Arkose Labs

BUILDING

CUSTOMER TRUST WITH SMARTER AUTHENTICATION

EBOOK

INTRODUCTION

Online commerce has completely transformed the way businesses interact with their consumers and is redefining the concept of customer service, as a result.

As in-person transactions give way to online interactions, businesses are now working overtime to differentiate their services in the digital sphere. Instant fulfillment and personalized offerings are key to enhancing user experience and combating the intrinsically impersonal nature of transacting online. To do this effectively, businesses are profiling increasing volumes of data and looking at behavioral patterns over time to understand consumers' evolving digital preferences.

However, all this will be futile if businesses fail to provide another vital component of good customer experience: a safe and secure online journey across all customer touchpoints. Fraudsters are attacking businesses at scale, leveraging sophisticated tools and large volumes of stolen consumer credentials. As the threat landscape intensifies, businesses are rethinking how they can strike the best balance between a seamless user experience while stamping out fraud. Achieving this is the only way to win consumer trust and loyalty in the long term.

THE THREAT TO CUSTOMER RELATIONSHIPS

In a digital world which is marred by widespread data breaches, winning and maintaining customer trust has never been more challenging. The frequency and scale of data breach incidents are making it easier than ever for fraudsters to abuse customer data on websites and apps.

It is now possible for fraudsters to not only know the bank account number of a consumer, but also details such as the branch in which the account was opened, the amount of money it has, payment history, and so forth. Combining this rich consumer data with the latest tools that help spoof devices and network details, fraudsters can impersonate genuine consumers with devastating accuracy and deceive fraud prevention teams.

When individuals have their credentials and payment details abused on a company's websites, apps or financial accounts, this breaks down trusted relationships and prompts individuals to switch over to a competitor. This, combined with the intensely competitive nature of online commerce, is making it increasingly harder for businesses to sustain consumer loyalty.

THE GROWING ATTACK SURFACE

Fraudsters are in the 'business' of making money - as much and as quickly as possible. As more and more businesses transition to digital, regional boundaries have blurred and customer touchpoints have multiplied, providing fraudsters with more opportunities to attack. Combining this with an easy access to commoditized fraud tools, fraudsters are able to improve their techniques, devise new attack types and monetize their exploits at a global scale - regardless of their location or geography.

A THRIVING CYBERCRIME ECOSYSTEM

Developing economies with access to cheap labor are becoming new hubs for large-scale attacks. Easy-to-use criminal toolkits and low-cost human resources are enabling fraudsters to attack businesses en masse. These human sweatshops and click farms are now a popular way amongst fraudsters to perpetrate low-value, high-volume attacks such as credential testing, circulating spam, writing fake reviews, new fake account registrations, as well as attacks that require more nuanced human responses which bots fail to mimic.

A parallel ecosystem has sprung up that not only supports large-scale organized fraud but also profits from heightened fraud and online abuse. Illegal online markets, identity farms, money mule networks and criminal toolkit dealers are thriving in this shadow economy.

Be it multi-channel fraud specifically targeting financial institutions, online gaming fraud, dating fraud, inventory hoarding or BOPIS, (buy online pickup in store), the attack techniques have evolved considerably according to the industry and use case, and often catch businesses by surprise. Fraudsters maneuver their resources depending on the attack type and leverage automated bots and sweatshops to maximize their returns as quickly as possible.

ULTIMATELY THE CONSUMERS SUFFER

While businesses identify vulnerable use cases and weigh the return on investment for their fraud prevention efforts, it is ultimately individuals who suffer the consequences of successful attacks.

When fraud strikes, not only do consumers face financial losses, they also face the disruption and stress of having their digital identity compromised. Consumers face long-term damage to their credit scores which can impact future borrowing. They must then spend disproportionate amounts of time and effort trying to reclaim their online identity, with the risk of future compromises remaining high.

The impact of fraud and online abuse is potentially the most severe for the more loyal customers. Businesses run loyalty programs and offer lucrative schemes to their privileged customers. Individuals will increasingly store payment card details in the accounts they purchase goods with most frequently. Furthermore, businesses lower their guard when it comes to authentication of known users in order to provide a frictionless online experience to these customers.

LOYAL CUSTOMERS ARE BECOMING MORE VULNERABLE

Here's a look into how loyal customers are becoming more vulnerable to fraud and online abuse across different industries:

Retail: One-click purchases, post-payment, faster checkout, discounts, speedy delivery, and easy returns are some of the ways online shopping platforms reward their loyal users. Fraudsters exploit these conveniences for payment fraud, account takeover, fake reviews, spam, manipulating delivery schedules, and BORIS (buy online return in-store).

Banking: Banks and financial institutions offer premium services to their loyal customers in the form of lower scrutiny when seeking credit or opening new accounts, speedy approvals, better saving schemes, privileged customer support, and so forth. When fraudsters take over accounts of authentic customers, they can abuse all these privileges to quickly transfer funds or get loan approvals and escape with the money as soon as it arrives in the account. This potentially leaves the customer to repay the unsolicited loan, or forces the financial institution to absorb the cost, and provides fraudsters access to compromised or bogus accounts to use for money laundering.

Dating and Social Media: When fraudsters break into verified accounts, they can use social engineering to manipulate users into sharing their personal details, which can then be used for more sinister crimes. Fraudsters can even pose as trusted friends or family to request wire transfers to con money out of individuals.

Gaming: Using stolen credentials, fraudsters take over 'rich' accounts on popular online gaming platforms to empty them of the digital currencies or in-game assets which have been accrued over a period of time. These are sold on the black market and through third-party sites. Other forms of abuse on gaming platforms include exploitation of online messaging systems to scam genuine customers or phish their personal details.

Travel: Businesses reward their returning customers with a variety of services, such as loyalty programs, access to premium services and discounts. Loyalty points are particularly attractive for fraudsters on two counts. The points accrued in consumer accounts are a digital currency that can be redeemed in exchange for a variety of travel and lifestyle products. The scrutiny of the loyalty accounts is often low compared to other payments and financial transactions. Therefore fraudsters can easily abuse loyalty points and cash out with little resistance.

Children and the elderly can be vulnerable to fraud, with the FBI reporting that cybercrime targeting older adults increased fivefold since 2014. Senior citizens can be lucrative targets as they are likely to have more savings and less likely to monitor their accounts actively. Those who are relatively inexperienced in the online world are more vulnerable to social engineering, with fraudsters posing as representatives from familiar institutions under the pretext of helping them navigate the digital world.

Children, on the other hand, are top targets for identity theft, with Javelin reporting that up to one million children have been affected by this in the US. Fraudsters are preying on youngsters to harvest social security number and other breached personal data in order to manipulate their digital identities and create synthetic identities. Fraudsters are also using social media and video gaming platforms to access the personally identifiable information of youngsters to use for sinister crimes including money laundering.

PUTTING AN END TO THE CAT AND MOUSE GAME

As fraud evolves, the losses that fraudsters can inflict on businesses can be rather severe. Business growth, operational costs, revenues, customer experience, and brand reputation are all at stake as digital businesses look to fight fraud and online abuse. Businesses depend on harnessing consumer data—transactional and historical—to distinguish between fraudsters and genuine users. However, in the post-breach era where digital identities have been corrupted at scale and fraudsters have easy access to sophisticated tools to circumvent detection, sophisticated fraud is becoming increasingly difficult to spot solely using data-driven fraud detection. Businesses are caught in a constant cat and mouse game with fraudsters as they attempt to evolve their defenses as a response to evolving attack techniques.

Customer experience is key to business growth and with so much at stake businesses must rethink their fraud prevention approach in order to achieve the optimal balance between user experience and accurate fraud prevention. They need a longer-term approach that eliminates fraud from its roots while staying ahead of evolving fraud techniques.

A NEW LONG-TERM APPROACH TO FRAUD PREVENTION

Arkose Labs helps global companies deliver a more secure online experience by striking at the root of fraud—its business viability. Arkose Labs Fraud and Abuse Prevention Platform provides unified risk-based and step-up authentication which is designed to sap the time and resources required from fraudsters to attack at scale, undermining their potential profit.

In an attempt to improve online user experience, businesses have shied away from step-up in recent years. However, Arkose Labs' unique approach allows businesses to re-embrace targeted friction as a powerful way to stop fraud and abuse on their online properties, while enhancing the customer journey.

Dynamic authentication workflows adapt to the risk profile of traffic in order to provide true customers a simple way to prove their legitimacy, while blocking automated attacks and malicious humans. More robust protection protects good customers from fraud, improves their online experience and ultimately encourages loyalty.

Optimizing customer experience is a central component of the Arkose Labs platform. Deep risk profiling works behind the scenes from the moment a user hits your site or app, ensuring that most trusted consumers progress unchallenged. Rather than blocking transactions out of the gate when there are suspicious flags, good customers are given a chance to prove their legitimacy by completing puzzles.

With usability still kept front and center, authentication challenges are designed to be fun, easy and non-disruptive for genuine customers. On the other hand, these cause automated attacks to fail and dramatically sap the time and resources required for fraudsters to complete challenges at scale. Rather than generic challenges being presented to all traffic, the decision engine determines the most effective challenge to present based on the risk profile.

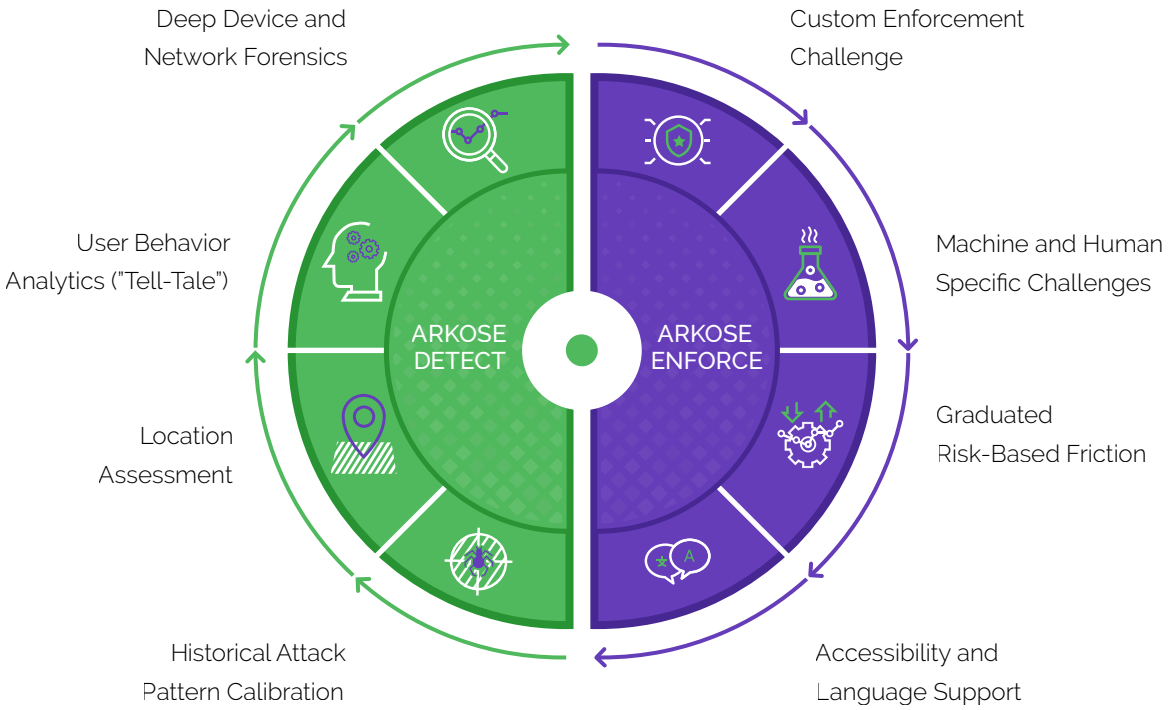
Businesses moving from stand-alone risk-based authentication to this combined approach have typically seen far more accurate fraud detection, with no negative impact to customer throughput. Authentication is easy for legitimate humans but roots out automated and sweatshop-driven activity, preventing the breakdown in trust from consumers being stung on your sites or apps.

HOW DOES ARKOSE LABS HELP YOU ACHIEVE THIS?

The Arkose Labs Fraud and Abuse Prevention Platform remediates illegitimate transaction attempts in real time. The platform is powered by Arkose Detect, a dynamic risk assessment engine, and Arkose Enforce, an adaptive, step-up challenge-response mechanism.

Arkose Detect analyzes data from billions of user transactions across a wide range of parameters to accurately assess the risks associated with each user. Determining the underlying intent of a user, traffic is segregated according to their risk profiles.

Arkose Labs Fraud and Abuse Prevention Platform



Arkose Detect is Trained by Arkose Enforce Results

Arkose Enforce leverages insights from Arkose Detect to present all users with an opportunity to prove their authenticity. Genuine users find these challenges quick and simple to solve. On the other hand, high-risk users are presented with incrementally complex authentication challenges which are tailored to the risk profiles, until fraudsters give up or move on.

The results from enforcement challenges are fed back into Arkose Detect, which helps sharpen future risk assessment and predictions. The platform is geared towards self-optimization with a feedback loop between Arkose Detect and Arkose Enforce that ensures the challenges are truly targeted for risky profiles - not generic challenges that are presented to everyone showing any level of risk.

Improved accuracy means that returning customers continue to enjoy a secure and seamless online experience, and encourages customer loyalty.

KEY RESULTS

Arkose Labs has helped its partners realize the following key results on deployment of the Fraud and Abuse Prevention Platform:

1. **Higher Customer Throughput:** Increases good customer throughput by 15-25%.

2. **Fraud Elimination:** Detects and blocks both human- and bot-driven attacks to reduce fraud by 50-90%.

3. **Protection Against Multiple Attack Types:** From credential testing to payment fraud, fake new accounts, account takeover, spam, scraping, fake reviews, denial of inventory, or any other complex attack, Arkose Labs platform accurately stops fraud across industries and use cases by intelligently adapting to the evolving fraud techniques.

4. **Long-term Protection:** Self-optimizing platform uses the feedback loop between Arkose Detect and Arkose Enforce to continually enhance assessments. This helps eliminate fraud from its roots and prepare for the evolving threats with confidence.

THE ARKOSE ADVANTAGE

The Arkose Labs solution helps digital businesses set themselves apart by providing an optimal balance between security and customer experience on their websites and apps.

Key differentiators include:

Digital Intelligence and Forensics: Arkose Labs challenges illegitimate interactions by working behind the scenes to validate third-party signals and historical behavior patterns. Outcomes are shared across the network to improve fraud detection and user experience for all customers.

Graduated Risk-based Friction: As attack patterns change, defense protocols automatically evolve. The graduated friction pushes the fraudsters beyond their window of economic opportunity, while ensuring legitimate users are provided with the opportunity to prove their authenticity, without disrupting their overall user experience.

100% Attack Remediation SLA: Arkose Labs is the only fraud prevention company that guarantees a solution which evolves and scales with the sophistication of fraudsters.

Real-time Remediation: Adaptive, step-up challenges that include machine and human-specific challenges disrupt the fraudsters' attacks without negatively impacting user experience for valued users.

Historical Attack Pattern Calibration: The Arkose Labs platform unearths and correlates patterns across use cases and industries for fresh insights into attack trends and more accurate anomaly detection.

CONCLUSION : RETHINKING FRICTION FOR CUSTOMER LOYALTY

Many businesses find themselves on a journey to search for the best balance between security and user experience in order to acquire new customers and improve loyalty. Conventional wisdom of the last few years construes 'friction' in any form as a problem for user experience. However, this view is becoming outmoded in the face of an increasingly hostile threat landscape and the fact that digital identities have been corrupted at scale.

Cybersecurity is becoming an increasingly mainstream issue, and with greater consumer awareness, organizations must demonstrate that they are proactively protecting users. When data-driven fraud detection is combined with targeted, intelligent friction, it can bring a positive component to online experience. It helps businesses reassure customers that protections are in place to stamp out fraud, ensuring transactions are secure for their most valued customers.

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

Address:

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

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

Schedule Demo