Rideshare Giant Saves $2.5M Annually in SMS Toll Fraud Costs

A prominent rideshare and delivery giant prioritized streamlined customer acquisition through online sign-ups but inadvertently opened doors to SMS toll fraud, causing skyrocketing SMS bills that threatened millions in annual fraudulent charges.

The Challenges

SMS Toll Fraud at Scale: Cyberattackers obtained phone numbers from premium-rate carriers through collusion or weak telecom security, then deployed bots to trigger OTPs, causing millions in fraudulent SMS charges while splitting proceeds with carriers.

Friction-Sensitive Customer Base: Platform's user base was extremely sensitive to online friction, requiring any verification mechanism to operate seamlessly in background without hindering legitimate signups.

Limited Traffic Visibility: Lacked sufficient insight into customer acquisition traffic patterns and potential threats including account takeover, promotion abuse and fare scraping.

The Arkose Titan Solution

Comprehensive OTP Protection: Deployed Arkose Titan platform across every touchpoint safeguarded by OTPs during registration, aggregating real-time device, network and behavioral signals to spot hidden signs of bot and human-driven attacks.

Targeted High-Risk Country Strategy: Focused on sessions from 5 countries with highest SMS costs, analyzing and selectively choosing unique threat signatures as basis for applying friction.

Adaptive Challenge Deployment: Presented Arkose challenges to suspicious sessions, posing difficulties for bots that forced attackers to abandon attempts or pivot to human fraud farms, which were also effectively thwarted.

Passive Authentication for Legitimate Users: Built detection models on passive authentication techniques, enabling genuine users to pass through unchallenged and navigate smoothly with little to no interference.

Business Results

$2.5M in Annualized Savings: Achieved approximately $2.5 million annual reduction in SMS toll fraud spend for select high-risk countries.

99.5% Frictionless Experience: 99.5% of low-risk traffic passed through unchallenged, with the 0.5% that experienced challenges exceeding industry completion standards.

94.4% Attack Abandonment Rate: 94.4% of challenged sessions immediately gave up, indicating high detection accuracy and effective bot deterrence.

Enhanced Traffic Visibility: Major improvements to top-of-funnel data including IP intelligence, device intelligence and fingerprinting, real-time IP aggregation and offline page load ID analysis.

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.