THE PAYPERS

Insights into Payments and Beyond

Fraud Prevention in Ecommerce Report 2021/2022

Best Practices Into Stopping Fraud to Convert More Orders and Increase Revenue

Endorsement partner:

MRC Building Better Commerce
Fraud & Payments Professionals

Key media partner:

mpe MERCHANT PAYMENTS ECOSYSTEM

Arkose Labs

Top 5 Steps to Prevent Account Takeover Attacks

Vanita Pandey is a visionary CMO and a recognised anti-fraud expert, currently leading the global marketing strategy at fraud-prevention firm Arkose Labs. Prior to her current role, she served as the global VP of Product Marketing at ThreatMetrix, which she helped lead to a successful acquisition by FTSE 100 company RELX's LexisNexis. Vanita also has deep payments industry experience having held top strategic marketing roles at Simility (acquired by PayPal) and Visa.

Vanita Pandey ▪ *Chief Marketing Officer* ▪ Arkose Labs

The rise of the digital economy has been a boon for businesses as well as for consumers, who now have easy access to goods and services from around the world. Unfortunately, when money is involved, fraudsters are just around the corner. They are exploiting the digital infrastructure to orchestrate a gamut of attacks — account takeover (ATO) in particular, which is one of the biggest headaches for businesses today.

After a successful account takeover attack, fraudsters commit CNP (**card-not-present**) fraud, redeem reward points, launder money, and seek loans. That said, they do not limit themselves to just swooping out all the money from the account. They also use account takeover as a means to control a compromised account remotely and abuse it for many other criminal activities.

How account takeover attacks cause regulatory, financial, and reputational losses

Apart from financial losses, ATO poses reputational risks for businesses. This is because consumers place a lot of trust in businesses when it comes to ensuring secure transactions. An account takeover attack is construed as the business' failure in maintaining adequate security, and hence consumer trust. This can deal a big blow to the relationship-building efforts and cause unforgiving customers to switch over to competitors. Furthermore, non-compliance with the regulations can attract hefty penalties, causing an additional burden.

How fraudsters use bots and sweatshops to achieve scale

Account takeover attacks are on a steady rise. Data from Arkose Labs reveals that 5% of all digital traffic is an ATO attack. This can be attributed to large-scale and frequent incidents of data breaches that fuel these attacks. Fraudsters harvest the invaluable personal information of millions of consumers from these data mining activities and use them for account takeover attacks.

Automated bots are the most popular method fraudsters use for account takeover because automation helps them achieve scale and maximise returns on investment. Further, many bots are so advanced that they can accurately mimic human behaviour online. Using the advancements in machine vision technology, these bots can bypass fraud prevention solutions.

Apart from malicious bots and scripts, fraudsters also 'hire' human fraud farm workers to launch large-scale account takeover attacks. These malicious humans can easily circumvent fraud prevention solutions that are specifically designed to protect against bots. Also, they can quickly clear the legacy challenge-response mechanisms that require more nuanced human interactions.

Why commonly used authentication cannot fight account takeover attacks

Massively corrupted digital identities and advanced tactics used by fraudsters make it even more difficult for businesses to fight the menace of account takeover. Unfortunately, a lot of commonly used authentication methods fail to stop ATO fraud and end up annoying customers. Authentication methods such as two-factor authentication (2FA) are not completely reliable, as the SMS may get delayed or intercepted by fraudsters. Knowledge-driven authentication fails as often customers forget the answers. ➔

Data-driven authentication methods rely on clear 'good' or 'bad' signals from user data. Since fraudsters can accurately mimic true users, they succeed in transmitting 'good' data signals. A true user, on the other hand, may be tagged 'bad' due to a change in online behaviour. Further, businesses are increasingly facing traffic that does not transmit clear 'good' or 'bad' signals. These signals fall in a gray area, which data-driven solutions cannot decipher. Businesses, therefore, need a robust solution that can fend off account takeover attacks without disturbing the user experience.

Five steps to robust account takeover protection

Arkose Labs platform provides businesses with a solution that can effectively deal with the traffic in gray areas. It makes the attack long-drawn and eats into the returns to make the attack financially unattractive. The Arkose Labs solution uses the following five steps to provide protection against account takeover attempts:

1. **Shift the attack surface** – Arkose Labs platform shields the customer touchpoints by diverting the attackers to targeted step-up challenges. This disrupts the attackers' plans and relieves the burden from in-house fraud prevention teams.

2. **Targeted friction** – Keeping user experience front and centre, Arkose Labs targets high-risk users with higher friction. Continuous intelligence assigns each user with a risk score and provides minimal friction to good users.

3. **Stepped-up attack remediation** – For high-risk users, the platform presents 3D challenges that are dynamically tailored according to the risk profile. These include specific challenges for bots, advanced bots, sweatshops, and lone human attackers.

4. **Future-proof protection** – Continuous feedback between risk analysis and the challenge-response mechanism enables enforcement challenges to adapt to the evolving risk profile of the traffic. This ensures the enforcement challenges always stay ahead of the changing threats.

5. **Easy integration** – The Arkose Labs solution seamlessly integrates with the existing technology stack of the business and requires minimal IT work.

Arkose Labs erodes the financial incentives that fraudsters associate with account takeover attacks so that digital businesses have robust, long-term protection.

Click here for the company profile

Company	Arkose Labs
	Arkose Labs bankrupts the business model of fraud. Recognised by Gartner as a 'Cool Vendor in Fraud and Authentication', the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput. Based in San Francisco, CA with offices in Brisbane, Australia, and London, UK, the company was honoured as the 195th fastest growing companies in the US on the 2021 Inc. 5000 list.
Background information	
Year founded	2017
Website	www.arkoselabs.com
Target group (Merchants/ecommerce; PSP/acquirers; SMBs; Banks/FS; Corporate; Fintech; Telecom)	Merchants/ecommerce PSP/acquirers SMBs Banks/FS Corporate Fintech Telecom
Supported regions (US; Europe; Middle East; APAC; Africa; LATAM; India; China; Global)	Global
Contact	Jean Creech Avent, Global Head of Communications and Brand, j.creechavent@arkoselabs.com
Company's motto	Bankrupting the business model of fraud
Member of industry association and/or initiatives	MRC, Worldwide Web Consortium
Core solution	
(Fraud/risk management and decisioning platform; Customer authentication; Identity verification; Behavioural biometrics; Data provider and intelligence; Chargebacks management; Bot risk management; KYB/Merchant onboarding; KYC)	Fraud/risk management and decisioning platform Customer authentication Identity verification Behavioural biometrics Data provider and intelligence Bot risk management
Core solution/problems the company solves	Arkose Labs enables enterprises to protect their users' accounts and ensures account integrity while keeping their business safe without causing customer friction. We help businesses protect from ATO, loyalty fraud, gift card fraud, API abuse, and many other forms of attacks.
Technology	
(On-premise; Cloud enabled; Native cloud; Hybrid)	Native cloud

Data input

Identity verification	proprietary capability	third party	both
Identity document scanning			
Video scanning			
Personally Identifiable Information (PII) validation	x		
Small transaction verification	x		

View company profile in online database

Email verification			
Phone verification			
Social verification			
Credit check			
Compliance check			
Online authentication	**proprietary capability**	**third party**	**both**
Behavioural biometrics	x		
Physical biometrics			
Device fingerprinting	x		
Geo-location	x		
Remote access detection	x		
Mobile app push			
3-D Secure 2.0			
Hardware token			
One-time passwords			
Knowledge-based authentication			
Intelligence	**proprietary capability**	**third party**	**both**
Abuse list	x		
Monitoring	x		
Address verification			
Credit bureau			
Information sharing	x		
Data ingestion/third-party data			
Stateless data ingestion and augmentation	x		
Methodology			
Machine learning (Rule-based; Supervised ML; Unsupervised ML; Hybrid)	Rule-based Supervised ML		
Decisioning			
(Manual review; Case management; Decision orchestration)	Decision orchestration		
Chargeback management			
(Chargeback dispute; Guaranteed fraud protection)	N/A		
Business model			
Pricing model	SaaS-based pricing model		
Fraud prevention partners	N/A		
Year over year growth rate	110%		
Number of employees	200		
Future developments	Detection enhancement, Digital identity graph, MFA, ongoing enhancement to the enforcement platform		
Customers			
Customers reference	Microsoft, PayPal, Sony, DropBox		

Arkose Labs

CREDENTIAL STUFFING

Spiked
98% during last 12 months*

Cost
US$6 Million on average*

Fraudsters' volumetric approach to account takeover attacks happen fast, quickly overloading your businesses' servers while putting your consumers at risk.

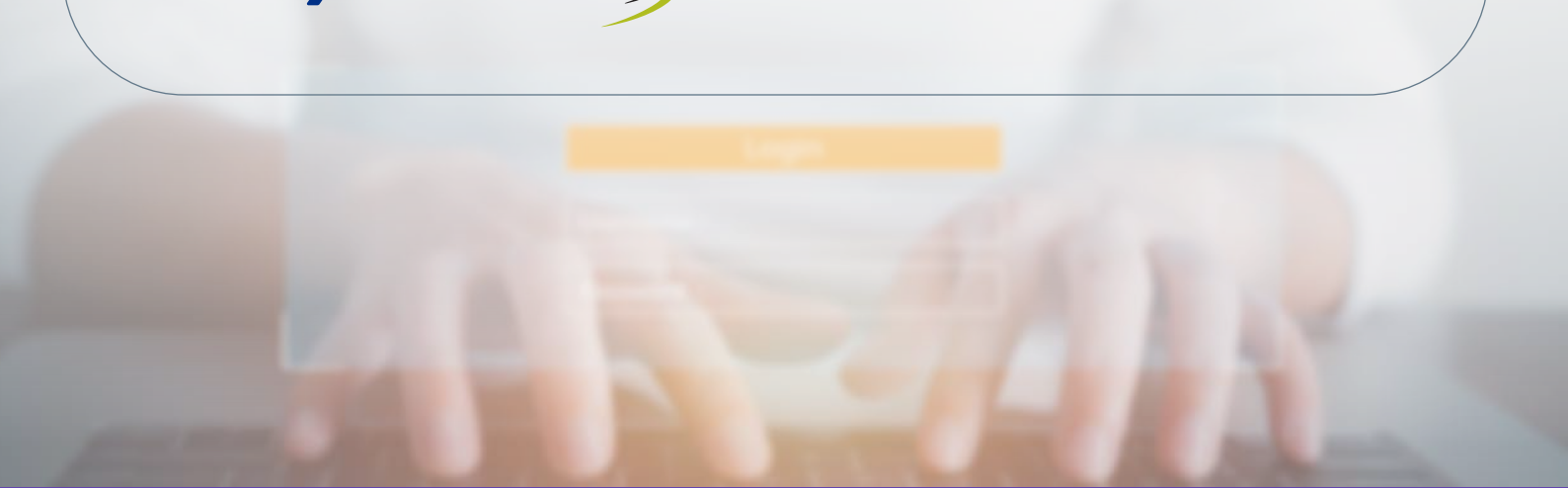
Had Enough?

Contact Us >

We're backed by the industry's only US$1 million credential stuffing warranty.

Trusted by

PayPal BLACKHAWK NETWORK venmo



Sources: The 2021 Q4 Arkose Labs Fraud and Abuse Report; Information Age: https://ia.acs.org.au/article/ 2020/ credential-stuffing--the-annual--6-million-challenge.html