Global Social Media Platform Saves $3M Monthly in SMS Toll Fraud

A global social media platform with millions of active users worldwide was losing hundreds of thousands of dollars monthly to SMS toll fraud, as attackers used automated bots to trigger OTPs to premium numbers.

The Challenges

SMS Toll Fraud at Scale: Bad actors registered mass fake accounts and deployed bots to trigger OTPs to premium numbers at $0.095 per SMS, risking millions annually in fraudulent charges.

International Revenue Share Fraud (IRSF): Fraudsters colluded with high-cost telcos to profit from SMS messages, redirecting verification codes to premium rate numbers they controlled and sharing profits with compromised carriers.

Bot-to-Human Attack Evolution: When initial defenses blocked bot attacks, fraudsters shifted to coerced human labor to continue exploiting SMS verification flows.

The Arkose Titan Solution

Comprehensive SMS Flow Protection: Deployed Arkose Titan platform in front of SMS verification process at registration and signup to detect and mitigate IRSF attacks before OTPs were triggered, and stopping automated bot scripts used by fraudsters.

Real-Time Device and Behavioral Analysis: Leveraged embedded machine learning to assess devices in real time alongside behavioral intelligence, identifying fraudulent sessions and presenting challenges to suspected attacks.

Adaptive Response to Human Labor: Implemented aggressive countermeasures to eliminate exploitation when attackers pivoted from bots to coerced human fraud farms.

AWS-Powered Global Infrastructure: Leveraged strategic AWS data center locations to detect, isolate and completely mitigate attacks across web and mobile applications worldwide.

Business Results

$3M Monthly Savings in SMS Fraud: Achieved $3 million per month reduction in fraudulent SMS charges across high-risk countries, demonstrating immediate and substantial ROI.

72% Reduction in Targeted Country: Slashed SMS toll fraud spend by 72% in the most heavily attacked country, restoring profitability to previously threatened operations.

Eliminated Human Fraud Farm Exploitation: Reduced throughput for coerced human labor to 0% in targeted regions, completely shutting down SMS flow exploitation.

Reduced Downstream Operational Costs: Saved millions in support time managing compromised accounts, fraud case management for payment teams, and infrastructure costs from removing high volumes of bot traffic.

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.