Arkose Labs

Global Bank Uses Arkose Labs to Protect Logins and Stop Application Fraud

CASE STUDY

Customer:
Global Retail Bank

⚠ Business Problem

- Bank is major target for loan application fraud and ATO attacks
- Required a user-centric way to stamp out bot and human attacks
- Legacy solution was ineffective and created customer friction

Solution

- Arkose Labs platform deployed to protect global digital banking sites
- Flexible solution embedded into login and registration flows
- User-friendly authentication using bespoke, on-brand challenges

Results

- Proven superiority in stopping automated attacks
- Improved user experience versus legacy approach
- 100% SLA guarantee against bot-driven fraud and abuse

Overview:

The client is one of the largest global banks, with millions of retail customers around the world. They also have significant operations in corporate banking, investment banking, insurance, and several other lines of business. With more than $1 trillion in total assets, the bank plays a significant role in powering the global economy. Facing a highly competitive environment from both fintechs and traditional competitors investing heavily in digital, the bank needed to ensure a digital experience that would be both seamless for customers as well as safe and secure.

The Business Problem

The bank was facing frequent and significant attacks targeting user accounts. Fraudsters used bots to power credential stuffing attacks at scale, account takeovers, and new loan and credit application fraud. The client had relied on legacy, text-based CAPTCHAs for fraud prevention and authentication, but these were ineffective at stopping automated attacks. It was imperative for the bank to have a solution in place that could stop the onslaught of attacks. With password/username combinations and other PII readily available on the dark web, fraudsters can easily launch credential stuffing attacks at a mass scale to take over user accounts and then commit downstream fraud.

Further, fraudsters use this data along with social engineering to create highly sophisticated synthetic identities for new account fraud, which can be difficult to detect. Banks need to defend against these onerous attacks while still enabling a digital experience that is friction-free and intuitive for good users.

Arkose Labs Solution

Arkose Labs takes a unique approach to fraud prevention and user authentication, one that seeks to undermine the financial incentive behind fraud, thus dissuading bad actors from even launching attacks in the first place.

The Arkose Labs Fraud and Abuse Platform combines real-time intelligence, rich analytics, and adaptive step-up challenges to progressively diminish the profitability of attacks while adapting to evolving attack patterns.

Arkose Labs' custom enforcement challenges are context-based, adaptive visual challenges that will thwart both automated and human-driven account takeover attempts. Rather than outright blocking traffic and negatively impacting the user experience, the Arkose Labs approach is to use targeted friction, which is reserved purely for high-risk traffic. Due to a sophisticated proof of work algorithm operating on the back end, the vast majority of good users can pass unchallenged.

Arkose Labs also produced a custom white paper for the bank, detailing its fraud prevention and user experience philosophy and explaining in detail how the solution would work once implemented.

Results

The Arkose Labs platform allowed the bank to drastically slash the number of successful attacks, protect genuine users, and ensure a safe digital banking experience for all customers.

The platform does not just mitigate the effects of fraud but provides powerful remediation which blocks 100% of malicious bot traffic, and enables businesses to deflect attacks from bots, skilled cybercriminals, and sweatshop outfits. This allows good users to maintain the seamless digital authentication experience they have grown accustomed to while providing friction and frustration to fraudsters.

Furthermore, a dedicated managed services team works with every Arkose Labs client to ensure the platform is always fine-tuned to deal with the latest evolving threats. Arkose Labs regularly provides custom insights to the bank, allowing it to adapt and alter its own internal fraud controls as needed.

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