Arkose Labs

Leading Fintech Platform Deploys Arkose Labs Solution to Protect its Crypto Exchange

CASE STUDY

A Global Fintech Platform

Business Problem

- Automated, bot and human-driven attacks
- Fraudulent new accounts
- Account takeover of genuine customer accounts and abuse of dormant accounts to escape detection
- Customer dis-satisfaction due to disruption in user experience

Solution

Arkose Labs Fraud and Abuse Prevention platform combined real-time decisioning with adaptive step-up enforcement challenges to filter out bots and organized sweatshop attacks to protect the crypto exchange from abuse and safeguard the interests of genuine customers.

Results

- Increased good customer throughput by 10%
- Reduced use of stolen and/or fake user details by fraudsters for new account origination and account takeover attempts
- Stopped malicious human-driven and automated bot attacks
- Safeguarded interests of genuine customers

Overview

This global financial services platform enables individuals, institutions and entrepreneurs across the globe to use, trade, invest and raise capital with open crypto technologies. With focus on inclusion, the company is delivering products and online services that are safe and easy-to-use.

The company has a global customer base and its crypto exchange deals in over 60 cryptocurrencies and provides numerous trading tools to enable its customers to access new opportunities like early listings of new projects, airdrops and forks. It even provides its customers with the facility to trade on-the-go through its app. Institution and high-volume traders can access onboarding support, large-scale trades, higher transaction limits, concierge service, tax reporting assistance and more.

The Business Problem

Cryptocurrencies, especially bitcoin, have become particularly popular among fraudsters. In many recent incidents of ransomware locking down municipal systems, fraudsters demanded bitcoins as ransom to unlock the government systems. Crypto exchanges have become destination for genuine customers and fraudsters alike looking to trade. As the popularity has grown, these exchanges have come under the scrutiny of regulations across the globe and are having to comply with increasing number of rulesets and guidelines. Since the company's crypto exchange enables quick movement of money and instant transactions using cryptocurrencies, fraudsters found ample opportunities to exploit the exchange for monetary gains. The global growth of business, a host of options to create wealth, numerous cryptocurrencies to trade in, and the convenience of connecting card and bank accounts for crypto trading, opened the company's exchange for fraud and online abuse.

Using stolen and/or fake customer details, automated bots, and sweatshops/click-farms, fraudsters perpetrated multiple attacks including new account origination, account takeover, payment fraud, and money laundering. Fraudsters also abused the dormant user accounts for fraud without getting detected. Due to increasing fraud and online abuse, the company suffered colossal financial losses. The company faced an increased risk of non-compliance as crypto transactions are highly regulated apart from customer dis-satisfaction due to disruption in user experience.

"Arkose Labs not only helped reduce the ATO attempts but also provided us with a future proof way to protect against evolving attacks"

—Director of Engineering

The Arkose Labs Solution

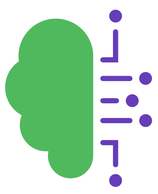
The Arkose Labs Fraud and Defense Platform was deployed to resolve the problems the company was facing. Within a few weeks of deployment, the company saw a 10% increase in good customer throughput without any increase in fraud. The solution successfully detected and stopped human-driven as well as automated attacks by enabling in-depth scrutiny of user log-in attempts. This significantly reduced the number of fraudsters trying to use stolen/fake credentials to create new fraudulent accounts and/or account takeover existing genuine accounts.

This was made possible by bankrupting the fraud model through enforcement challenges. While genuine users could easily pass these tests, fraudsters were forced to spend more time. Additionally, these adaptive stepped-up challenges required more investment in terms of resources, tools, and technology to clear them at scale. This reduced the returns from the attack and made it far-less attractive for the fraudsters.

The key features that protected the company's platform from fraud and online abuse while safeguarding customer interests are:

Deep-dive Forensics

Analyzing digital intelligence retrieved from the originating devices, networks, and locations, helps gain insights into user profiles, making it possible to accurately distinguish between suspicious and genuine users.



Continuous Intelligence

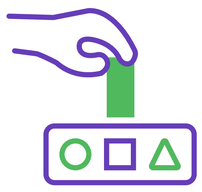
These deep-dive insights when combined with behavioral analytics, provides a 360-degree view of the user, which help accurately understand the underlying intent of the user and the associated risks.

Global Telemetry

Insights from the Telemetry data combined with the risk assessment of each user, helps present appropriate enforcement challenges to the suspicious users.

Enforcement Challenges

The adaptive stepped-up enforcement challenges protect the company from malicious automated attacks by accurately filtering out bots and organized sweatshops. These challenges are designed with a view to enable genuine users to clear them without any difficulty, but force fraudsters to spend more time and resources.



On-brand

The elements from the company's brand identity are used to create customized, on-brand enforcement challenges so that they blend-in with the overall brand positioning without causing any disruption to user experience.

Long-term Approach

The data from user sessions is used to retrain the Telemetry which improves future predictions and enables self-adaptation in keeping with the changing attack techniques. This empowers the decision-makers to future-proof their fraud prevention approach.

The multi-level, integrated approach provides the company with continuous risk assessment that not only stops individual attacks but also delivers a long-term solution that reduces fraud and operational costs while delivering a seamless customer experience.

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.

Schedule Demo

demo@arkoselabs.com
(800) 604-3319
arkoselabs.com