Sharing Economy Giant Eliminates ~$300K in Daily SMS Toll Fraud with Arkose Titan

A sharing economy leader with 150 million users across 200+ countries, this company operates a high-volume marketplace where platform integrity is paramount.

The Challenges

Low-and-Slow SMS Abuse: Sophisticated fraudsters exploited SMS workflows by triggering one-time passwords (OTPs) to premium-rate numbers to collect payouts from colluding carriers. Global SMS Toll Fraud was measured at $300K during just one 12 hour period where Arkose Titan was not engaged.

Human-Driven Threats: Attacks primarily originated from humans or human fraud farms—rather than bots—making them notoriously difficult for standard technology to detect.

Inadequate Legacy Systems: The company's internal device identification and previous vendor solutions failed to surface the "low-volume" fraud blending with legitimate traffic.

The Arkose Titan Solution

Deterministic Risk Signals: Leveraged the unified Arkose Titan Platform to gather reliable risk data, providing full visibility into suspicious device behavior.

Arkose Device ID Integration: Implemented Arkose Device ID into the SMS flow to provide deterministic signals and rich device identification data whenever a user requests an OTP.

Multi-Layered Platform Approach: Leveraged Arkose Titan which includes both Arkose Device ID and Arkose Bot Manager to create a unified defense against both automated volumetric attacks and human-initiated fraud.

Contextualized Data Intelligence: Delivered detailed data directly to the customer's internal teams, allowing them to distinguish between recognized devices and high-risk activity.

Business Results

Massive Savings: By blocking an estimated $300,000 in SMS toll fraud daily, annual savings could approach $100 million.

Detection of Human Fraud Farms: Uncovered specific high-volume patterns including one device requesting 140 OTPs in a single hour, suggesting organized fraud farm activity.

Global Threat Visibility: Pinpointed 724 unique abusive devices operating from known SMS toll fraud hotspots, including Egypt, Singapore and Pakistan.

Data-Driven Control: Empowered the company to take targeted action against fraud without disrupting the experience for its 150 million genuine users.

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.