Arkose Labs

THE FUTURE OF FRAUD vs. FRICTION

Next Generation Authentication for Secure eCommerce

WHITEPAPER

INTRODUCTION

Online and mobile commerce is growing at breakneck speed across the globe, with face-to-face transactions increasingly being replaced by digital interactions. The global eCommerce ecosystem is buzzing with activity round the clock as consumers take advantage of the convenience of accessing a huge array of goods anytime and anywhere.

The rise of digital commerce is redefining relationships between retailers and their consumers. No longer able to rely on in-store interactions to build relationships and encourage repeat business, businesses are left looking for new ways to forge strong bonds with consumers. While it has never been easier to tap into a wider customer base, it is a highly competitive marketplace and online retailers need a differentiated offering to cut through the noise.

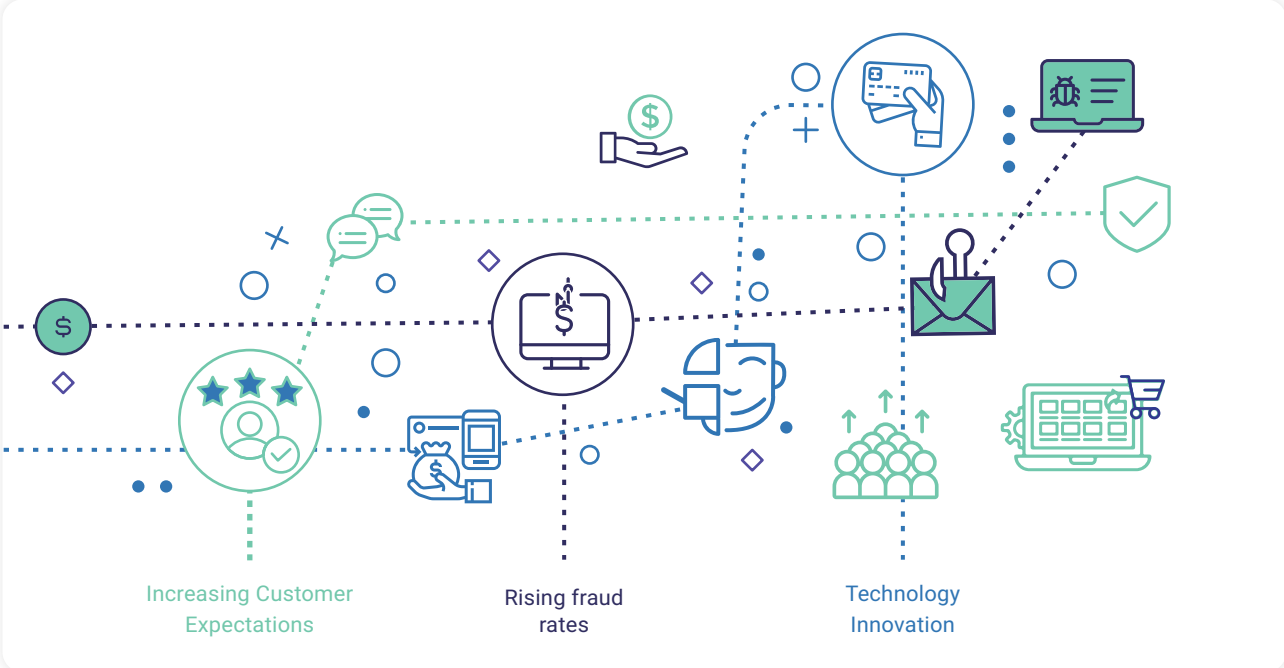
Retailers are leveraging technology to boost sales and deliver stand-out customer experience, for example, one-click payments, personalized shopping recommendations, and the rise of social commerce. Customer expectations have evolved, with digital-savvy customers now looking for instant access to goods and services tailored to their specific needs.

However, in the meantime, fraud rates are rising and security departments are battling against increasingly complex attacks. These attacks deliberately exploit efforts made by ecommerce departments to please online shoppers and with many merchants prioritizing conversion rates over tackling fraud, this can inadvertently make the industry a prime target for fraud. With rising fraud losses and increasing incidents of damaged customer trust due to fraud, it is time for the ecommerce industry to reassess the correct balance between strong anti-fraud measures and offering a seamless customer journey.

ECOMMERCE'S BATTLE WITH FRAUD VS FRICTION

Fraudsters see the retail industry as a prime target for the monetization of stolen data in the wake of the large-scale data breaches that are occurring with increasing frequency. Cybercriminals are launching an array of attacks that include credential testing using fake account registrations, account takeovers and fraudulent payments using stolen credit card details.

eCommerce companies, on the other hand, find themselves caught between the competing forces of rising fraud levels and rising customer expectations. Modern consumers demand security, however, show little tolerance for any delays or barriers in their online shopping experience.



In the first generation of solutions fighting the rising tide of fraud attacks on the ecommerce sector, the focus was on blocking bad actors – often to the detriment of legitimate consumers. This resulted in a major backlash, with 'friction' in any shape or form deemed the nemesis of commercial success.

These legacy fraud solutions have largely been ripped out or replaced, with the current focus on risk-based

analysis that works behind the scenes. This has led to far more sophisticated analytics which can derive insight into the true intent and identity of a user based on the devices they use, where they transact from and the behavior they display.

However, over time this approach has been compromised by sophisticated and organized fraud operations which use knowledge of fraud detection parameters against the businesses they attack. The zero-friction approach to fraud detection is backfiring, with rising levels of fraud impacting both company profits and damaging the individuals who get stung on retail websites and apps.

At a time when technology has evolved significantly – both on the offensive and defensive side – is it time to reassess the role of friction in achieving the optimal balance between user experience and security online?

THE INCREASING GRAY AREA IN DATA-DRIVEN FRAUD DETECTION

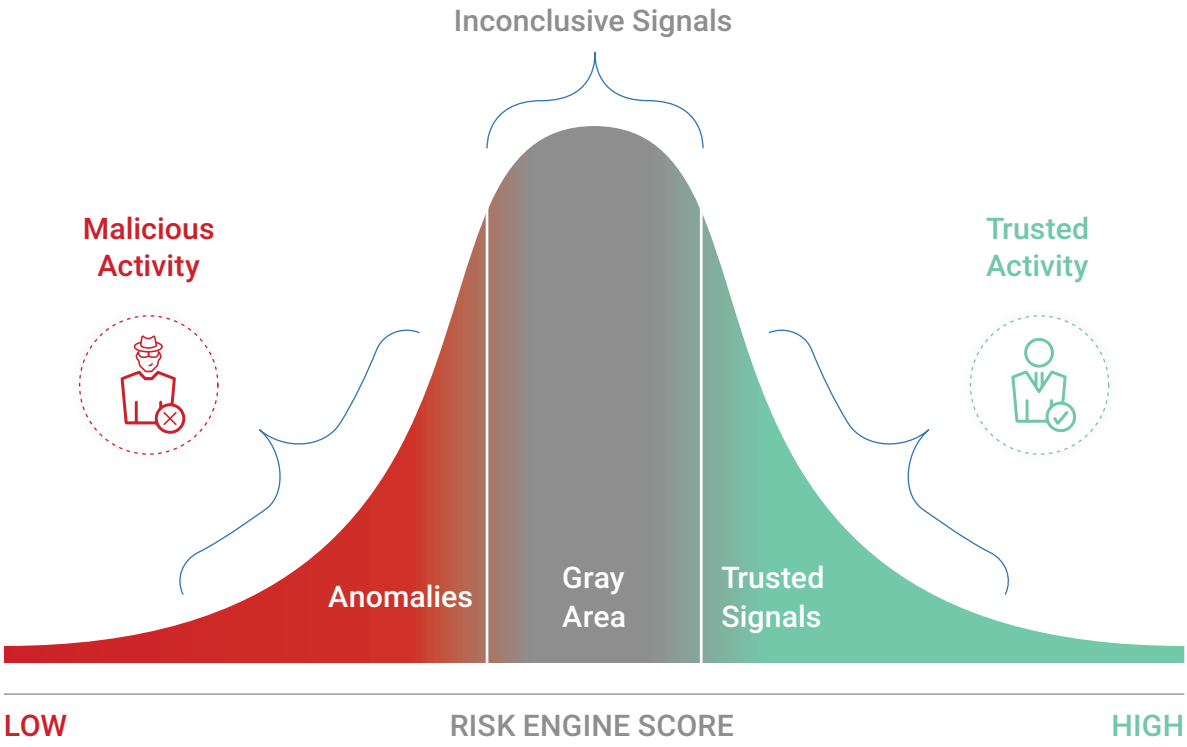
Fraud prevention in recent years has honed in behavioral and digital identity analytics to differentiate between good and bad traffic in a way that is transparent to the user. These data-driven decision engines are geared towards extremes, looking for clear 'trust' or 'mistrust' signals. However, if one factor is off, for any number of legitimate reasons, it can throw off the whole fraud prevention model. Consumer behavior is evolving quicker than ever before and fraudsters are increasingly skilled at mimicking legitimate behavior. As a result, there is a growing gray area between activity that is recognized as trusted and that which is flagged as fraud, with fraudsters exploiting this uncertainty at scale.

1. **The gravity of the data breach problem** has now entered a distinct new stage. 2019 has been the most prolific on record and the variety of data now available to fraudsters has reached new heights. Beyond the data, typically associated with data breaches, fraudsters can now access information specifically used to trick data-driven fraud prevention systems, such as cloned device fingerprints and residential IP addresses associated with a user.

2. **Businesses are coming up against increasingly nuanced attacks** that are orchestrated using advanced tools and techniques to evade defenses. Fraudsters use multi-step attacks which do

not initially reveal the end goal and they are skilled at covering their tracks. They have access to increasingly sophisticated tools, for example, smart bots which mimic human behavior accurately to trick behavioral biometric tools and sophisticated obfuscation technologies that facilitate Single Request Attacks. A comprehensive global cybercrime ecosystem also provides access to fraud sweatshops to carry out large-scale attacks from real humans.

3. **Data-driven fraud prevention** often does not account for unexpected behavior from good consumers. As an increasingly mobile consumer base travels internationally, transacts from different devices and uses VPNs for non-malicious reasons, it can quickly move genuine users into the gray area between trusted and suspicious.



HOW THE GRAY AREA PUTS BUSINESSES IN THE RED

Fraud prevention teams are experiencing increasing levels of uncertainty when analyzing traffic on their sites, and this is typically dealt with in ways that are problematic for the ecommerce business and the consumers they serve.

✕ False Negatives	✓ False Positives
Companies that prioritize order acceptance and conversion rates above everything else can develop a certain tolerance to fraud on their websites and apps. If fraud rates stay below a certain threshold, it is seen as the "cost of doing business". When anti-fraud systems fail to identify malicious activity, however, this can have seriously unpleasant consequences for the individuals involved. Additionally, it perpetuates the fraud problem long-term. It proves the financial incentive for cybercriminals to continue attacks; the proceeds are used to invest in fresh data and more sophisticated tools; and it allows fraudsters to share information on successful tactics.	Retailers who deal with uncertainty by blocking transactions or asking users to jump through hoops to prove who they are, will quickly alienate consumers and lose business to competitors. Additional manual reviews and fielding enquiries from customers with blocked transactions puts undue pressure on in-house teams and leads to spiraling costs. With increased operational costs and damaged customer relations, the long-term profitability of a company in the cut-throat ecommerce market is put under threat.

RETHINKING FRICTION TO SUCCESSFULLY NAVIGATE THE GRAY AREA

As good consumers' behavior is evolving, and fraudsters are able to mimic legitimate consumer activity more effectively than ever before, the time has some to rethink the role of friction within an effective ecommerce fraud defense mix.

To combat the growing gray area in online fraud detection, ecommerce companies need a secondary screening step to work hand-in-hand with risk-based assessments. Embedding targeted friction in the workflow is a smarter way to improve the security and user experience for good customers, while providing businesses with invaluable insights into the true intent of users.

STEP ONE

Risk-based Assessment

Risk-based authentication which profiles user activity behind the scenes, throughout the customer journey, is a vital component of any fraud prevention strategy. However, considering the limitations of this stand-alone defense, risk decisioning should avoid blocking any activity out of the gate and potentially turning away legitimate users. By combining risk-based assessments with secondary screening, good customers are offered a way to prove they are legitimate before they are blocked.

STEP TWO

Classify the Risk Type

When the decision engine detects risky activity, this must be classified by the type of threat in order to inform subsequent authentication steps. eCommerce companies are facing attacks across the customer journey ranging from early-stage credential testing to payment attacks aiming at more immediate monetization. The attack mix includes automated bots of differing sophistication, large-scale attacks originating from teams of low-skilled humans in sweatshops, and attacks from more skilled lone fraudsters. By classifying and triaging traffic based on its risk level, the suspected fraud type, and the attacker profile, this lays the ground for highly effective secondary screening.

STEP THREE

Block All Automated Traffic

All automated traffic on eCommerce sites and apps is malicious and with the correct screening in place, all malicious automated traffic on ecommerce sites is detectable – no matter how sophisticated the bot. Traffic that shows red flags during the risk-based assessment can be presented with challenges, such as visual puzzles, that are simple for humans to solve but cause automated attacks to spontaneously fail. By focusing on fun challenges that do not detract from the user experience or throughput rates, this is a highly effective acid test to root out automated attacks without ever blocking real humans. To avoid fraudsters scripting past this step at scale, use images that cannot be categorized by low-cost image processing tools and keep moving the goalposts with puzzles that are constantly evolving.

STEP FOUR

Incremental Challenges to Target Malicious Humans

For traffic that shows tell-tale signs of originating from organized sweatshops or lone fraudsters, increasingly complex challenges are needed to sap time and resources. Attackers are looking for the quickest and easiest route to monetization and will quickly abandon attacks when it becomes impossible to attack at scale while still preserving return on investment.

Rather than shying away from friction and allowing the growing gray area in fraud detection to undermine secure commerce on websites and apps, businesses need to embrace a dual approach which validates risk-based data insights with intelligent step-up authentication.

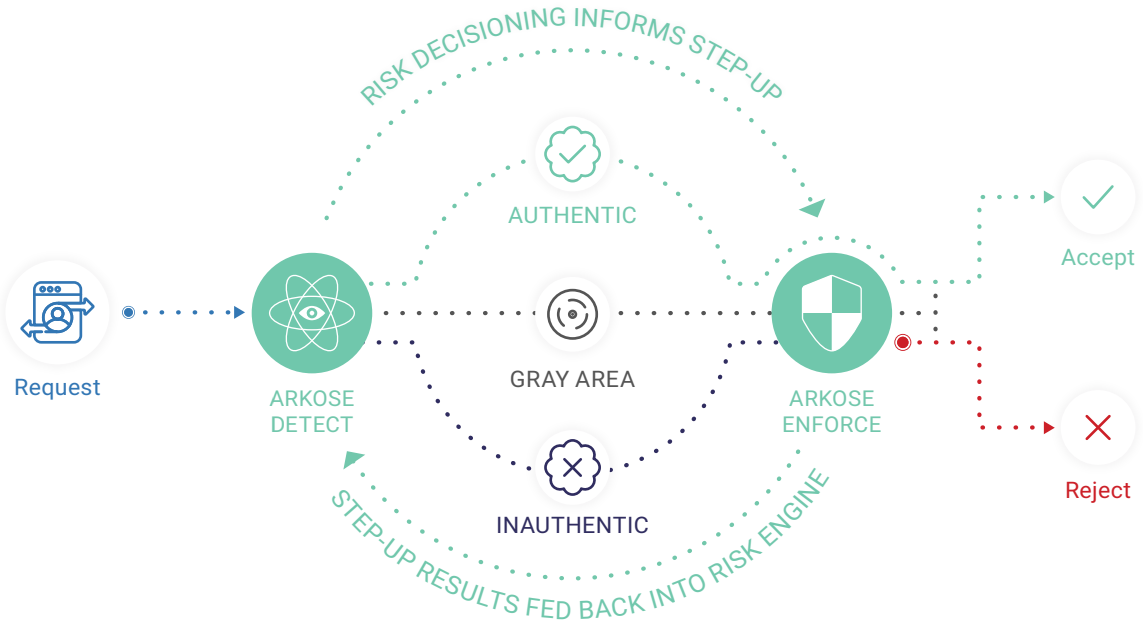
Vital to the success of this bilateral approach is a constant feedback loop between the data-driven profiling and the enforcement challenges. Accurate insights at the risk profiling stage will correctly classify the likely underlying intent, allowing for a more targeted challenge-response mechanism that will block 100% of automated traffic and root out sweatshop and fraudulent activity. By feeding the results of the enforcement challenges back into the risk engine, this continuously improves risk profiling and safeguards the online experience for legitimate consumers.

HOW DOES ARKOSE LABS HELP YOU ACHIEVE THIS?

Arkose Labs' Fraud and Abuse Prevention Platform acts as an intermediary between the businesses' digital properties and the fraudsters that attack them, helping fraud teams navigate the increasing uncertainty about the true intent of user traffic. This avoids placing undue burden on in-house teams and stops spiraling costs and decreased throughput typically associated with out-of-band authentication and manual reviews.

The platform allows businesses to deploy risk-based, step-up authentication in a unified and coordinated manner. The major uptick in accurate fraud detection is inspiring many digital businesses to completely rethink the role of friction on their websites and mobile apps.

Arkose Enforce, Arkose Labs' challenge-response mechanism, is unique in its ability to use visual challenges that are easy and fun for true customers to complete, whereas nearly impossible for fraudsters to circumvent at scale. This overcomes the two fatal flaws in first generation image-based authentication, which often frustrate good users and are vulnerable to cyber criminals scripting around them en masse.



CASE STUDY: Arksoe Labs Helps Digital Business Increase in Good Customer Throughput by 10%

Challenge: Stolen and fake user details were being leveraged by fraudsters for new account registration and account takeover attempts, with bots and human sweatshops being deployed to attack at scale.

Solution: Arkose Labs Fraud & Abuse Defense Platform delivered real-time decisioning combined with adaptive step-up enforcement challenges to actively root out all automated traffic and identify malicious human-driven attacks.

Results: Genuine customers were protected from abuse on this site and good customer traffic went up 10%.

CONCLUSION: STEPPING OUT FROM THE DARK

Many ecommerce fraud departments are experiencing mounting demands on their time and budgets, while barely keeping rising fraud levels at bay. Competitive pressure has led to many retailers implementing a friction-free online shopping experience in recent years– despite this making the industry a prime target for large-scale identity testing and payment fraud.

As both retailers and consumers increasingly recognize the need to have more accurate fraud detection procedures in place to prevent widespread abuse, it is time to reassess the role of friction in online fraud prevention.

Rather than shying away from introducing friction into the customer journey, we need to rethink how this can be leveraged as a positive component that supports risk-based decisioning in a complex threat landscape.

Successfully navigating the growing gray area between traffic recognized as trusted or malicious, using a combination of authentication techniques, provides multiple benefits that go far beyond reducing fraud losses. By slashing rejection rates for good users, stamping out abuse of consumers' credentials on your websites and apps, and putting visible protections in place that prove to valued customers that you care about protecting them, you can build a trusted relationship with the consumer.

As a result, ecommerce companies can finally embrace a zero-tolerance approach to fraud, with active protections in place for their consumers and the ability to accept good transactions with confidence.

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Its patented platform combines Arkose Detect, a sophisticated risk engine, with Arkose Enforce, which uses targeted step-up challenges to wear fraudsters down and diminish their ROI. The world's largest brands trust Arkose Labs to protect their customer journey while delivering an unrivaled user experience.

© 2020 Arkose Labs. All rights reserved.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006