
A GUIDE TO

# **Complete Protection** Across the Customer Account Lifecycle

DATAVISOR

# Contents

# Introduction

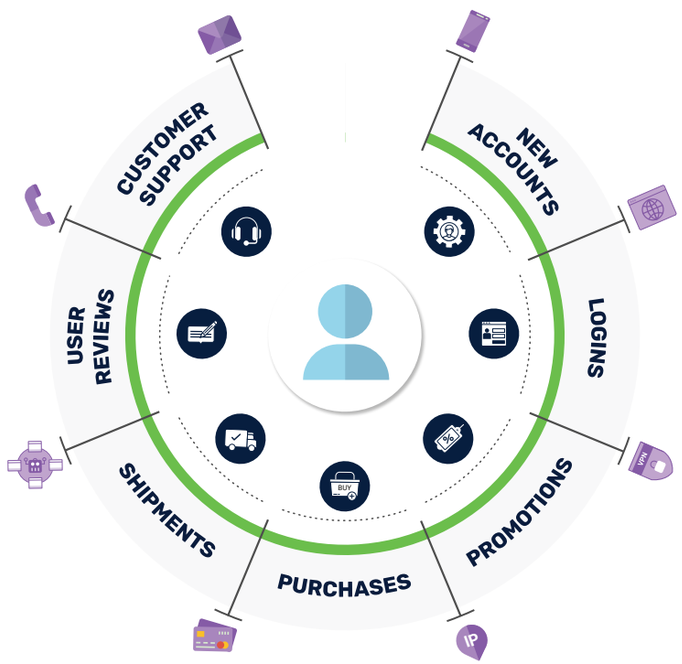
Modern organizations must completely rethink how they approach fraud prevention. Today's fraudsters have in their arsenal a growing number of sophisticated techniques to infiltrate customer accounts or impersonate good customers. They can mass-register fake accounts and wait in stealth mode for weeks or days to launch large-scale attacks. Or, they commandeer good user accounts to execute phishing schemes, promotion abuse, payment and shipping fraud, and more.

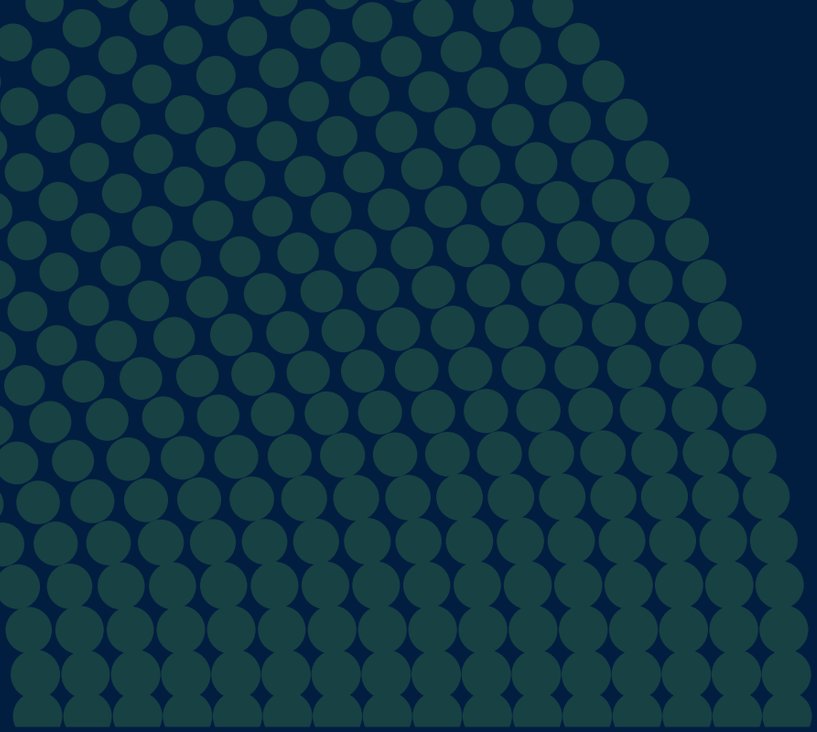
Traditional point solutions only address one use case, or they look for fraud only at the transaction level. They rely on rules and reactive machine learning techniques that can no longer match the speed, scale and complexity of modern fraud attacks — and organizations suffer from financial loss, negative customer experiences and a tarnished reputation.

To fight all types of fraud, businesses must leverage the full spectrum of fraud detection and prevention capabilities available — bot detection, device identification, behavior analytics and machine learning — to assess the risk of users interacting with their digital channels, and gather the broadest and deepest insights to protect the customer's journey. Rather than relying on one-time risk assessments at the entry point — a login or payment transaction — they must implement solutions that continually assess risk across the entire customer lifecycle. In this way, businesses will be able to detect and prevent fraud attacks with precision and accuracy, and retain valuable customers by providing a frictionless experience.

# The Key to Continuous Fraud and Risk Protection

With its comprehensive platform for enterprise fraud and risk management, DataVisor delivers continuous protection across the entire customer account lifecycle. In this ebook, we'll explore six of the most common types of fraud, and explain how DataVisor enables complete, proactive protection for each use case.





STAGE 1

# Fake Accounts

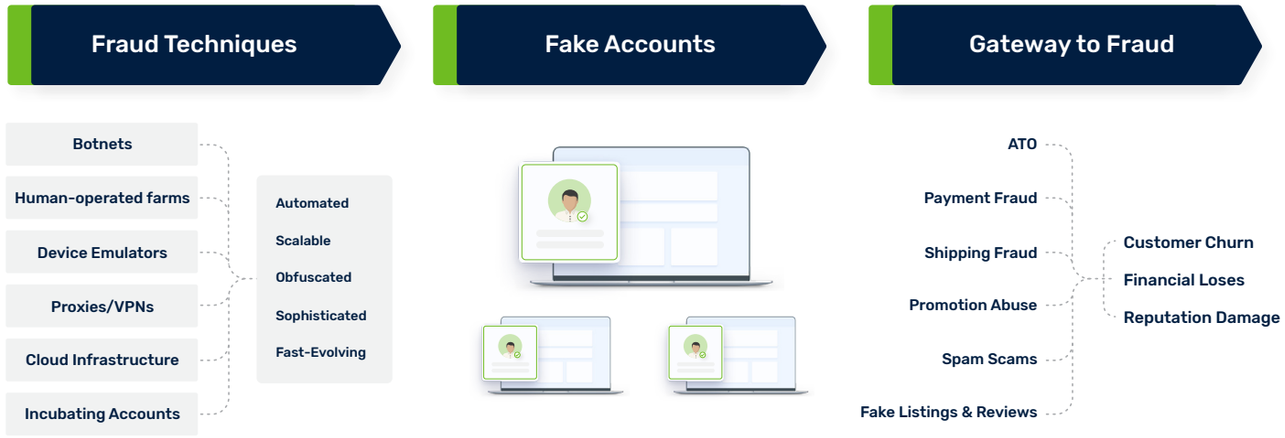
A common method fraudsters use to commit fraud is mass registration of fake accounts. Traditional fraud and risk solutions monitor transactions and activities as the fraud is happening but fail to address the root cause, and there's no real-time capability to identify fake accounts until they're already in use. By then, it's too late. Early detection is necessary to catch fraudsters red-handed, before the damage is done.

THE PROBLEM

# Fake Accounts Open the Door for Fraudsters

Modern fraudsters use automated AI-driven botnets or human-operated farms to mass register fake accounts at scale to commit application and payment fraud, promotion and content abuse, scams and more. They may use device emulators and cloud infrastructures to obscure or disguise their digital fingerprints. Often, attacks are launched immediately after the accounts are created — a slow response can result in huge fraud losses. Legacy, reactive approaches fail to detect incubating accounts, which at first may seem authentic, but can be used at a later date to execute attacks of massive scale.

*** The Fraud Report:** How Fake Users Are Impacting Business




**82%**

of companies confirm fake users are a big problem; 44% report they are a significant problem.*

**5.4B**

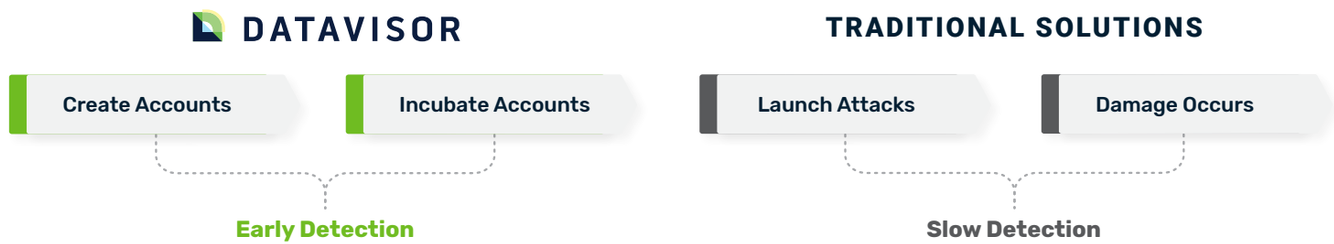
fake accounts were removed by Facebook in 2019; 64% increase from 2018.*

# THE SOLUTION

## Early Detection Is CRITICAL

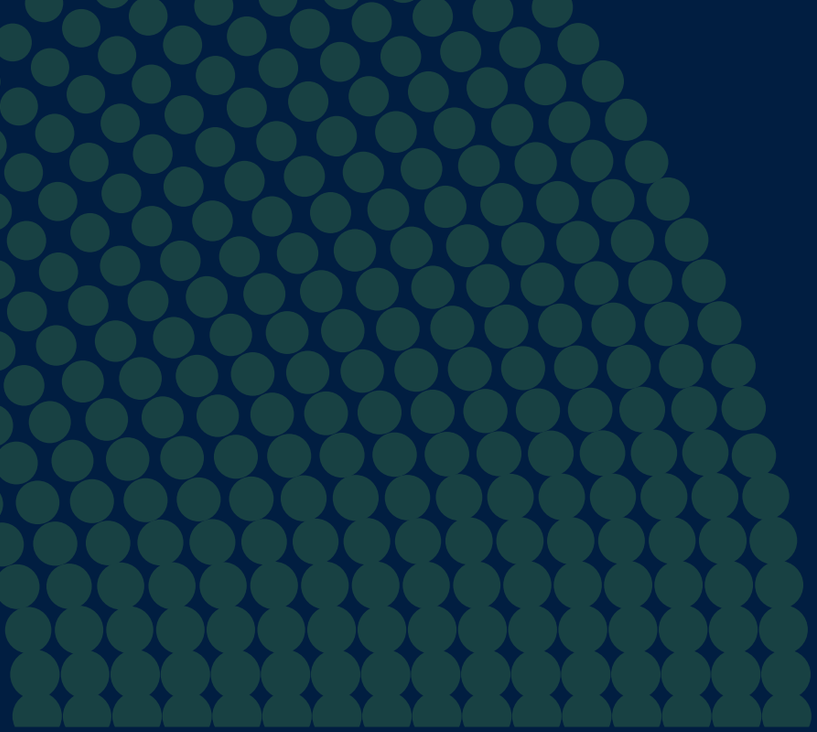
DataVisor solutions detect fraudulent activity in real time, the moment an account opens, stopping the process before any damage occurs. They leverage UML to holistically analyze digital fingerprints, metadata and more, and enable accurate decision-making, even with limited information. By capturing malicious activity fast and early, DataVisor stops fraud at the gate and prevents downstream damage from incubating accounts.

DataVisor's solutions deliver immediate ROI, because they don't rely on historical data or labels. Using linkage analysis, they can detect groups of fake accounts simultaneously, enabling fraud and risk teams to make bulk decisions to thwart coordinated, large-scale attacks.




*DataVisor customers have achieved **99%** detection accuracy and have been able to capture **80%** of attempted fraud at account registration — a **7X** uplift in fraud detection.*

99%



STAGE 2

# Account Takeovers

Account takeovers have increased by 31% in 2020, and that percentage is growing. Fraudsters release bots to gather user credentials and other data, then take over their accounts. But traditional authentication methods add friction to the customer experience and produce high rates of false positives — and, they're too slow for fast-moving bots. Once again, early detection is critical to preventing account takeovers and the criminal activities that follow.

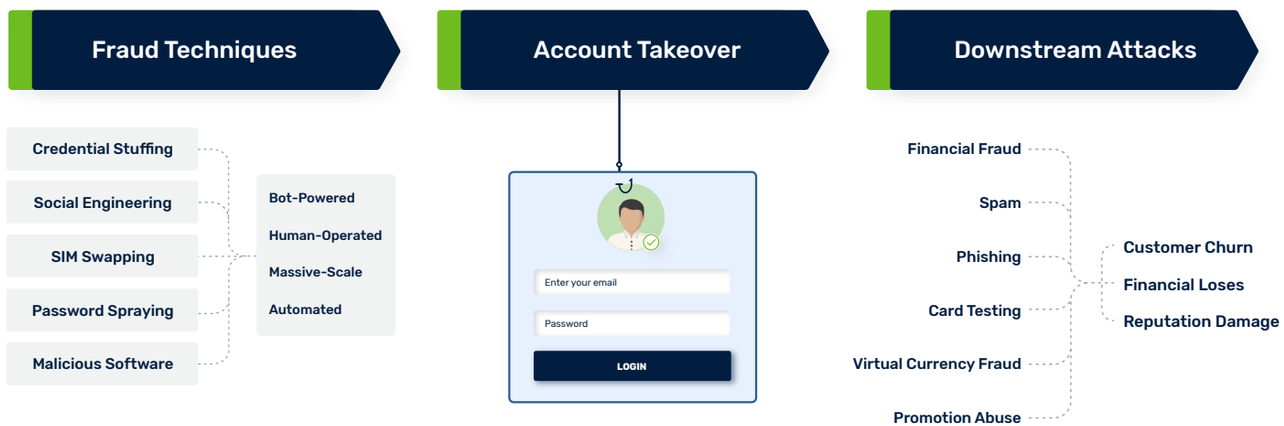
# THE PROBLEM

## Account Takeovers Are Damaging Your Businesses and Customers

Fraudsters use credential stuffing, social engineering (phishing), SIM swapping, password spraying and other techniques to compromise good users' accounts, and steal personal and financial data to commit fraud. Automated bots can perform upwards of 100 attacks per second, making it easier and faster for fraudsters to do their dirty work.

Unfortunately, traditional fraud detection methods add friction to the customer experience and often produce false positives, denying good customers access to their own accounts. This causes frustration and customer attrition. What's more, they're slow to stop fraud — 72% of the time, fraudulent transactions occur within one hour of the initial compromise. Bots can impersonate many different devices with different IP addresses. Such hyper-distributed attacks go undetected — until it's too late.

***** Forter's Fifth Fraud Attack Index
****** Forter 2019 ATO whitepaper




**31%**

increase in ATOs year over year, showing no signs of abating. *

**100**

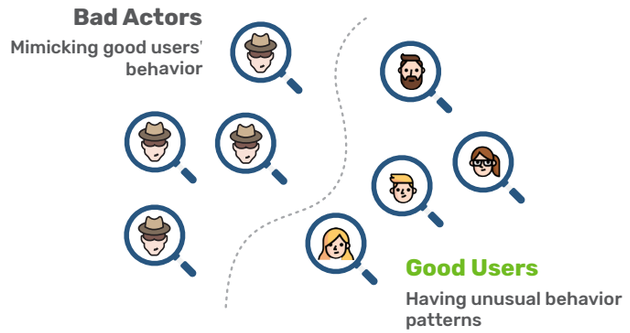
attacks per second, by **BOTS**, making it easier and faster for fraudsters to commit account takeover.**

# THE SOLUTION

## Ensure **Good Customers** Aren't Victims of Fraud

Protecting user accounts without adding friction to the customer experience requires assessing behavioral changes early and with high accuracy. DataVisor's solutions distinguish good users from bad actors who mimic good user behavior to protect customer accounts before an attack occurs — and without the use of legacy knowledge or historical labels.

DataVisor tracks out-of-pattern behavior associated with individual accounts and uses UML to identify group-level, large-scale takeover behaviors in real time. Holistic analysis against a vast Global Intelligence Network of more than 1 trillion events enables proactive protection at the point of compromise — whether the attack is distributed, bot-powered or human-operated — stopping fraudsters in their tracks, reducing false positives and providing good users with seamless, friction-free account access.




**DATAVISOR**

**Individual-Level Analysis**

Track anomalous behaviors based on each account.
Detect sophisticated attacks in real time while add no friction to good users.

**Group-Level Analysis**

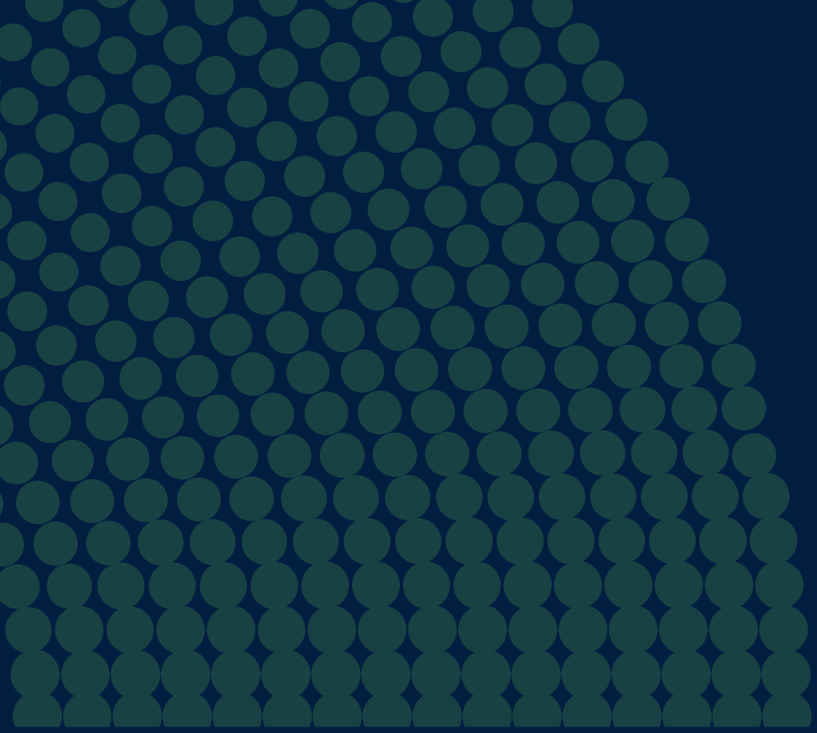
Use unsupervised ML to perform cluster analysis.
Uncover bot-powered or human-farm-operated attacks at large scale.

**Global-Level Analysis**

Use global data from 4.2B protected accounts to track transition probability.
Distinguish fraudsters who mimic good user's behaviors from real customers.

*DataVisor customers have reported up to **45%** increases in detection accuracy and false positive rates as low as **0.7%**.*

45%



STAGE 3

# Promotion Abuse

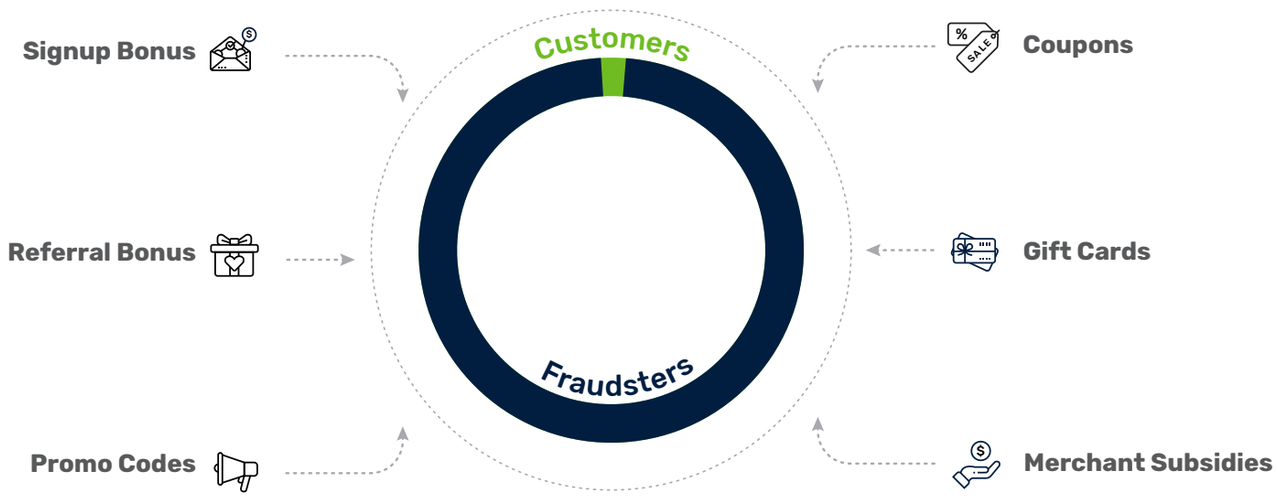
Promotion abuse is increasingly common, as fraudsters tap into digital channels to cash in on sign-up bonuses, discounts and other types of promotional offers. Bad actors can “game the system” by mass-registering fake accounts to take advantage of these offers with no intention remaining loyal to the brand. Without a scalable technology for detecting and preventing promotion abuse, profitability is at stake.

THE PROBLEM

# Fraudsters Are **Taking Advantage** of Promotions

Promotion abuse is hard to identify, because fraudsters use sophisticated tools such as automated bots to execute high-scale coordinated attacks. Rules-based systems are ineffective in detecting rapidly evolving attack techniques. As many businesses rely on promotions to attract new customers, promotion fraud can not only eat away profits — rigid fraud prevention techniques can impede a business's ability to engage new customers with promotional campaigns. This can hamper new market growth and competitiveness.

***** Forter 2018Q1 Fraud Attack Index report




**217%**

increase in coupon abuse from Q4 2017 to Q1 2018.*

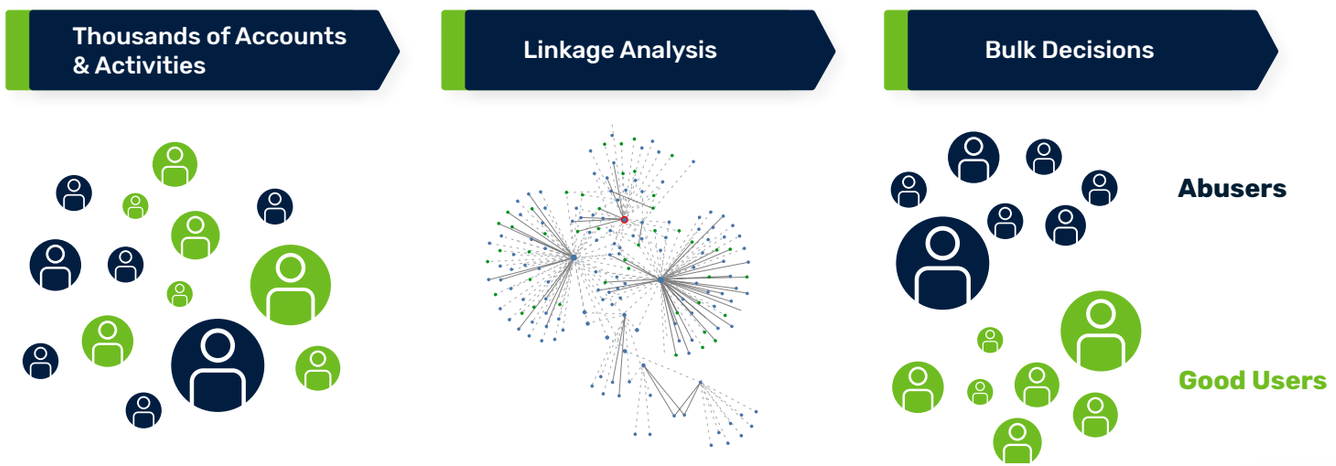
# THE SOLUTION

## Ensure Valuable Promotions Reach

# Real Customers

DataVisor's solutions leverage UML and linkage analysis to stop promotion abuse at scale. UML, deep learning and big data analysis enable proactive fraud detection for both known and unknown fraud patterns, delivering a 300% uplift in detection rates for some DataVisor clients, compared to legacy, rules-based solutions.

DataVisor's linkage analysis capabilities enable fraud and risk teams to manually review less-suspicious accounts for deeper insights and uncover hidden connections among linked entities. By doing so, DataVisor simplifies bulk decisions and provides up to 100X increases in review efficiency.




*One DataVisor customer saved* **$20 millions** *in fraud losses, while maintaining the ability to launch large-scale promotions that benefit their business by attracting new customers.*

$20M

STAGE 4

# Payment Fraud

Consumers store credit and debit card details to make payments online, and fraudsters are watching. If organizations fail to stop fraud in the first few seconds of a transaction, it's too late — the criminals have already succeeded. Yet accidentally declining transactions for good customers can impact reputation and profitability. Proactive, early detection is essential — and UML is the answer.

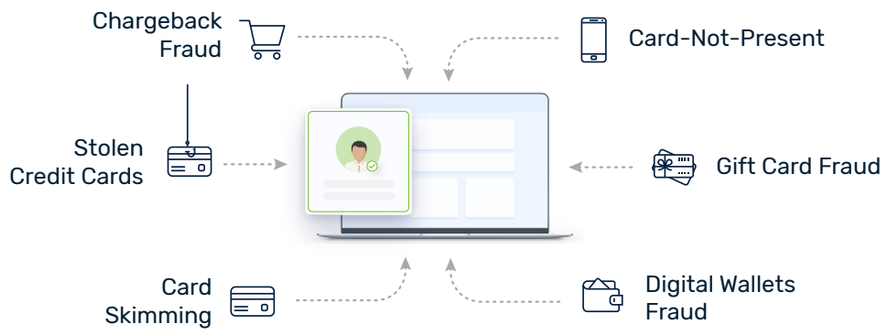
THE PROBLEM

# Hijacked Accounts and Data Lead to Fraudulent Transactions

Millions in chargebacks resulting from fraudulent transactions continue to slip through legacy detection systems. In fact, **77% of merchants** report their company has been a victim of some type of fraud, including stolen credit cards, card skimming, chargeback and gift card fraud.

Fraudulent transactions are extremely difficult to catch because the decision to block a transaction must occur within seconds. Yet accidentally declining a good user's transaction negatively impacts the customer experience, and this has a downstream effect on the company's profits. Customers lose trust in the brand and turn to competitors, causing financial losses and reputational damage.

*** Food Delivery Unicorn Uses DataVisor for Fraud-Free Global Expansion**




**Reactive & Slow Detection**

**Significant Fraud Loss**

**82%**

of merchants say their businesses are vulnerable to fraud from mobile transactions.*

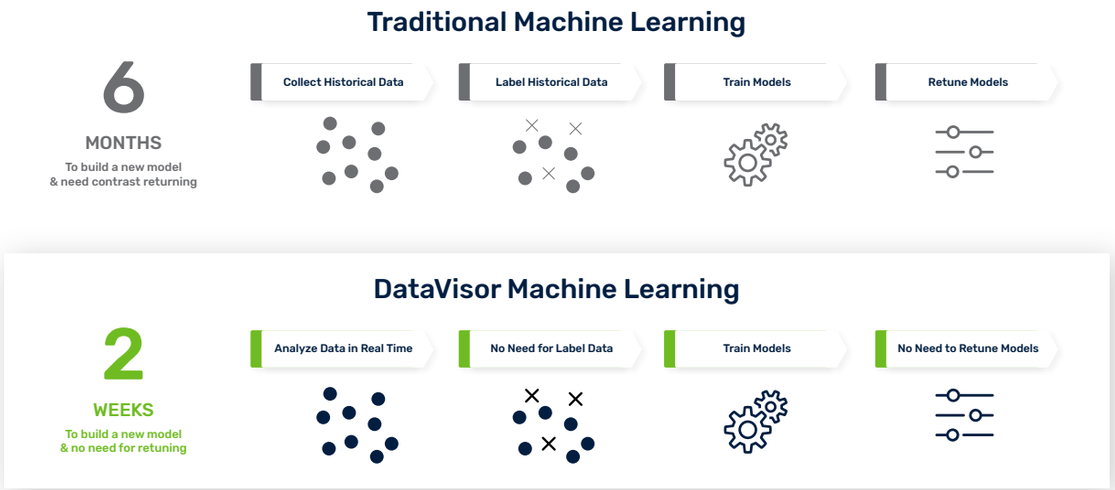
**77%**

of merchants report their company has been a victim of some type of fraud, including stolen credit cards, card skimming, chargeback and gift card fraud.*

# THE SOLUTION

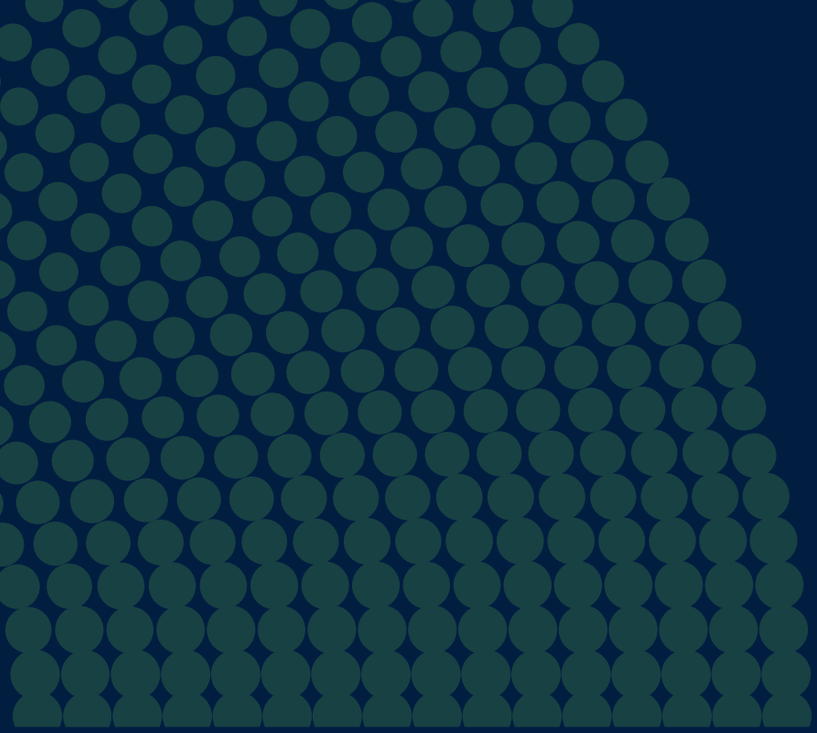
## Detect Payment Fraud in Real Time

DataVisor protects real-time payments, wire transfers and peer-to-peer transactions against sophisticated payment fraud at scale. Using UML to spot new and fast-evolving fraud patterns without the need for historic labels, large datasets or training time, DataVisor can detect and prevent fraudulent transactions in milliseconds, delivering rapid ROI. At the same time, legitimate transactions are processed without delays or complex verification processes, reducing false positives and removing friction from customer transactions.




*One DataVisor customer was able to detect 20% more fraud attempts with DataVisor compared to its existing solution, with* **94%** *accuracy, resulting in more than* **$12 million** *in savings.*

94%



STAGE 5

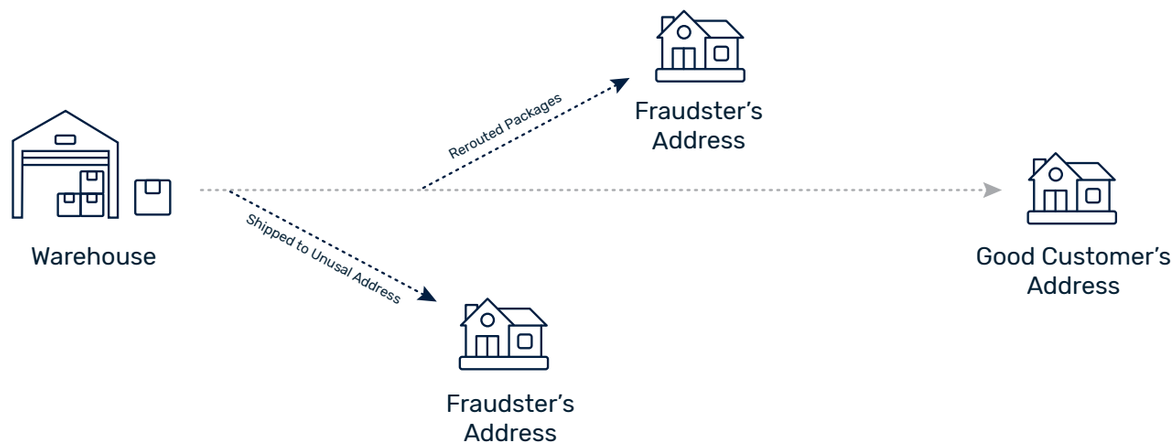
# Shipping Fraud

You may have heard of “porch-pirates” — criminals that steal packages off porches. But criminals are stealing packages via digital channels, as well, breaking into user accounts online and rerouting packages to steal the goods. As deliveries involve many customer touchpoints, preventing shipping fraud requires an omnichannel approach and the ability to monitor both structured and unstructured data in real time and across all customer touchpoints.

THE PROBLEM

# Stolen Credentials Lead to **Pilfered Packages**

Shipping fraud can occur over digital channels, before the packages ever arrive at their destination. Fraudsters use fake or stolen credentials to pose as customers and redirect deliveries to their own addresses. Experian reports that shipping fraud has increased by 60% in the Westrn U.S. in recent years, and with more and more online orders being placed since the beginning of 2020, that percentage will keep climbing. As people continue to avoid stores and order products for delivery, fraudsters will continue to cash in.




***** American Express Insights 2019 Digital Payments Survey

**37%**

increase in the rates of shipping fraud.*

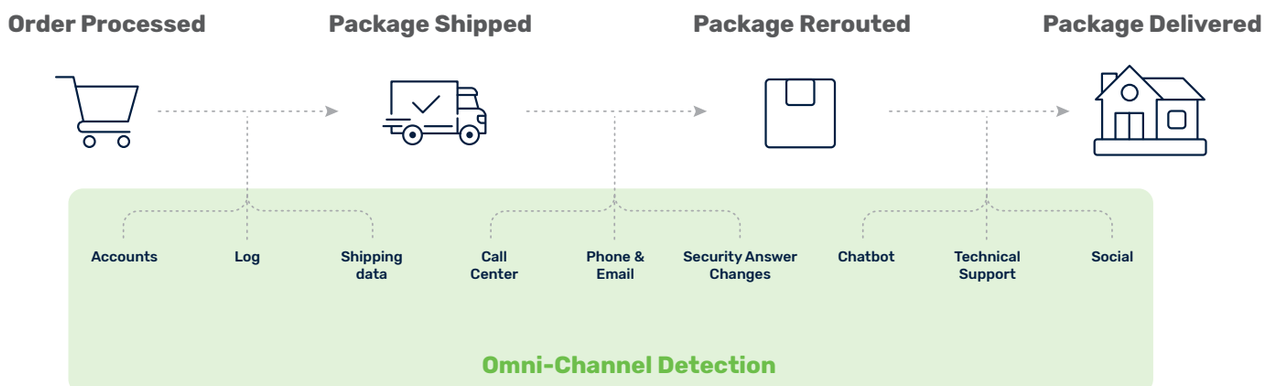
**60%**

increase in attack rates of shipping fraud in the Western U.S.*

THE SOLUTION

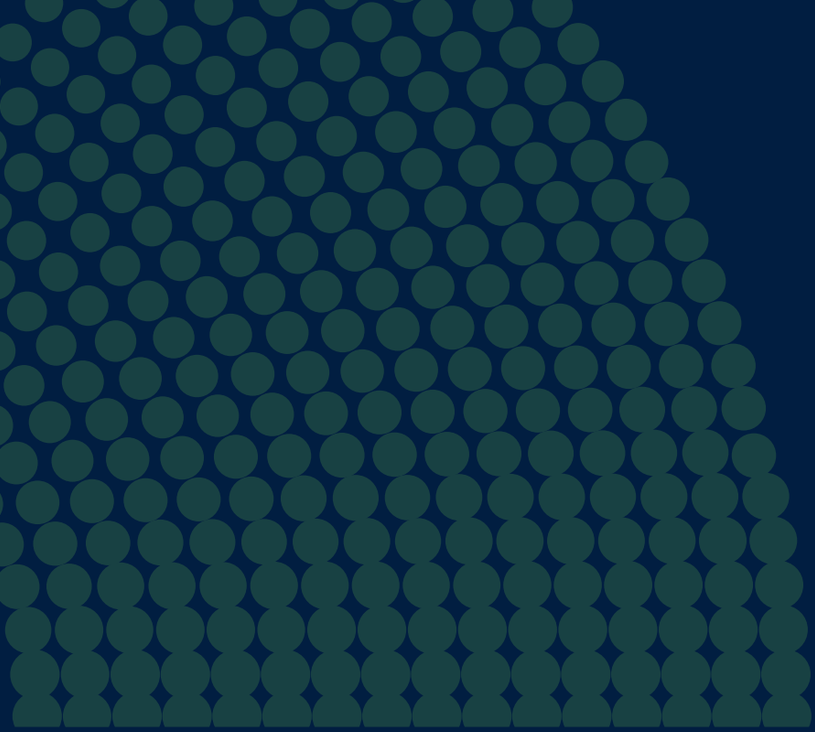
# Boost Detection with **Omni-Channel** Data

DataVisor analyzes customer behavior holistically, taking into account structured and unstructured data across every touchpoint, whether digital or physical. Information from the transaction, customer account, call center log and endpoint devices are analyzed together to create a digital fingerprint that helps to accurately distinguish legitimate customers from fraudsters with speed and precision. This omnichannel approach reduces false positives while increasing fraud detection accuracy, and enables fraud and risk teams to make contextual, informed decisions.




*DataVisor customers in the shipping industry have achieved up to **60%** increases in detection rates, and **40%** increases in review efficiency.*

60%



STAGE 6

# Content Abuse

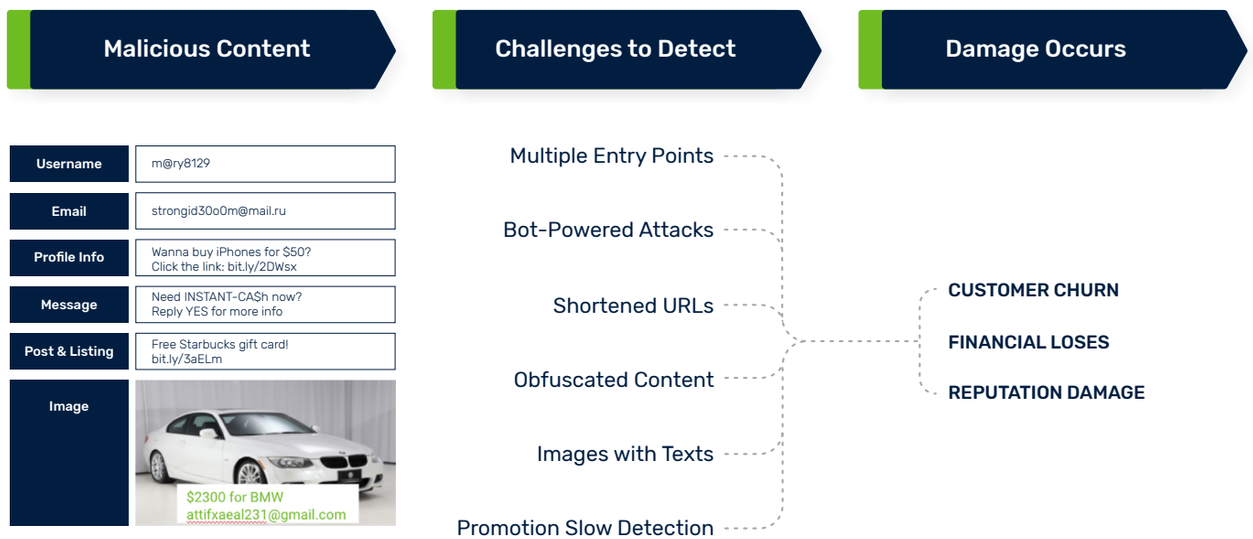
Businesses depend on high-quality content to build trust and engage customers. Unfortunately, content abuse is more common than ever, and online platforms that become polluted with toxic content suffer reputational damage and eventually drive customers away. AI-powered fraud and risk solutions can help put an end to content abuse.

# Malicious Content **Erodes Trust**

Content abuse is rampant on today's online platforms. Fraudsters create and disseminate fake or malicious content by posing — and posting — as real users, using multiple entry points and bot-powered attacks that are fast and adaptable, and increasingly difficult to spot. Abusive, fraudulent or deceptive user-generated content can severely damage a brand by eroding user trust, leading to churn.

Fraud solutions that rely on manually-created features, rules and blacklists can't keep pace with rapidly evolving content abuse techniques — only deep-learning models and holistic analysis can stop content abuse in real-time and help organizations avoid financial and reputational damage.

***** Experian Inc. and Internet Retailer, 2017 E-commerce Fraud Report




**50%**

of people who see a scam on a site are unlikely to return.*

**2%**

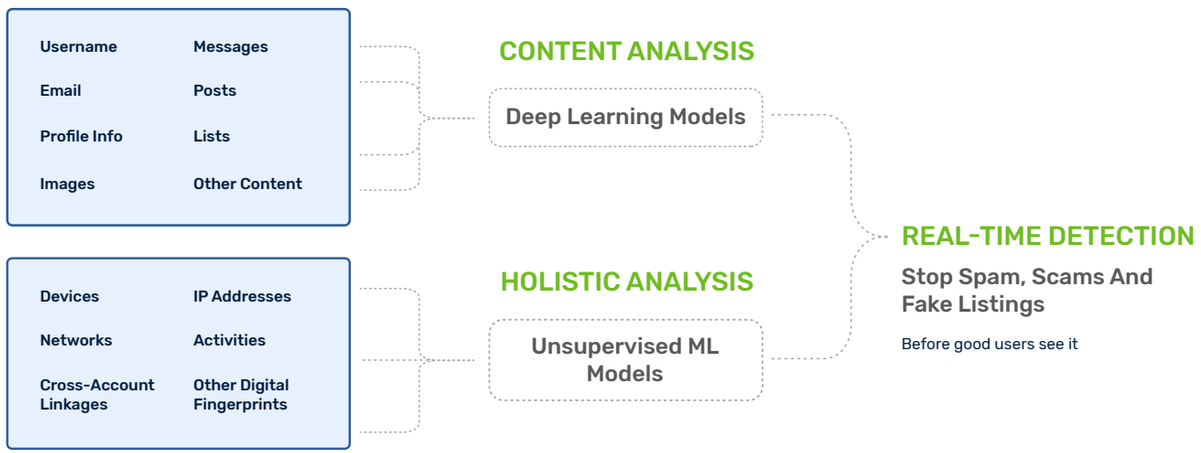
of all uploaded content is a scam.*

THE SOLUTION

# Prevent Fake Content from Being Posted

DataVisor's solutions detect spam, scams, fake listings and other malicious content in real time. Its patented UML technology holistically analyzes structured and unstructured data together for comprehensive content analysis, revealing shared patterns and uncovering hidden connections that point to bot-scripted or malicious content.

DataVisor reviews hundreds of linked bot or human-operated accounts simultaneously, making intelligent bulk decisions to automatically block the bad ones and purge damaging content. This not only helps maintain platform integrity, it reduces overhead, increases efficiency and bolsters the brand's ability to drive engagement.




*One DataVisor customer was able to stop **80%** of all spammers and scammers at sign-up.*

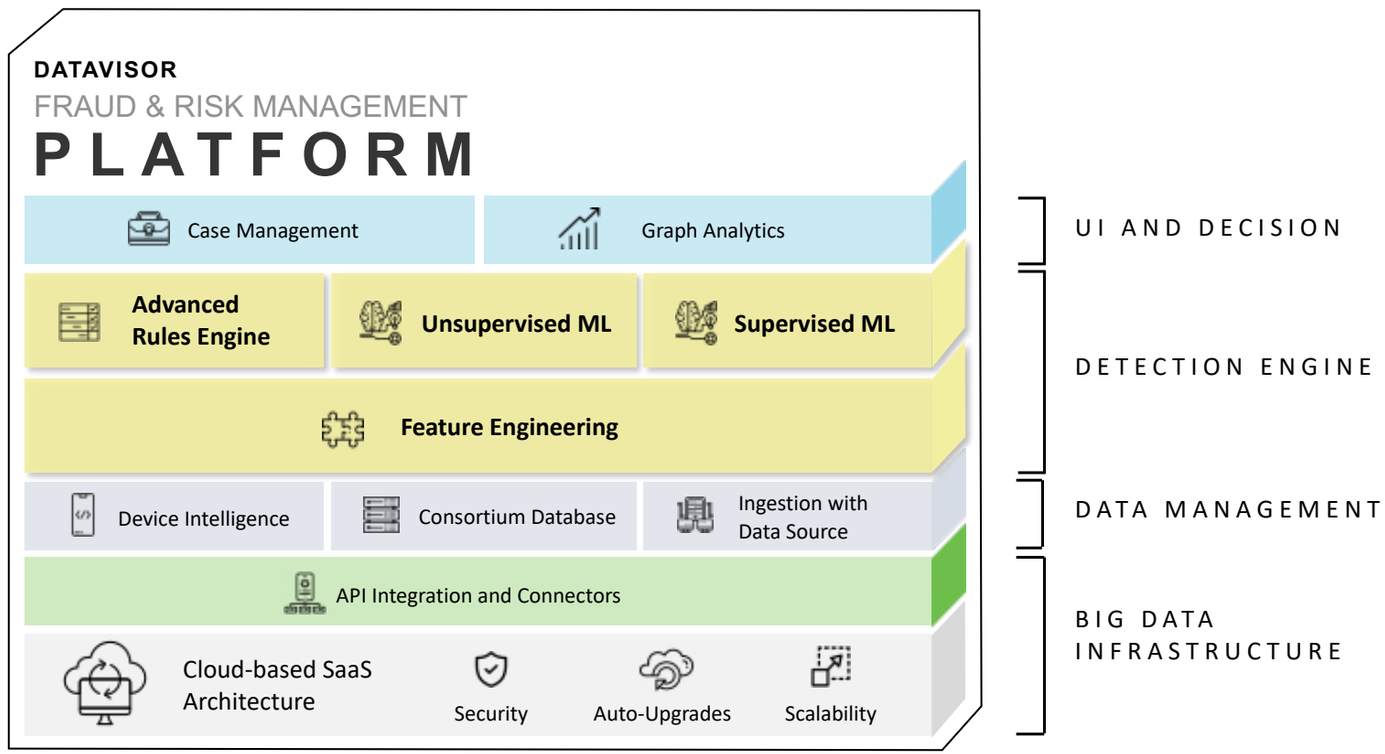
80%

# Comprehensive Detection Platform:
## Continuous Customer Lifecycle Protection

DataVisor delivers a comprehensive fraud and risk management platform that protects organizations from all types of fraud. Unlike point solutions that only address a particular use case or provide protection for a single point of entry, DataVisor assesses events across the entire customer account lifecycle by leveraging:

- Device intelligence
- Patented unsupervised machine learning technology and deep-learning algorithms
- An advanced rules engine powered by AI-enriched features
- A vast Global Intelligence Network (GIN) of more than 4.2 billion user accounts
- Advanced analytics and case management
- Advanced bot detection

With this unmatched collection of technologies and capabilities, DataVisor delivers the only fraud and risk management platform for continuous protection throughout the customer account lifecycle.



## 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 4.2B 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