Guard Your Online Marketplace Against Fraud

A DATAVISOR FRAUD PREVENTION E-BOOK

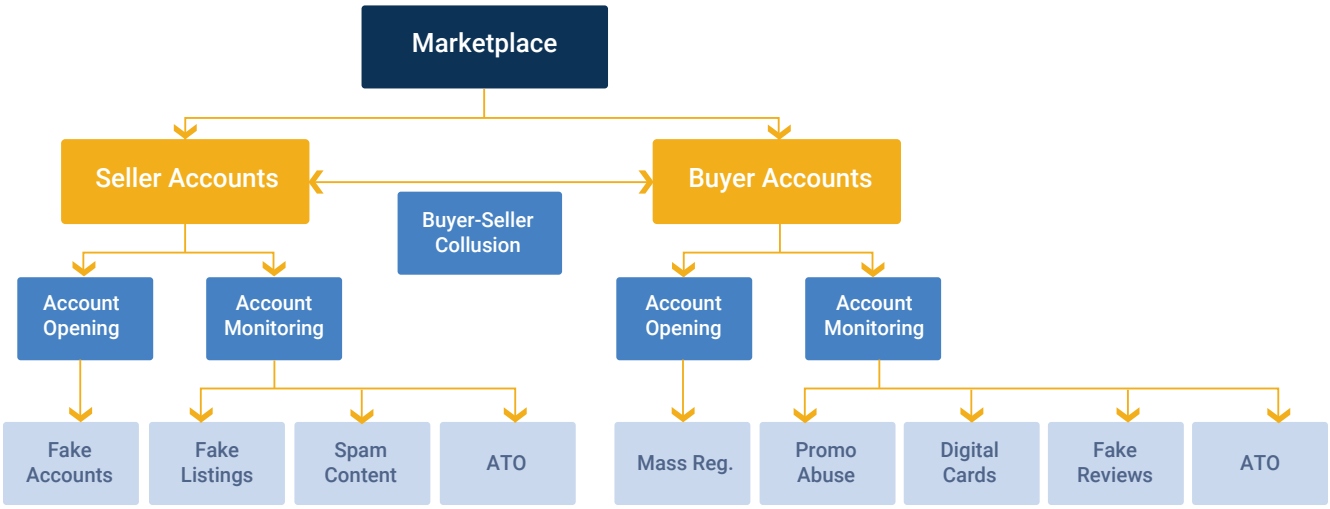
DATAVISOR

Contents

Marketplaces Today Face Numerous Challenges

The growth of online marketplaces has exploded in the last decade.

Marketplaces today face numerous challenges, challenges that cost these businesses billions of dollars every year. E-commerce companies, which includes marketplaces, lost an estimated 6.7 billion dollars in 2016 because of chargebacks due to fraud. A key challenge for online marketplaces is that much of the fraud and content abuse taking place on marketplaces go unreported. Unreported fraud and abuse lead to marketplaces not having a lot of reliable historical fraud data to draw from. Unfortunately, solutions that exist in the market today, whether it's rules or machine learning, require reliable historical labels. These solutions only detect fraud patterns that are recognized and has been seen before by fraud teams.



Apart from the financial losses resulting from fraudulent transactions and traditional chargebacks, marketplaces, because of their open business model, face reputational risk resulting from poor buyer-seller experience. The impact of fraudulent and malicious activity can be crippling, and often the end of traffic from users who have lost trust in the marketplace. Dual-sided marketplaces face threats from both buyers and sellers, making detection complex and time consuming. Tech-savvy buyers and sellers have access to tools to infiltrate the platform at scale and create a perception of legitimacy that fool even machine learning systems.

If you're a member of a marketplace trust and safety team, then you're already aware that marketplaces are grappling with rising levels of content abuse and fraud every day. What you may not be aware of is just how sophisticated marketplace fraud has become and the speed in which fraudsters can commit online fraud.

IN THIS E-BOOK WE EXPLAIN:

- How fraudsters compromise online marketplace platforms
- Attack techniques fraudsters are using
- Differences between fraud prevention tools

Fraud Begins with an Account

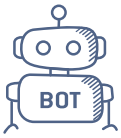
User accounts are the primary targets for fraudsters and are the most vulnerable feature of every online service. Fraudsters are constantly finding ways to exploit user accounts, and among the techniques fraudsters use are the mass creation of fake accounts, sleeper cells, and account takeover (ATO).

FAKE ACCOUNTS AND SLEEPER CELLS

Fraudsters use tools or scripts that automate the creation of fake accounts so that accounts are created in bulk quickly. The fake accounts often have similar attributes such as similarly formatted email addresses, same mobile device ID, and older web browsers. Fraudsters sometimes set up numerous sleeper cells; accounts that lie in wait, for months or years, before they are used for fraud. Fraudulent accounts incubate an average of 35 days before attacking.

ACCOUNT TAKEOVER (ATO)

Account takeover is where a fraudster takes over an account using the online credentials of the account holder. Account takeover is the fastest growing fraud threat for e-commerce sites. According to Javelin Strategy and Research, ATO losses tripled in 2018, reaching a whopping $5.1 billion. Fraudsters are using sophisticated tools and techniques to take over accounts such as:



- **Botnet** – A botnet is a network of devices where each device is running one or multiple bots. The devices and bots are controlled as a group to complete a variety of malicious activities. Fraudsters use botnets to hack accounts with weak passwords, and at a high velocity. Some bots can make millions of hacking attempts per hour.

- **Location Spoofing** – Fraudsters can hide the true locations of devices behind proxies, virtual private networks (VPNs), or data centers.

- **Device Emulators** – Fraudsters often use emulators to reset the Device IDs of mobile phones to avoid fingerprinting detections.

- **Brute-Force Attack** – A fraud method where fraudsters attempt to hack an account through trial and error. These hacking attempts are usually automated. The fraudsters use tools that generate usernames, passwords, and passphrases automatically until the correct ones are found.

Marketplace Fraud is Sophisticated

To effectively battle fraud, marketplace trust and safety teams must understand what they are up against and must also choose the right tools.

This section highlights what marketplaces are up against. We cover tools in the next section.

SCAMMING BUYERS WITH FAKE PRODUCT LISTINGS

Fraudsters have been selling counterfeit products and scamming buyers out of their hard-earned money long before online marketplaces even existed. However, modern fraudsters are finding innovative ways to scam people through fake product listings on online marketplaces. Product listing fraud is sometimes referred to as marketplace fraud. Fraudsters create fake product listings on marketplaces to scam money from buyers, pull a bait and switch, or phish for personal information.

- **Scam Money from Buyers** - To scam money from buyers, the fraudster will post an item for sale that is non-existent or counterfeit. The fraudster may list a popular luxury item like an automobile or a designer handbag. The buyer purchases the item but ends up either with a counterfeit or the item never ships at all.
- **Pull a Bait and Switch** - Sometimes fraudsters pull a "bait and switch" adding unrelated keywords to product listings. For example, a product listing would include a popular item (e.g. handbag or high-end jewelry) in the title and description. However, when an interested buyer clicks on the product page, the buyer is redirected to an unrelated advertisement or spam message instead.
- **Phish for Personal Information** - Some fraudsters use fake product listings to phish for personal information. These listings include links to third-party websites that collect information about buyers. Buyers end up submitting personal information such as email, password, credit card number, and address.

Product Listing Fraud is Difficult to Detect

Product listing fraud is difficult to detect because interactions happen primarily offline and many of the product listings are created and end quickly. Many marketplaces only connect sellers and buyers. So, payments and exchanging goods are up to the buyers and sellers to facilitate, often outside of the online marketplace. These offline interactions result in less information that can be tracked in an online manner for detecting fraud. Many marketplaces are already issue this by encouraging buyers and sellers to keep the interaction on their platform so they can be monitored for suspicious activity.

Fraudsters also use many techniques to mask their identity and activities. Device farms, anonymous proxies and VPNs, and auto-generated email addresses are some of the tools fraudsters use to prevent detection. Fraudsters can also fake their GPS location.

Product listing fraud is nuanced, and in many cases, coordinated. Traditional fraud prevention solutions are not designed to see the patterns and connections that indicate product listing fraud.

BOOSTING FAKE PRODUCT LISTINGS WITH FAKE REVIEWS

Once fraudsters have created fake product listings, they use the tools provided by marketplaces to boost the ratings and popularity of those listings. Some fraudsters also generate fake negative reviews to damage the reputation of other sellers on the marketplace. Marketplaces often get hit with sophisticated fraud campaigns that review multiple businesses at different times.

Fake reviews are a threat to marketplaces and the legitimate sellers who use them because of the damage that is done to their reputations. Retail juggernauts like Amazon and eBay use a variety of tactics to tackle the problem of fake reviews. For example, Amazon has features like verified purchase and algorithms to try to detect unnatural reviews. However, fraudsters are finding ways to bypass these measures such as hiring cheap labor to purchase the products and write fake reviews. Cheap labor can be found on crowdsourcing labor sites like CrowdFlower, Clickworker, and Amazon Mechanical Turk. There are also fake review underground communities via slack channels and dark web marketplaces.

Some fraudsters use bots to auto-generate a large number of fake reviews from templates. Detection is difficult because the fraudsters use residential IPs and routers to evade IP reputation detections. The fake reviews usually include same or similar content such as specific phrases, misspelled words, and word tenses. Traditional fraud prevention solutions can be programmed to detect similarities in the content of reviews. But fraudsters make changes to that content quickly; far more quickly than traditional fraud prevention solutions can handle. Unsupervised machine learning is an effective tool for detecting fake reviews because it can detect patterns in content and coordination between accounts.

DAMAGING MARKETPLACE REPUTATION WITH SPAM

When it comes to the trust and safety of both buyers and sellers, spam is a serious problem. Bad actors use the communication tools of the marketplace to send massive volumes of spam messages or to harass other users. If buyers and sellers perceive the marketplace to be toxic with spam, they will be inclined not to come back.

Some forms of spam are easy to detect. For example, a single account spamming marketplace users every two seconds would be detectable by even the most basic fraud prevention system.

But a thousand accounts sending a single spam message at different times per hour would be more difficult to detect. Some fraudsters go even further by adding spam to the profile description of fake accounts (profile spam) or creating sleeper cells that incubate for months before launching large-scale spam attacks. These spam messages could include offensive content or sell illicit services such as prostitution which puts the marketplace at risk by violating regulatory compliance and damaging brand reputation.

> *With the right tools, marketplace trust and safety teams can take steps to ensure that content abuse like spam and fake reviews are detected and prevented quickly.*

LOSING CASH TO SOPHISTICATED PROMO ABUSE SCHEMES

Promo abuse is not a new problem. But today, fraudsters are taking promo abuse to a whole new level. Some forms of promo abuse are easily detected. For example, Uber and Lyft sometimes offer free rideshares to new users. Some scammers create numerous new accounts to take advantage of the new user promotion. Auto-generated disposable phone numbers and email addresses with similar formats are used to disguise the fact that the accounts are for the same scammer. A basic fraud prevention system should be able to detect these simple fraud patterns e.g. similar phone numbers, same carrier, and similar email formats.

Some types of promo abuse are sophisticated, and fraudsters launch promo abuse attacks at a grand scale. For example, certain types of marketplaces offer new users a promotion where they will receive a cash bonus for creating a new account or referring new users who create new accounts. These types of promotions are a valuable target for fraudsters. One example of large-scale promo abuse involves more than 20,000 mass-registered accounts per day. These accounts were created specifically to accumulate "new user" cash bonuses. The fraudsters hid their activities behind fake device IDs and mac addresses. They also hid their device locations behind proxies and VPNs.

TARGETING E-GIFT CARDS AT HIGH SPEED AND SCALE

Fraudsters used to focus their sights solely on in-store physical gift cards. They would take some gift cards off the rack, write down the numbers, and get the codes off the back of the cards. Then they would use software to find out when the cards had been activated and if they have balances. Then the fraudster would jump into action stealing the balances of the cards. Some fraudsters still target physical gift cards, but the real money to be made is with e-gift cards.

E-gift card fraud is a problem for marketplaces year-round. But between Black Friday and Christmas, e-gift cards are a top target for fraudsters. Fraudsters are targeting e-gift cards, and at a scale and speed traditional fraud prevention tools cannot keep up with. For example, many fraudsters use botnets and brute force attacks to gain access and take over e-gift card accounts online.

> *GiftGhostBot is an example of a botnet used to execute a brute force attack on e-gift card websites. This botnet was discovered in 2017, and it can test up to 4 million gift card account numbers per hour. Most fraud prevention systems are not equipped to deal with coordinated brute force attacks of this magnitude.*

CREDIT CARD FRAUD IS NOT WHAT IT USED TO BE

Credit card fraud used to be simplistic. A lone scammer would use a stolen credit card to buy high-end products online. They may have stolen the number from a phishing scheme or perhaps they bought the number from a hidden marketplace on the dark web.

Lone scammers are still around and so is basic credit card fraud. But credit card fraud is increasingly a group activity. Fraudsters are coordinating- they are creating fraud rings and using tools to buy products online with stolen credit cards at a staggering speed and massive scale.

Fraudsters are using stolen credit card numbers to commit types of fraud on marketplaces that are complex and difficult to detect such as card testing and triangulation fraud.

Card Testing

Card testing is an example of how scammers have changed their tactics when it comes to using stolen credit card numbers. Fraudsters obtain credit card information in a number of ways. One way is to buy credit card details from a dark web marketplace. Another way is through malicious software that retrieves credit card and banking information from a personal device such as a laptop, tablet, or smartphone.

> *Fraudsters will first test the cards to make sure the stolen credit card numbers are valid and active by making small purchases. If successful, the fraudsters will move on to larger, more expensive purchases using the stolen credit card numbers. Fraudsters use bots or scripts to initiate automated mass card testing.*

In the first four months of 2017, card testing increased

200%

compared to the same period in 2016.

Triangulation Fraud

Triangulation fraud is complex; it involves stolen credit card numbers and three parties: A fraudulent seller on an online marketplace, a legitimate e-commerce website, and an unsuspecting legitimate consumer.

First, the fraudster purchases a stolen or synthetic ID and sets up a marketplace storefront. Then the fraudster purchases products from a legitimate e-commerce website using one or more stolen credit card numbers. The fraudster lists the products for sale on the online marketplace where legitimate buyers purchase the goods. The buyers are unaware that the goods were purchased with stolen credit cards and that the storefront is operated by a fraudster. And the legitimate e-commerce company ends up with chargebacks for the transactions involving stolen credit card details.

Not All Fraud Prevention Solutions Are the Same

Rules-based Systems

Rules-based detection systems are commonplace for marketplaces. They are easy to implement and effective at catching basic forms of fraud. However, they cannot detect large-scale, coordinated fraud and fraudsters can bypass rules easily. Rules-based systems are also prone to false positives and result in poor customer experience.

Risk Signals

Some marketplaces compliment their fraud prevention systems with risk signals like biometrics and device fingerprinting. A risk signal solution is easy to implement and provides real time reputation scoring. Two drawbacks to using risk signal solutions are that they are based on reputation history and become quickly outdated. These solutions are also unable to analyze patterns across multiple data sources and can be easily bypassed by tech-savvy fraudsters.

Fraud-specific Machine Learning Platforms

Most machine learning based solutions in the fraud prevention space take the supervised machine learning approach. These solutions are capable of higher accuracy than rules-based systems, and provide real-time scoring. Supervised machine learning solutions are effective at identifying patterns from known fraud. Like rules-based systems, supervised learning systems require reliable historical fraud data and models need to be trained with this data. However, by design, supervised machine learning approaches are unable to detect new or unknown fraud- the fraud must be discovered first, labeled, and then used for training (which can take weeks). So, these models are always a one step behind the latest fraud patterns and techniques.

General Purpose Modeling Platforms

General modeling solutions are available that companies can use for a variety of use cases including fraud prevention. These solutions are not designed for fraud prevention specifically, so they require domain knowledge. In order for fraud teams to utilize general modeling platforms, they must first understand what type of models and machine learning features are suitable for detecting a particular type of fraud. Also, general modeling platforms typically require the user to do all the data preparation work themselves. Data scientists and analysts spend up to 80% of their time cleaning and preparing data for analysis. General modeling solutions allow machine learning projects to be started quickly with automation and standardized workflows. General modeling solutions also abstract the complexity of machine learning tools such as TensorFlow, SparkML, and Scikit-learn. However, these solutions only detect known patterns and frequent retuning is required. Most of the algorithms available for general modeling solutions are based on supervised learning models.

Unsupervised Machine Learning

Another option for fraud prevention using machine learning is using the unsupervised machine learning approach. However, many misconceptions exist about the effectiveness and application of unsupervised machine learning. The majority of unsupervised machine learning solutions available today provide relatively simplistic anomaly detection. In general, simple anomaly detection has a high false positive rate and does not detect new or evolving attack patterns effectively. Simple anomaly detection can only alert against some suspicious data point or trend, which may or may not be a new attack pattern. Still, unsupervised machine learning models are effective at finding connections across all accounts and transactions. And they require less tuning and re-tuning compared to supervised machine learning models. However, not all such solutions are specifically designed for fraud; some require domain knowledge. And in some cases, these unsupervised machine learning algorithms are unable to scale to production level data sets.

Capabilities You Need in Your Fraud Prevention Toolkit

Some tools are needed so that trust and safety teams can scale fraud operations effectively to keep up with marketplace growth. Other tools are needed for day to day fraud prevention operations.

CAPABILITIES TO SCALE FRAUD PREVENTION

- **Rules Engine** – Creating and maintaining rules manually is time-consuming. And it's difficult, if not impossible, to add, modify and maintain the thousands of rules that would be needed to detect new forms of fraud. However, known fraud signals such as black lists, usage policies, and sanction lists are best implemented as a rule instead of a machine learning model. Many solutions today offer capabilities to automate the process of rules creation and management, allowing fraud teams to adapt to new forms of fraud and attack methods more easily.
- **Machine Learning Platforms** – Machine learning allows fraud prevention processes to scale with the growth of the marketplace. A system powered by machine learning provides greater coverage, better customer experience and improved work efficiencies than one that is based on rules alone. These solutions look at activities holistically and across users and hence capture suspicious activities that often evade human eye.
- **APIs** – Any fraud prevention solution must include APIs for easy integration. Sometimes an effective fraud prevention solution requires tools from multiple vendors to be combined into one comprehensive fraud prevention solution.
- **Pre-built Integrations** – A solution with prebuilt integrations will reduce the time it takes to connect data sources and third-party platforms.
- **Cloud Computing Power** – To scale your fraud prevention solution, you need massive computing and storage power.

CAPABILITIES TO STREAMLINE FRAUD OPERATIONS

An effective fraud prevention solution not only scales with the growth of your marketplace but also provides tools necessary for day to day fraud prevention operations. Here are a few tools that should be included in every fraud prevention toolkit.

- **Real-time Scores** – Real time, transparent scores should always be part of your fraud prevention toolkit. A risk score solution should not be a black box and should include understandable reason codes.
- **Dashboard** – Detailed reporting and interactive visualizations help trust and safety teams understand why transactions are flagged as fraud and the types of fraud your marketplace is encountering. Real-time alerts that surface potential fraud in real time is imperative as fraudsters launch high velocity attacks that can result in huge financial losses and reputation damage within a short time window .
- **Global Digital Signals** – An effective fraud detection system needs an intelligence network that applies deep learning algorithms to an industry-wide set of digital data. The network should provide real time insights on risk based on a wide range of data including IP addresses, geographic location, email domains, mobile device types, operating system, browser agents, and phone prefixes.

Conclusion

FRAUDSTERS ARE TARGETING ONLINE MARKETPLACES RIGHT NOW

Card testing, fake product listings, fake reviews, spam, and many other types of fraud and content abuse are happening right now on online marketplaces all over the world. Marketplaces are already losing the trust of sellers and buyers, and may not even know it. Many marketplace sellers and buyers don't report fraud and content abuse- instead, they leave.

How Can DataVisor Help

Marketplaces don't have time to wait when it comes to implementing a modern and effective fraud prevention solution. DataVisor is a machine learning powered solution designed specifically for proactive fraud detection and prevention.

Speed to Detection

DataVisor's proprietary unsupervised machine learning algorithms can scale, analyzing billions of users and accounts in real time without requiring large datasets and historic loss experience labels for training, tuning and retuning models resulting in faster time to detection and ROI.

Fast Integration

The DataVisor platform features a Detection API that allows marketplaces to integrate with their workflow within weeks. DataVisor integrates with cloud services such as AWS, Azure, Alibaba Cloud, and Google Cloud for scalability and speed.

Advanced Analytics

Threat console allows customers to monitor the threat level within its platform, including high risk fraud attacks and the detection history.

About DataVisor

DataVisor is the leading AI-based fraud detection platform that proactively identifies and stops known and unknown fraud and restores trust in digital commerce. Combining advanced fraud analytics and intelligence network of more than 4B user accounts globally, DataVisor protects businesses against account opening, account takeover, user acquisition and transaction fraud initiated by fraud syndicates and sleeper cells. Using proprietary unsupervised machine learning algorithms, DataVisor helps business detect emerging fraud patterns without the need of historical loss labels. The DataVisor solution is deployed across a variety of industries, including financial services, e-commerce, social platforms, telecom and insurance. Depending on customer requirements, DataVisor solution can be deployed over cloud or on-premise, and can be integrated as a stand-alone application or as one of the fraud signals.

For more information on DataVisor solutions:

info@datavisor.com

www.datavisor.com

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

DATAVISOR

Guard Your Online Marketplace Against Fraud

A DATAVISOR FRAUD PREVENTION E-BOOK

DATAVISOR