Arkose Labs

EBOOK

THE ULTIMATE GUIDE TO ACCOUNT TAKEOVER FRAUD

PROTECT YOUR CUSTOMERS AND YOUR BOTTOM LINE

INTRODUCTION

Businesses have been engaged in a demoralizing battle to protect customer identity, through years of major data breaches. Millions of personal records have been exposed and data breaches have become so frequent that people have become desensitized to the risk. The problem is compounded by customers who reuse passwords for multiple accounts, making it easy for fraudsters who have access to hundreds of thousands of digital to hack into accounts.

This makes it dangerous to take digital identities at face value, however, overly complex authentication processes deter good customers. Businesses grapple with the challenge of balancing effective customer screening while maintaining a smooth user experience for genuine customers.

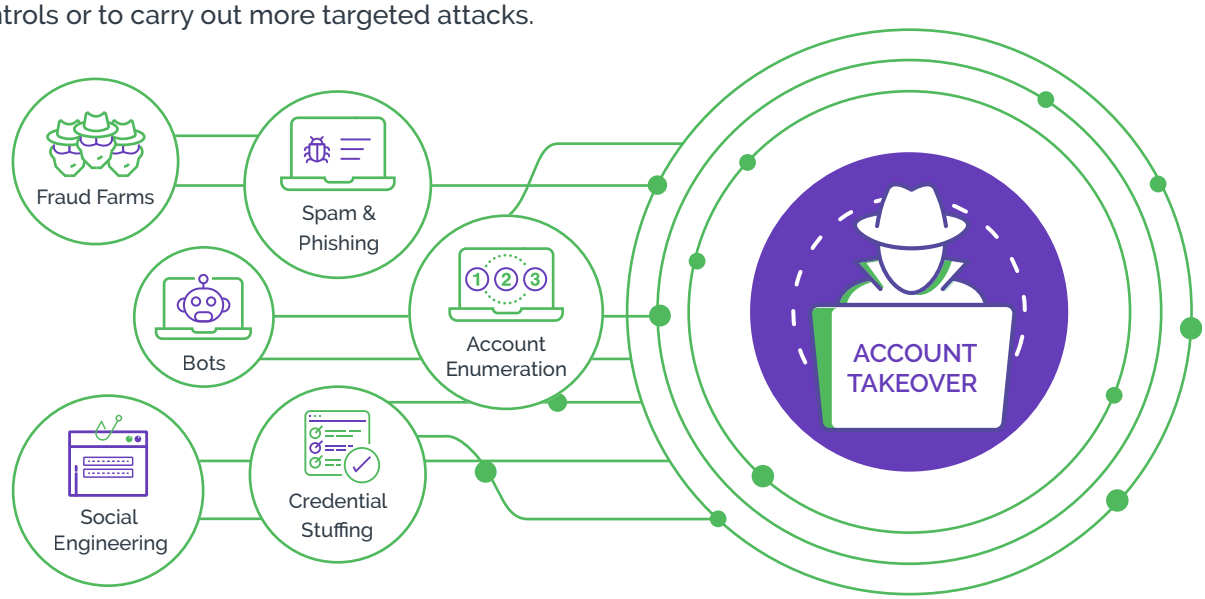
Account takeover is where a fraudster takes full control of a legitimate account and uses it for fraudulent purposes. Account takeover is a lucrative prospect for fraudsters and one in every five login attempts on the Arkose Labs network represented an ATO attack, during elevated attack levels at the beginning of 2020.[1]

HUMANS OR THE MACHINE?

ATO attack patterns are becoming more sophisticated. Fraudsters will tailor their attacks to maximize profit using bots, human labor or a combination of the two. While organizations still see large-scale identity testing and credential stuffing attacks using automated tools, fraudsters are increasingly leveraging low-cost human labor in 'sweatshops' or 'click farms' to bypass fraud prevention systems, and launch more nuanced attacks. Fraud prevention strategies need to be designed to actively detect and protect against both human-driven and automated attacks.

[1]Arkose Labs Q2 Fraud and Abuse Report

Account takeover is achieved by a wide range of malicious activity, that enables fraudsters to harvest user credentials and break into accounts at scale. Large-scale account takeover is mostly bot-driven, allowing fraudsters to mount multiple attacks for maximum ROI. Human labor is used to circumvent controls or to carry out more targeted attacks.



Fraudsters are increasingly playing the long game, launching orchestrated, multi-step attacks that allow them to disguise malicious intent. Whereas payment fraud often is only profitable until a consumer or bank spots abuse and blocks the card, account takeover can have a longer lifespan, leading to different frauds which begin with just one compromised account. Attacks are targeted and can vary significantly by industry.

Account enumeration and account validation: Fraudsters exploit account registration processes to test whether an account identifier is valid or not.

Social engineering: Phishing is the most common form of social engineering, where fraudsters manipulate individuals into divulging personal information or direct customers to fraudulent websites. This is a highly effective method of harvesting identity data at scale.

Fraud farms: Fraudsters leverage low-cost human labor to mimic good customers and bypass anti-fraud measures designed to eliminate automated attacks.

Credential stuffing: This is a large-scale automated attack, where bots try multiple username and password combinations until a match is found, providing them with the tools for account takeover.

FRAUD ENTRY POINTS FOR WEB-CONNECTED DEVICES:

Customers use multiple platforms to access digital services. Any customer touchpoint can act as a potential attack surface for fraud.

DESKTOP
Web Browser

MOBILE PHONES
SDK

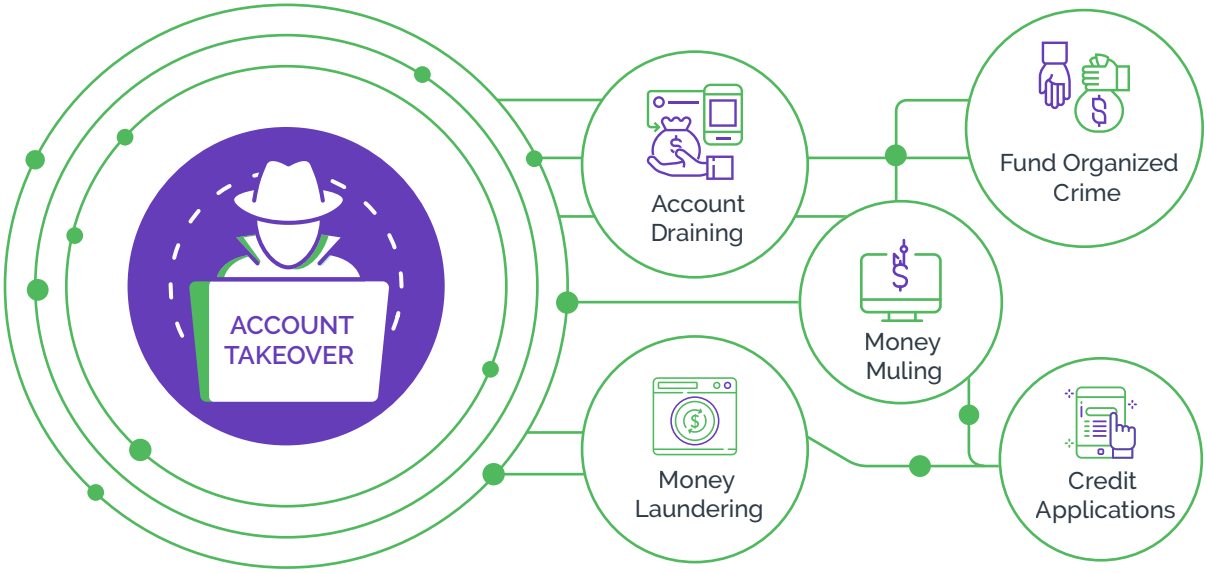
GAMING CONSOLES
Online Platforms

API
Software Interfaces

SPOTLIGHT ON BANKING AND FINTECH

Account takeover in banking and fintech presents a lucrative prospect for fraudsters. Fintechs have been a major disrupter in banking, putting mounting pressure on traditional banks to deliver a seamless user experience and digital-first products. Both fintechs and traditional banks walk a tightrope between offering low-friction user experience and ensuring account security. Compromised financial accounts can lead to serious downstream consequences. They can be used to both fund and channel the proceeds of organized crime including drugs, human trafficking and terrorism.

Fraudsters use stolen data and corrupted digital identities to mount attacks on multiple fronts



Account Draining: Fraudsters use stolen identity credentials to take complete control of financial accounts. The accounts are drained of funds, and the money often 'laundered', making it difficult to trace the theft.

Money Laundering: 'Dirty' money (the proceeds of crime) is passed through a complex series of bank transfers, obscuring the origins of the funds to make it appear legitimate. The 'clean' money returns indirectly to the criminal.

Money Muling: Money muling is a form of money laundering where fraudsters either recruit legitimate customers to transfer dirty money, or take control of legitimate active or dormant accounts and use them to transfer funds.

Credit Applications: Stolen identity data is used to make fraudulent credit applications. Compromised account data might be held for months before fraud is committed, making it difficult to identify the source of the breach.

SPOTLIGHT ON E-COMMERCE

As consumers were forced to shift their shopping habits to digital platforms, traditional retailers have had to embrace e-commerce. Though efforts have been made to safeguard payment mechanisms, account security is often an area left too vulnerable for fraud to originate. Account takeover is a rising problem in retail, but many vendors are unaware of the prevalence of attacks, and ill-prepared to deal with them when they occur. The fallout can be serious for all parties, with the account holder suffering the consequences of identity theft, and the retailer experiencing severe reputational and business damage.

Hacked account: Fraudsters use hacked accounts to send spam, phishing and other malicious content to other users, perpetuating the cycle of crime.

Stolen payment credentials: These are used to make fraudulent purchases on other sites, affecting both the victim, and the sites who end up issuing chargebacks and losing revenue.

Identity theft: Detailed personal information is sold to illegal data exchanges on the dark web, leading to many more incidences of cybercrime for the victim.

THE LIMITATIONS OF LEGACY APPROACHES

Despite significant investments in technology and resources to solve the ATO issue, attacks persist because financial incentive still exists. Fraudsters are quick to adapt and circumvent the defense technologies that are put in place. By implementing mitigation-focused strategies that fail to truly get to the core of the issue, businesses struggle with diminishing returns on their security investments, or a drop off in good customer throughput.

01 Risk Scores

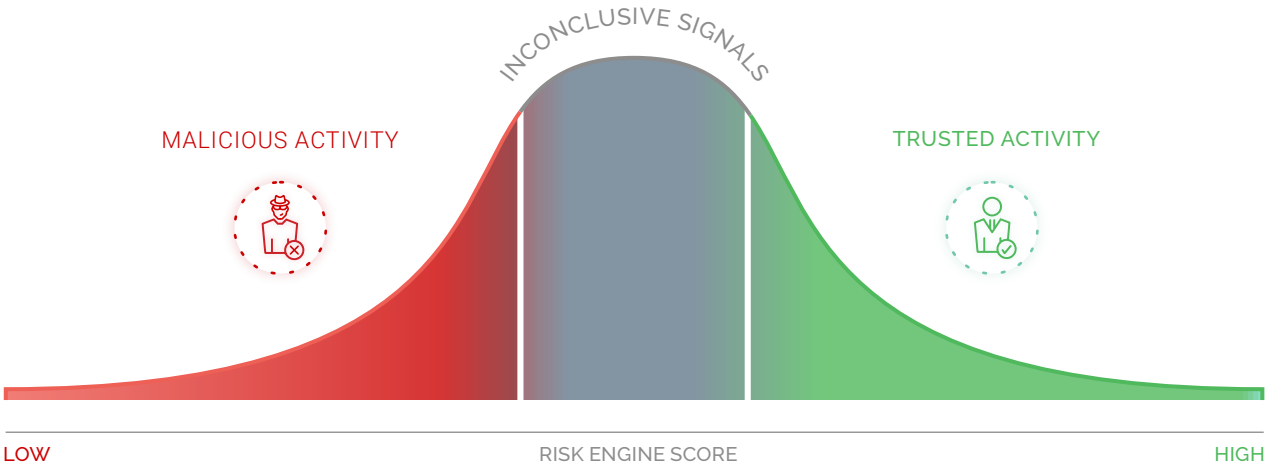
In order to provide users with a frictionless login experience, businesses have invested in risk-based fraud detection solutions that reduce losses. Risk engines produce a threat score based on device, identity and behavioral analysis. The depth of assessments possible has come a long way, however, using these as a stand-alone approach to eliminating fraud has become problematic in the ever-evolving fraud world.

These systems are designed to spot extremes, identifying users who display clear 'trust' or 'mistrust' signals. Unfortunately, fraudsters have developed sophisticated methods of masking their identity, while genuine customers display unpredictable behavior. More and more traffic is falling into a 'gray area' as it is difficult for fraud prevention systems to distinguish between 'good' and 'bad' activity.

Due to the limitations of probabilistic risk assessments, businesses are layering in multiple solutions within very complex tech stacks. SaaS solutions that should be straightforward to implement, in theory, are being stymied due to the difficulty in getting actionable intelligence from a mix of threat scores, leading to increasingly long time-to-value when implementing new technology. Businesses are seeing diminishing returns on adding different threat scores as they can lead to alert overload and fraud score fatigue.

THE GREY AREA OF FRAUD DETECTION

Additionally, fraudsters have detailed knowledge of the parameters that businesses use to spot fraud and use this against them - therefore holding the balance of power. Mitigation-focused solutions tend to be reactive, aiming for damage limitation rather than long-term prevention.



02 Multi-Factor Authentication

Out-of-band authentication is implemented in order to make the barrier too high for fraudsters to attack at scale. While MFA provides maximium fortification, using it as a one-size-fits-all approach leaves a less-than-desireable good user block rate.

Additionally, fraudsters have developed ways to circumvent these at scale and authentication priced by authentication token can become very expensive. Fraudsters will bypass SMS verification using fake accounts, whereas genuine customers run the risk of being blocked or blacklisted when they have bad mobile reception or are operating similar areas to fraudsters.

CASE STUDY

FINTECH NEOBANK SLASHES ATOS BY 75%

Overview: A global Fintech was seeing nearly 30,000 credential stuffing attempts a day, with attackers looking to hack into valuable user accounts. Fraudsters would deploy bots targeting back-end APIs. By by-passing web forms, fraudsters could write simple scripts that allowed them to attack at greater volume and velocity.

Arkose Labs Solution: The company implemented the Arkose Labs platform to protect its login forms and backend APIs. Arkose Labs monitors all traffic for known signals of abuse, using behavioral fingerprints, velocity, and rate monitoring, and a proprietary user IP database. Suspicious traffic was met with tailored enforcement challenges that cannot be solved by bots.

Results: The fintech saw more than 75% reduction in ATO attacks after implementing Arkose Labs. Furthermore, it realized cost savings of $100K per month related to remediating compromised attacks.

03 CAPTCHA

On-page CAPTCHAs are a way to protect accounts from automated ATO attacks and the market is saturated with many free or low-cost solutions. Often designed to weed out large-scale untrained bots, traditional CAPTCHAs can fall victim to trained automation and human fraud attacks. Machine vision technology enables bots to recognize and complete photo-based challenges at scale. Some CAPTCHA vendors offer a free 'security' service, while monetizing the classification of images - but this provides very low-level protection. Due to a lack of innovation among legacy CAPTCHA solutions, the user experience is clunky and results in high dropout rates among good users and loss of business. Additionally, they can be somewhat of a blackbox solution, with limited customization and a lack of visibility into the reasons that traffic is challenged.

Dropbox

CASE STUDY

ARKOSE LABS REPLACES LEGACY CAPTHCA TO PROTECT 600M ACCOUNTS

Overview: Dropbox has over 600 million registered users across 180 countries--both individuals and businesses rely on the platform to share, store and collaborate on critical files. However, it popularity made it a prime target for account takeover attacks.

Arkose Labs Solution: The company replaced its existing solution, which disrupted user experience and provided limited protection against attacks, with Arkose Labs. Risk assessments combined with targeted step-up, differentiated between bots, malicious humans and good users.

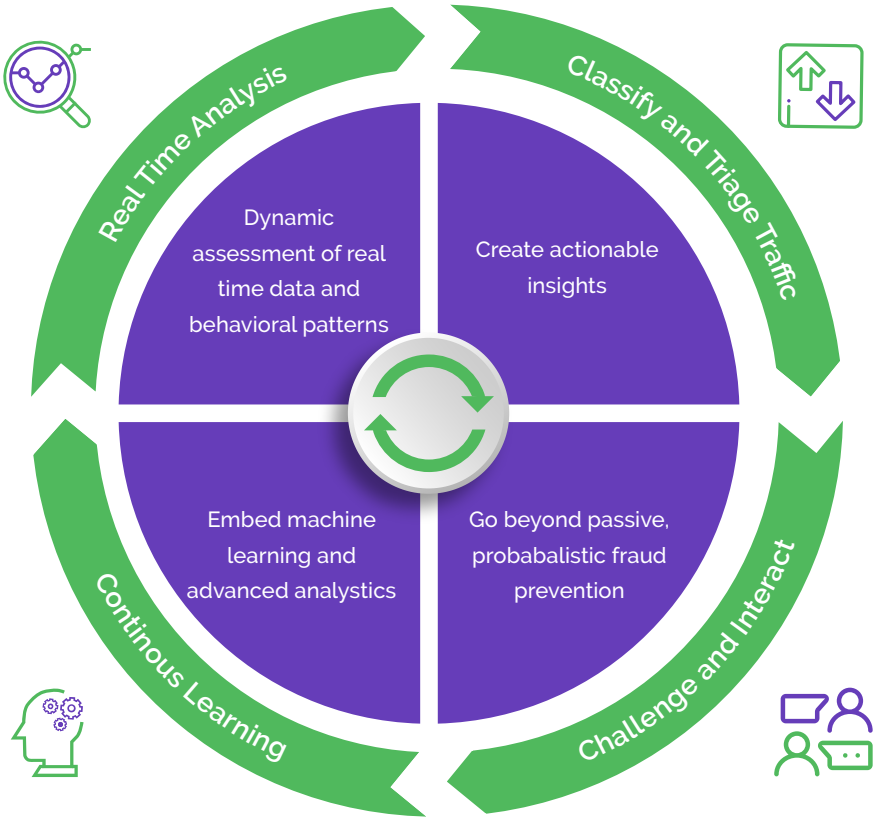
Results: Dropbox eliminated automated ATO attacks and sapped the time and resources required for fraudsters to launch attacks. This compelled them to abandon attacks - all while reducing intervention rates for good users by 70%.

BANKRUPTING FRAUDSTERS: A LONG-TERM APPROACH

For too long, businesses have been stuck in a game of cat and mouse with fraudsters. Fraud losses have been tolerated as just another overhead, allowing fraudsters to hone their skills and develop their attack models, learning from every attack. Fraud is ultimately a business; profit the main motivator. To effectively eliminate fraud, businesses need a fraud prevention strategy that focuses on slashing the financial rewards and draining fraudsters' resources.

The challenge is to do this, while maintaining a smooth user experience for genuine customers. Traditional fraud prevention strategies can show a high level of false positives, preventing good users from accessing sites and accounts. This damages customer trust, company reputation and profit. Security must always be balanced with accessible, customer-focused user experience.

EVIDENCE-BASED DETECTION AND REMEDIATION



Real-Time Analysis: Businesses must perform sophisticated real-time analysis of traffic to look for even subtle indicators of fraud. However, beware external solutions that require the collection of large sets of personal information, as they can cause a privacy and compliance headache - instead focus on behavior, device and network characteristics, and how they are connected.

Classify and Triage: Multiple risk scores can become difficult to action. Instead take an approach that classifies and segments traffic based on the risk grouping. Triaging traffic based on whether it is likely to be legitimate, a bot or human sweatshop, provides actionable intelligence that can inform the system of any required secondary screening and the type of enforcement required.

Challenge and Interact: To understand the intent of traffic in a deterministic way, secondary screening of high-risk traffic is required, in tandem with the risk assessment. Test and challenge high-risk traffic using interactive technology that causes all automated attacks to fail. Graduated risk-based challenges can frustrate fraudsters by increasing the amount of friction they experience, leading them to abandon their attacks.

Continuous Learning: Reap the benefits of a fraud prevention system which combines risk assessments with challenges, by leveraging a continuous feedback loop to improve fraud detection rates, while decreasing challenge rates for good users. Embedded machine learning will provide advanced anomaly detection and evolving protection, taking the burden away from in-house teams.

OUR APPROACH: DETERRENCE NOT MITIGATION

The Arkose Labs Fraud and Abuse Prevention Platform delivers a long-term approach to deterring and eliminating account takeover attacks. It slashes the profit of attacks by combining real-time intelligence, deep device analytics and tailored step-up challenges, while evolving with attack patterns. The platform comprises two key component which work seamlessly together.

Arkose Detect

A dynamic risk engine that analyzes user data and tracks behavior patterns across multiple devices and networks in real-time. Traffic is triaged according to risk profiles, and directed to Arkose Enforce for secondary screening, when necessary.

Arkose Enforce

Arkose Enforce provides step-up enforcement challenges that are tailored according to the exact risk profile. The challenges are progressively difficult, and designed to effectively differentiate between good customers, human fraudsters and bots. Genuine users easily clear the challenges, while fraudsters are forced to waste significant time and resources as they attempt to complete increasingly difficult puzzles. They are unable to clear challenges at scale; the ROI of the attack becomes negligible and compels fraudsters to abandon the assault.

THE ARKOSE ADVANTAGE

- Eliminates 100% of automated attacks
- Protects against human-driven attacks and roots out organized click farms
- User experience is kept front and center of the authentication process
- Step-up challenges are tailored to risk profile
- Continuous feedback loop between risk engine and enforcement challenges enables the platform to evolve with attack patterns
- Wastes fraudsters' time and resources
- Shifts the attack surface away from the business

CONCLUSION

Account takeover fraud is on the rise and the effects can be far-reaching. The profits of fraud feedback into the criminal ecosystem, funding the drug trade, human trafficking, and terrorism. A single identity breach can open the door to thousands of fraud attacks, making it imperative for businesses to prioritize fraud prevention throughout their operations. To deliver the best customer experience it is important to balance robust security with positive UX.

Arkose Labs offers a new approach, focused on bankrupting the business of fraud. The platform accurately triages trusted users, fraudsters and bots at the point of entry, directing them to targeted challenges appropriate to risk profile. Challenges are fun; genuine users clear them easily, while fraudsters are forced to waste time and resources which dramatically reduces the ROI of attacks. Arkose Labs' platform ensures businesses see a huge reduction in false positives and prevents 100% of automated attacks. Human-driven attacks are detected and stopped early in the fraud life-cycle. This takes the pressure off in-house teams and allows them to focus on business development and customer satisfaction.

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized as a 2021 Cyber Defense Magazine "Hot Company in Fraud Prevention", 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

Address:


San Francisco


Brisbane


London

Schedule Demo