Fintech Pioneer Launches Securely: Proactive Protection for High-Risk Mobile App

A major player in the crypto space, this organization launched a new mobile-first social application designed to combine digital currency rewards with social engagement—creating a high-value target for fraudsters before day one.

The Challenges

Pre-Launch Vulnerability: The app needed proactive fraud protection before launch, not reactive fixes after abuse patterns emerged.

Mobile-First, High-Risk Design: A 100% mobile, social-based app offering digital currency rewards created prime conditions for fake account creation, account resale, and rewards exploitation.

Geographic Fraud Exposure: Operating in high-fraud regions like Bangladesh, Nigeria, and Indonesia risked either unsustainable fraud costs or abandoning viable markets entirely.

Compressed Timeline: Aggressive launch deadlines required rapid deployment, stress testing, and integration—without room for trial and error.

Low-and-Slow Human Fraud: Beyond automated bots, sophisticated human fraudsters creating "legitimate-looking" accounts required behavioral pattern detection that takes weeks to establish baseline signals.

The Arkose Titan Solution

Proactive Production Planning: Deployed Arkose Titan before the app went live, shifting from traditional proof-of-value to production readiness—allocating SOC resources and fraud mitigation strategies pre-launch.

Mobile-First Device Intelligence: Leveraged Arkose Device ID to create persistent fingerprints across mobile devices, tracking bad actors even as they rotate accounts and attempt to blend in with legitimate users.

Behavioral Pattern Detection: Focused on identifying low-and-slow human fraud through week-over-week behavioral analysis, catching sophisticated abuse that evades traditional bot detection.

24/7 SOC Monitoring: Arkose's Security Operations Center continuously analyzed traffic to identify anomalies and fraud patterns unique to the app's social-crypto hybrid model.

Intent Classification: Delivered real-time analysis distinguishing legitimate user behavior (including beneficial bots like autonomous shopping agents) from nefarious account creation and rewards exploitation.

Business Results

Zero-Day Fraud Readiness: Launched with enterprise-grade fraud defenses in place, avoiding the costly cycle of launch-detect-remediate that plagues new apps.

Market Expansion Without Compromise: Maintained operations in high-fraud geographies that would otherwise require shutdown, preserving revenue opportunities while controlling abuse.

Friction-Free Growth Strategy: Enabled the customer to run user acquisition campaigns and optimize conversions without fear of fraudsters exploiting promotional offers.

Expert Partnership Model: Provided strategic guidance navigating the tension between e-commerce growth teams and security requirements—acting as the bridge between revenue goals and fraud mitigation.

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.