected right after they are posted

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

10x
increase in detection as compared with existing rules

20x
improvement in manual review efficiency

CASE STUDY: PROMOTION ABUSE, BUYER-SELLER COLLUSION

Food Delivery Unicorn Uses DataVisor For Fraud-Free Global Expansion

CLIENT

A global online food ordering and delivery platform with 100 million+ monthly active users and services in 20+ countries.

CHALLENGES

- The business was rapidly expanding, and encountering unique fraud problems in each new region, including promotion abuse and buyer-seller collusion.
- Existing rule-based solutions could not keep pace with the fast-growing business and were incapable of capturing unknown fraud in new markets.
- The client needed a modern infrastructure solution to support real-time decisioning and handle massive data volumes.

SOLUTIONS

- Leveraged unsupervised machine learning to capture bot-registered malicious accounts early at the registration stage and uncover buyer-seller collusion.
- Provided a proactive solution to ensure the fast-growing business could start getting immediate results without the need for historical data and labels.
- Provided real-time detection and supported high QPS with low latency.

RESULTS

detection uplift

fraudsters caught at registration

$6M

savings in fraud losses

CLIENT CHALLENGES

The client is a fast-growing food tech unicorn that is reshaping the search, order, and delivery experience for over 100 million online users. The business has been rapidly expanding into new countries over the past two years, and now provides services in 10,000+ cities worldwide.

While growth was skyrocketing, the company was continuing to lose millions of dollars annually to fraud, and the problems were worsening as the business scaled. Attackers were continuing to evolve their attacks to evade existing detection systems, and the business was confronted by unique and previously unseen attacks types every time they expanded into a new region.

New Risks for New Markets

To penetrate new markets and maintain an aggressive growth trajectory, the client needed to move rapidly. This agenda, however, was at odds with the reality that their fraud team needed time to create new rules and train new models to address the new risks in each new market. With the company not able to build adequate defenses, their fraud losses increased accordingly. It quickly became apparent that to support their expansions, they needed a solution that could provide immediate protection on day one.

Promotion Abuse

The client's aggressive promotion campaigns attracted both customers and fraudsters, and the fraudsters were creating fake accounts at a massive scale to take advantage of the promotions— sign-on and referral bonuses, discounts, and more. They were using a combination of botnets and human farms to attack with high frequency at large scale, and this led to substantial financial losses for the business.

Buyer-Seller Collusion

Collusion among merchants, customers, and delivery riders was happening under the radar. "Customers" were making thousands of fake orders online, the "merchants" were pretending to prepare food, and the "riders" were acting as if they had delivered the food. However, while all of the parties received a vast number of subsidies from the platform, no actual food delivery ever took place.

No Real-Time Capability

The client needed to monitor activities in real time to block fake users and orders immediately, without creating any friction for good users. However, their existing solutions were not able to process the vast data volumes in real time, which slowed their decision processes, and left their detection efforts unable to scale on pace with the growth of the business.

FRAUD PATTERNS DETECTED

Buyer-Seller Collusion

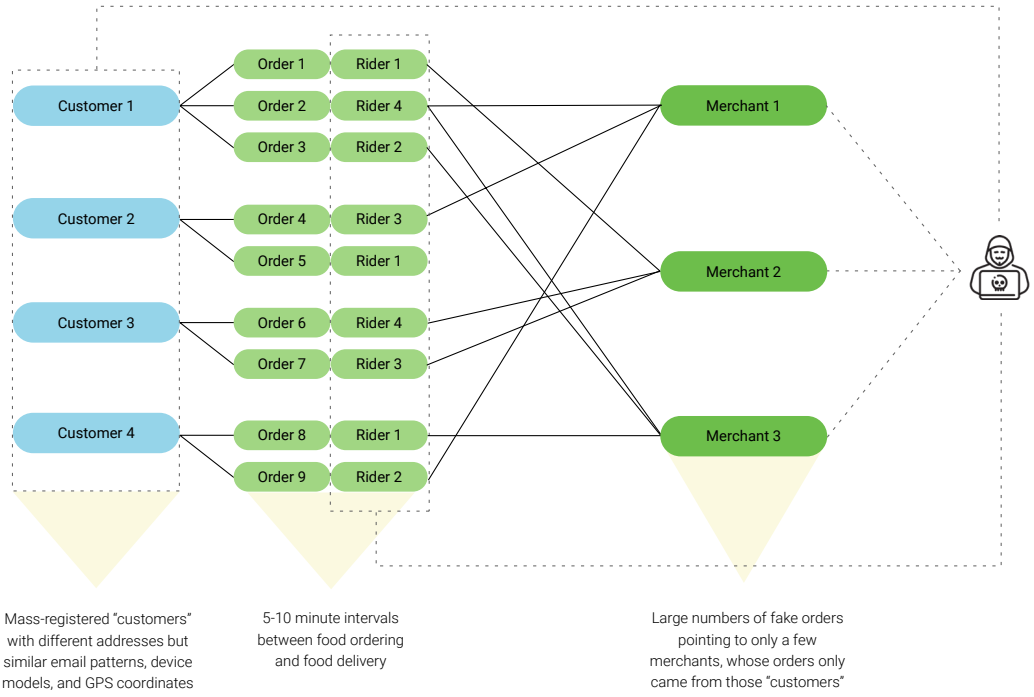
DataVisor uncovered an extensive collusion network containing over 50 customers, merchants, and riders, who conspired to place over 200 fake orders to fraudulently claim subsidies from the client.

Evasion Techniques

The fraud group used different delivery addresses for the orders. Most of the "customers" placed more than one order during lunchtime to mimic normal user behavior to evade simple detection rules.

Fraud Patterns DataVisor Detected

All of the "customers" shared similar email patterns, device models, and GPS coordinates. All the suspicious orders originated only from these "customers." The intervals between order times and order deliveries were consistently between 5 and 10 minutes—a range not actually possible.



CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

DataVisor's best-in-class AI and machine learning solutions empowered the client to expand rapidly into new global markets with the confidence that they could successfully manage risk, neutralize fraud, and secure their platform. The DataVisor solutions adapted rapidly to new and unknown fraud in each new region, detected large-scale attacks in real time before any damage was done, and exposed under-the-radar, coordinated collusion.

The client chose DataVisor as their strategic partner for international expansion, knowing that DataVisor's proactive, scalable, and intelligent solutions provided exactly what they needed to meet their audacious goals.

Fast Onboarding and Protection for New Markets

The client rapidly onboarded DataVisor's solutions within two weeks, and the new systems immediately began to detect unknown and fast-evolving fraud. By eliminating their reliance on out-of-date, legacy rules written for previous regions, the client was able to consistently and proactively detect new fraud on day one in each new region. Instead of losing time to exploring and testing rules, collecting data and labels, and building and training models, DataVisor's scalable and adaptive solutions enabled the business to save more than $6M in fraud losses.

Detecting Promotion Abuse at the Gateway

DataVisor's solutions preemptively detected the majority of promotion abusers at the registration stage, before they could launch any new attacks. Using unsupervised machine learning and big data analysis, the new solutions stopped highly damaging activities at scale, including malicious bot-scripted and human-operated attacks. In addition to providing significant detection uplift, DataVisor's solutions also delivered accurate results that enabled the business to consistently distinguish between good customers and fraudsters, ensuring optimal execution of promotion strategies.

Uncovering Hidden Collusion with Holistic Data Analysis

DataVisor's solutions discovered buyer-seller collusion by holistically analyzing activities, accounts, addresses, digital fingerprints, and more, to expose suspicious patterns and coordinated activities. While the malicious merchants, customers, and riders stealthy hid their behaviors and kept changing patterns, they nonetheless left subtle traces, and DataVisor's unsupervised machine learning technologies were able to connect the dots and expose the buyer-seller collusion.

Real-Time Detection and Big Data Capability

The client benefited greatly from DataVisor's modern infrastructure, which can handle massive data volumes and support real-time detection with high QPS. With DataVisor's highly scalable solution, the client was able to expand rapidly while defeating fraud, exposing collusion, and stopping promotion abuse in real time.

CASE STUDY: MASS REGISTRATION, FAKE LISTING

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.

CHALLENGES The mass registrations were highly coordinated but the current solutions could not identify cross-account linkages and therefore only captured a portion of the fraud ring. They were also not able to reliably detect large-scale fake listings due to an inability to analyze unstructured data and metadata.

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%

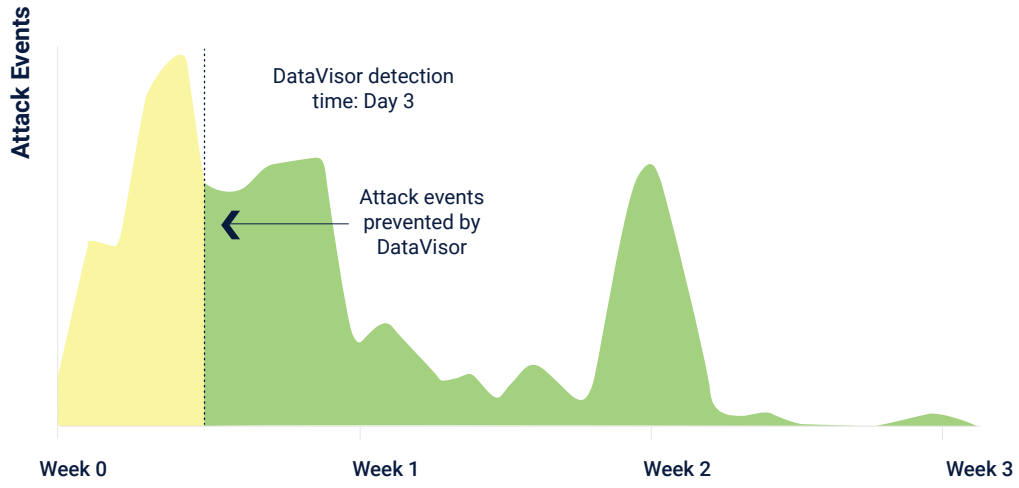
detection accuracy improvement over existing solutions

FRAUD PATTERNS DETECTED

- Disposable emails for registrations; bots for scripted logins from cloud hosting IPs
- 2-minutes 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 weekend.

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.



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.

CHALLENGES 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

detection uplift

increase in review efficiency using holistic analysis

>$4M

fraud loss savings

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 SOLUTIONS

The client began using DataVisor's solution—an advanced AI-powered platform 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 solution found hidden connections between seemingly isolated incidents, exposed new attack patterns, and unmasked highly sophisticated fraud attacks. 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, this approach made it possible 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 DataVisor's solutions were 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, DataVisor 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, DataVisor systems 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, it was 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, DataVisor's solution 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. Large clusters of mass registered users, after short incubation periods, were shipping scam mails at high frequency to harass victims, and deceptively entice them to fall prey to advertising frauds.

One such campaign 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.

CASE STUDY: FAKE LISTING, SPAM, ATO

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

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.

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 toreviewlarge volumes of false positive alerts generated by the static rules.

RESULTS

of fake listings detected right after they are posted

of spammers flagged within 2 days of sign-up

10x

increase in detection as compared with existing rules

20x

improvement in manual review efficiency

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-seemingISP IPs from the same country and were not active immediately after ATOs—they were incubating the accounts before posting the scam content.

Patterns detected

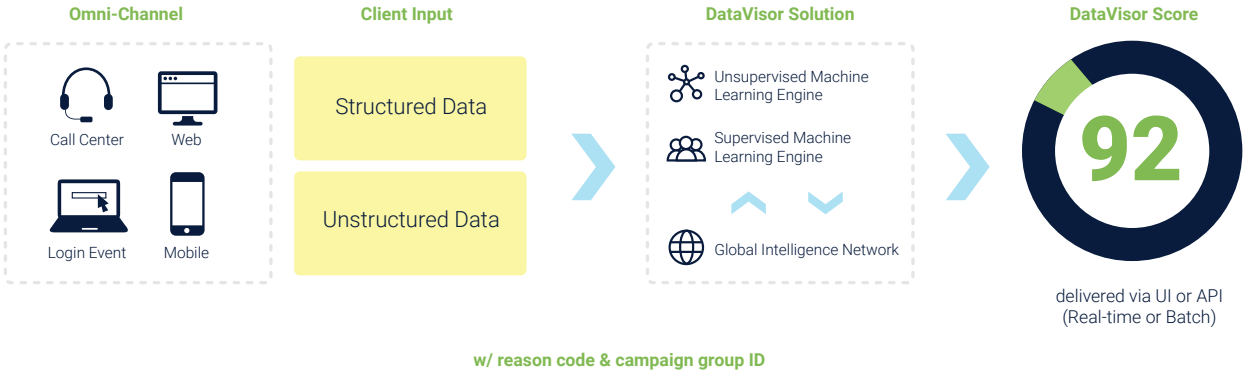
All 5,000+ accounts had 10 to 20 login events within a 3-minute window on the same day, where the time interval between consecutive logins was always the same. In addition, those accounts each made at least one luxury watch listing on the next day, with a particular brand mentioned in each listing description.

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.

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.



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
- 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 4.2 Billion+ Users and 800 Billion+ Events

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

Executive Summary

According to **numbers provided by the U.S. Department of Commerce,**consumers spent more than $601 billion online with U.S. merchants in 2019, and per **analysis of these numbers by Digital Commerce**, online spending represented 16.0% of total retail sales for the year. At the global level, retail e-commerce sales worldwide amounted to **3.53 trillion U.S. dollars in 2019,** and e-retail revenues are projected to grow to **6.54 trillion U.S. dollars in 2022**. These are remarkable numbers, and they're echoed by the rates of growth DataVisor sees with its e-commerce and marketplace clients, all of whom are enjoying similar levels of success.

Challenges

Growth of this kind is not without its challenges, however. Expansion into new territories can mean encountering new and previously unknown threats. Rapidly growing user bases can be breeding grounds for mass registration attacks that lead to spam, scams, and content abuse. Aggressive promotions can invite buyer-seller collusion.

Far too often, growth strategies outpace risk management strategies, and fraud teams are left scrambling to keep up, hampered by reliance on legacy solutions that require historical data, rules, and labels. Unable to accurately and efficiently process and analyze high volumes of raw data in real time, organizations end up either loosening protections and enduring increased fraud losses, or leaving static rules in place that lead to high false positive rates and worsening customer experiences. Most critically, in the context of rapid growth, continuous innovation, expanding payments options, significant increases in mobile usage, and more, most existing fraud solutions are simply being outmaneuvered by technologically savvy digital fraudsters who are leveraging the latest tools and techniques to launch automated attacks of increasing speed, sophistication, and scale.

Solutions

Successful defeat of the complex, fast-evolving, bot-powered fraud attacks threatening today's e-commerce and marketplace platforms requires the implementation of AI-powered solutions capable of proactively detecting and defusing sophisticated attacks in real time and at scale.

It is only through holistic data analysis and the use of advanced clustering and graphing techniques that it becomes possible to surface and expose the correlated patterns and connections across users and accounts that signal coordinated fraud activity. It is only by maintaining complete and comprehensive protection across the entire customer lifecycle that organizations can accurately and consistently differentiate between legitimate and fraudulent accounts and actions. It is only through the use of unsupervised machine learning that it becomes possible to analyze vast amounts of data in real time without time-consuming reliance on labels and rules. It is only by centralizing intelligence and deploying automated feature engineering informed by superior domain expertise that organizations can meet complexity with complexity, scale with scale, and speed with speed. It is only this kind of approach that can consistently produce the actionable insights that will power growth and minimize risk in today's digital economy.

Conclusion

Just as DataVisor has pioneered the application of transformational technologies to the challenges of modern, digital threat attacks, our clients are now leading the way in embracing future-facing solutions that empower them to protect their customers, their data, and their businesses in ways that will see them continue to grow and prosper in the new decade, and beyond.

YINGLIAN XIE
Co-Founder and CEO
DataVisor

FANG YU
Co-Founder and CTO
DataVisor

About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform for enterprises. 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, ecommerce, and social platforms.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

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

DATAVISOR