Arkose Labs

PROTECTING SHOPPER TRUST

The Role of Early Fraud Detection in eCommerce Account Security

EBOOK

INTRODUCTION

As the world was forced into a new way of buying and selling goods, ecommerce transformed from a piece of the shopping experience to the epicenter. Today's highly competitive online marketplace has forced many merchants to embrace the digital transformation and look for innovative ways to make shopping effortless across multiple channels.

As merchants strive to convert one-time purchasers into repeat customer accounts, trust is quickly becoming the modern currency of commerce. That trust is built on a secure environment for customers to interact with. Customers expect a seamless experience, but also want assurance they can safely shop, interact, and store their credentials on your platform. As digital footprints expand, protecting customers' identity becomes just as important as securing transactions.

But while merchants invest in technology that builds up trust, fraudsters are investing in new ways to break it down.

The face of fraud has forever changed with the digital transformation. Traditionally, retailers only worried about stolen credit cards. Today, leaked credentials are the new credit card, opening the door to a myriad of fraud and abuse spawned by compromising existing accounts or setting up fake ones using others' credentials.

These entry points are now fair game for fraudsters to launch evermore nuanced attacks such as credential testing, account takeovers, gift card fraud, and inventory hoarding. To combat persistent attackers and build a platform users can trust, retailers need a modern approach to early fraud and abuse detection.

THE NEW FACES OF FRAUD IN ECOMMERCE

Cybercrime is a legitimate business, now more profitable than all of the world's drug trade combined. This is not the work of a few lone fraudsters. A complex ecosystem of data brokers, fraud farms, and money mules make it possible to deploy large-scale, organized attacks and make big profits. Fraudsters keep costs low by using a combination of trained bots and employing cheap labor. Motivated purely by money, they are ruthless in their pursuit of infiltrating ecommerce platforms.

The new faces of fraud might not be the measurable ones seen on a profit & loss statement. Here's how attackers are profiting from retailers today and warning signs that sophisticated attacks need to be addressed where they originate.

Credential Stuffing & Account Takeovers

Credential stuffing is at an all-time high as attackers seek to corrupt the huge range of new accounts created during the pandemic. In fact, credential stuffing attacks doubled in the second half of 2020 across the Arkose Labs global network. Once credentials have been verified by mass automated attacks, the consequences are far-reaching.

Warning Signs:


Changing user security credentials


Loyalty point theft


Fraudulent purchases


Uptick in user support volume

Fake Account Registrations

Seamless registration processes ask less information from customers upfront, which makes it increasingly difficult to determine if a new customer is who they say they are. Mass stolen credentials have made it easier than ever to create fake accounts to abuse promos, disseminate spam, and launder money. Attackers may deploy bot-driven credential testing or employ low-cost human resources to carry out more nuanced attacks that circumvent bot detection solutions.

Warning Signs:


Promo abuse


Spam on peer-to-peer marketplaces


Coupon harvesting


Fake listings/reviews


Gift card fraud

Scraping & Inventory Abuse

Fraudsters don't always incur retailers direct losses. Attackers scrape sensitive business data off sites--such as inventory availability or pricing details--to sell them on third party sites or to competitors. Inventory hoarding is another way of inflicting harm without any need to complete a transaction. Automated scraping tools are adept at circumventing detection by obfuscating and randomizing device, network and IP characteristics.

Warning Signs:

- Overwhelming networks with bots
- Customer denial of inventory
- API attacks
- Third-party resale of high-valued inventory

ASSEMBLING A NEW FRAUD-FIGHTING TEAM

As traditional fraud prevention focuses primarily on the payment stage, these new forms of fraud aren't always rooted out before significant damage has been done. Nowadays, waiting to detect fraud at the time of payment is simply too late.

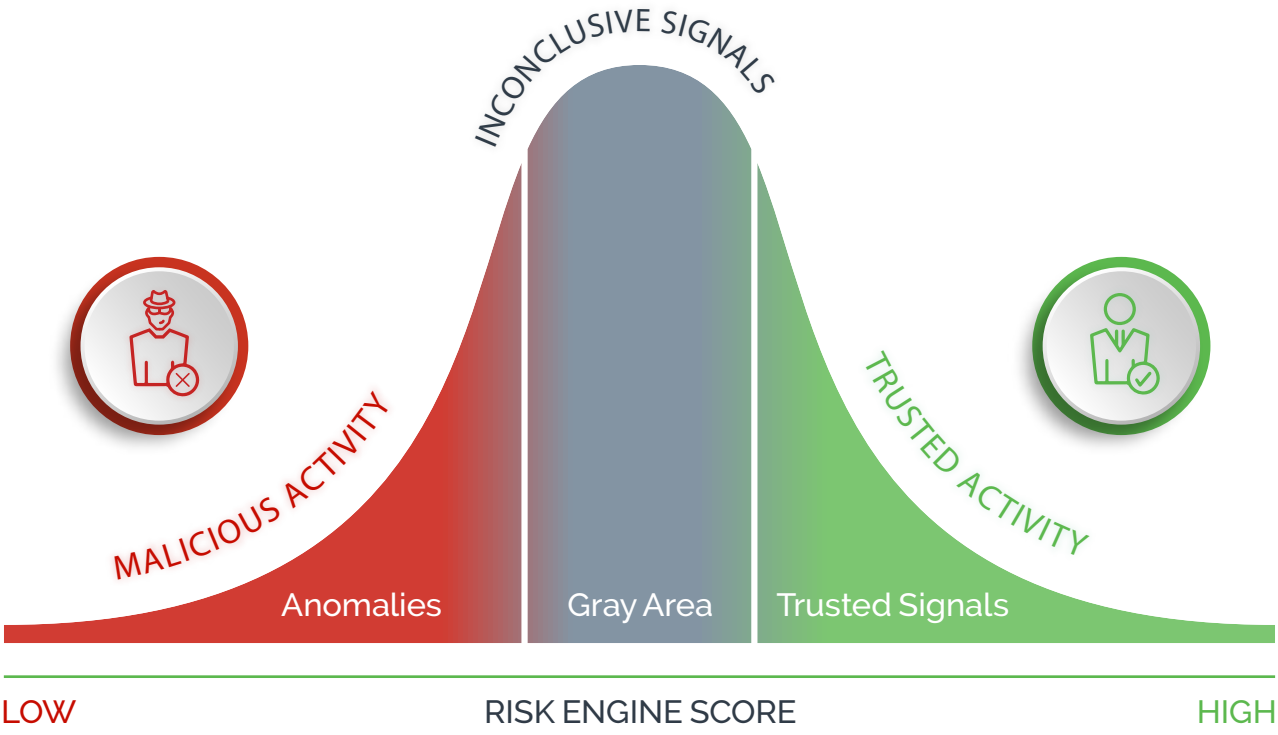
Fraud Costs Multiple Teams

- Revenue opportunities lost to user security hurdles
- Promotional budgets drained by promo abusers
- Infrastructure costs from high volume attacks
- High cost of authentication tokens
- Reimbursing lost funds from compromised accounts
- Extra transaction fees from attacks on payments

That means fraud can no longer be a problem solved by fraud teams alone. These increasingly nuanced and hard-hitting attacks cost teams across fraud, information security, and growth in poor completion rates, compromised user accounts, and authentication and infrastructure costs.

Teams can fight fraud together by catching attacks where they begin rather than after money is exchanged. Login & registration stages are better places to detect, challenge, and analyze fraud without hurting the good user experience. It requires the right level of targeted pressure on fraudsters to filter out mass scale fraud at earlier checkpoints, so you can have greater confidence it's a real customer at checkout.

THE INCREASING GRAY AREA IN RISK CLASSIFICATION



As fraud has increasingly far-reaching impacts on retailers, there is more pressure than ever to accurately decipher honest users from malicious actors. Data-driven decision engines are geared towards extremes, looking for users that display clear 'trust' or 'mistrust' signals. However, in a world where digital identities have been corrupted and intent can be faked, risk teams are left to make black and white decisions based on signals that are too gray.

This expanding gray area stems from a combination of new behavior patterns from good customers and sophisticated spoofing and cloaking techniques from fraudsters leveraging stolen data. For good customers, if one factor is off, for any number of legitimate reasons, they can get caught in the net and throw the whole model off. Meanwhile, fraudsters understand how decisioning models work and use this knowledge directly against the retailers they attack. The gray area is where costs increase, resources are expended, and decision-making confidence waivers. As risk engines catch up with new fraud patterns, retailers shouldn't have to choose between accepting fraud as a "cost of doing business" or putting additional checkpoints in front of good customers.

The Consequences of Misclassifying Gray Signals

False Negatives

- Impacts revenue & margin
- Increases chargebacks
- Perpetuates the fraud problem

False Positives

- Inhibits sales & growth
- Frustrates users
- Increases operational costs

While false positives & false negatives come with the territory, these problems will perpetuate when a growing portion of your traffic is unclear and there is no user-friendly method of secondary screening.

Retailers naturally lean towards minimizing false positives to reduce the impact on conversions. However, the more successful attacks take place, the better the fraud community's ability to launch future attacks. This is why fraud attacks continue to rise despite investments in anti-fraud measures deployed by many commerce platforms. Retailers must stop the cybercrime cycle of success in its tracks.

THE ARKOSE LABS APPROACH

To effectively manage fraud and abuse in this rapidly evolving ecosystem, ecommerce platforms need a long-term approach that evolves with new attacks and eliminates fraudulent traffic long before the checkout. Since abuse can only be sustained when the incentive outweighs the cost, retailers need a solution that makes attacks uneconomical for fraudsters without impacting good customers.

Arkose Labs has a vision for a world of zero-tolerance for fraud. This approach is based on the following core principles:

Undermine the economic incentive of fraud so it ceases to be a lucrative business. While there is still money to be made, fraudsters will find a way to do so by switching tactics, techniques, and targets. That is until their profits are slashed by prevention which renders attacks time-consuming, difficult, and expensive.

Know fraudsters' attack tactics and meet them with tailored pressure. When the tell-tale signs of fraud are present, the right amount of pressure is vital to stamp out automated and fraud farm driven attacks at scale. By distinguishing between human attackers at scale, bots, and genuine customers you can direct the right type of pressure to undermine the cost economics of each attack tactic.

Stop fraud long-term, beyond defecting individual attacks. To address fraud in the long-term, controls need to be adaptive, and continuously evolving. When you can detect the behaviors of motivated fraudsters and use secondary screening that moves the goalposts on them, attacks cannot learn to circumvent them at scale.

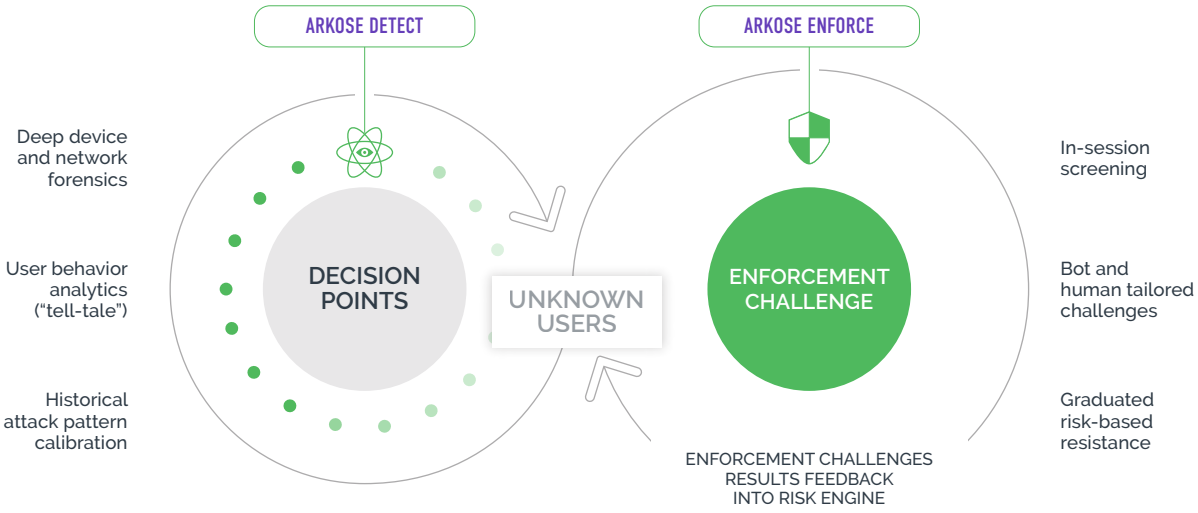
Shift the attack surface away from the businesses fraudsters target. Independent verification of identity avoids draining in-house fraud prevention resources and provides a buffer between the fraudsters and the sites they are so practiced in attacking.

Rather than playing a constant cat and mouse game with fraudsters, retailers need a long-term approach to disrupt fraud and put a stop to these large scale attacks.

ARKOSE LABS FRAUD AND ABUSE PREVENTION

The Arkose Labs Fraud & Abuse Prevention Platform combines real-time intelligence, rich analytics, and adaptive step-up challenges to progressively diminish the profitability of attacks while adpting to

veolving attack patterns. Working at the digital front-end, it provides a proactive layer of early detection to root out fraud, enhance your overall risk models, and make your platform a safer place to transact.



Arkose Labs Protects Ecommerce Against:

Account Takeovers

Mass Fake Accounts

Scraping

Fake Reviews

Carding

Inventory Hoarding

Credential Stuffing

CASE STUDY: eCommerce Giant Cuts Fake Accounts in Half

Challenge: A major ecomm platform was experiencing large scale bonus abuse on new accounts. Bad actors would employ bots or fraud farms to create new accounts at scale, which also spawned downstream abuse including fake reviews, selling fake items, and sending spam messages to other users.

Solution: The ecommerce platform chose Arkose Labs fraud and abuse prevention to compare to its homegrown solution on login and registration flows.

Results: With Arkose Labs, they saw a 54% reduction in fraudulent new accounts plus significant reduction in downstream abuse and chargebacks from early detection.

WIDENING THE LENS ON FRAUD PREVENTION

Many ecommerce platforms are experiencing mounting demands on their time and budgets, while fraud losses continue to rise. Both retailers and consumers are increasingly recognizing the scale of the problem as registrations and consumer accounts are under attack across all customer touchpoints. Rather than waiting for fraud to show up at the transaction stage, we must take a wider lens on fraud protection to create a secure experience regardless of if and how they transact with you.

Retailers need a next generation approach to surpass attackers' games and sabotage their efforts to undermine consumer trust. By successfully shrinking the growing gray area between trusted and malicious signals early, ecommerce platforms can take a zero-tolerance to fraud, slash rejection rates for good users, and create a secure & trusting experience with confidence.

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Offices:

San Francisco Brisbane London

Schedule Demo