Leading Fintech Slashes Account Takeovers by 75% and Saves $100K Weekly with Arkose Titan

A prominent U.S. fintech serving over 20 million customers with digital banking and personal financial management tools. A high-value target for credential stuffing attacks aimed at compromising customer accounts and draining funds at scale.

The Challenges

Approximately 30,000 failed login attempts per day, predominantly credential stuffing attacks targeting customer accounts.

Sophisticated bots bypassing traditional web forms and hitting back-end APIs directly, enabling high-volume, high-velocity account takeover attacks.

Compromised accounts resulting in $100,000 in weekly losses.

Needed to stop attacks without adding friction to a platform known for its seamless consumer experience.

The Arkose Titan Solution

Arkose Bot Manager deployed across login forms and backend APIs, with a secure token integrated into the web application and mobile SDK to validate each request in real time.

Behavioral fingerprinting, velocity monitoring, and proprietary IP intelligence used to identify and stop malicious bot traffic.

Arkose Device ID implemented to add a persistent device intelligence layer, combining stateless and stateful identification to distinguish genuine consumers from threats at app launch and across all critical touchpoints.

Device ID enabled detection of account takeovers from unrecognized devices, fake account creation based on inconsistent device data, and coordinated fraud ring activity.

Full device visibility from first interaction with no additional vendors or complex integrations required.

Business Results

75% reduction in account takeovers following deployment.

$100,000 in weekly losses eliminated from compromised accounts.

Improved device identification accuracy, enabling earlier detection of first-time attackers.

Consumer experience fully preserved with no added friction.

> "We're really good at making sure that known fraudsters aren't able to keep targeting us with the same device, stolen identity, or what have you. But we weren't as effective at catching them early on, the first time. That's where device identification becomes crucial."
>
> **— Engineering Leader**

SCHEDULE CALL WITH AN EXPERT

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.