SOLUTION BRIEF

SMS Toll Fraud

Protect your business from increasingly sophisticated, AI-powered attacks

The Evolving Threat Landscape

Have you ever wondered why it's often the CFO who first uncovers SMS toll fraud? It's because they meticulously track financial transactions and expenditures, making them more likely to spot the unusual patterns and discrepancies that signal these attacks. In SMS toll fraud—also known as SMS fraud, IRSF (International Revenue Share Fraud) or SMS pumping—bad actors exploit high-volume, high-cost SMS messages to premium-rate phone numbers. They move through the registration process with lightning speed, abandoning flows immediately after triggering the SMS send. By the time your company realizes you've been charged for non-existent registrations, the scammer has disappeared with their share of the inflated charges, and the money is almost impossible to recoup.

The Acceleration of Automated Attacks

The threat has intensified dramatically. What once required manual coordination and human effort now operates through highly sophisticated automation at unprecedented scale. Modern SMS fraud attacks demonstrate capabilities that fundamentally change the threat landscape. These threat actors:

Operate across global networks simultaneously
At Arkose Labs, we're tracking SMS toll fraud activity from 43 countries, with attacks coordinated across time zones and geographies without human intervention.

Adapt tactics continuously
Attackers pivot from basic bots to machine learning solvers to human fraud farms, switching strategies each time defenses improve.

Execute at machine speed and scale
Automated systems can trigger thousands of fraudulent SMS sends per hour without human intervention.

Mimic legitimate user behavior with precision
Advanced pattern recognition and behavioral analysis make fraudulent traffic increasingly difficult to distinguish from real users.

Systematically identify and exploit SMS attack surfaces
Automated scanning identifies every SMS touchpoint: sign-up flows, password resets, two-factor authentication and notification triggers.

The financial impact is staggering.

> A large gig-economy organization without proper protection experienced **losses of $300,000 in just 12 hours** when the SMS fraud protection feature was temporarily disabled.

Even sophisticated companies with traditional security measures in place are vulnerable. The pattern is clear: attackers are professionalizing and scaling their operations faster than traditional defenses can adapt.

Arkose Titan: Your Defense Against AI-Powered Fraud

The Arkose Titan platform disrupts the economics of SMS fraud, making it too costly and cumbersome for even AI-powered attackers to pursue. Our comprehensive approach delivers the upstream advantage—stopping bots before the SMS is triggered, preventing fraud before costs are incurred. This fundamental difference means no SMS is sent, no cost is incurred and no fraud occurs, while legitimate users remain unaffected.

Coordinated Intelligence Across the Stack

Arkose Titan's unified API coordinates device fingerprinting, behavioral analysis, email risk scoring and challenge-response mitigation in real time. When device intelligence flags anomalies, the engine automatically calibrates difficulty and risk signals flow instantly to downstream fraud tools.

Challenge Technology Built for AI Resistance

Our next-gen challenges combine Proof-of-Work computation with multimodal reasoning tasks that cost attackers via LLM vision APIs. Each challenge adds substantial time per attempt, so fraud operations burn through compute budgets fast.

Device Intelligence That Remembers

Multi-layered device identification tracks returning devices while behavioral biometrics establish baseline patterns for mouse movements, typing cadence and interaction velocity. Real-time signals create risk assessments accurate enough to pass 99% of legitimate users with zero challenges.

Transparent Decisioning for Security Teams

Every authentication generates detailed telemetry: 175+ telltale rules showing why we assigned each risk score, complete device intelligence and behavioral analysis. Security teams see our decision logic as it happens, enabling immediate investigation.

Consortium Intelligence Multiplier

Threat patterns identified at one customer instantly inform protection across our network. When Arkose Labs spots new threats, every customer benefits from updated detection rules within hours.

Platform Capabilities

- **Arkose Bot Manager**
  Advanced bot detection and mitigation
- **Arkose Email Intelligence**
  Real-time email address authenticity validation
- **Arkose Device ID**
  AI-enhanced device identification
- **Arkose Scraping Protection**
  Comprehensive defense against unauthorized scraping
- **Arkose Edge**
  Lightweight server-side API security

Proven Results: Real-World Impact

Organizations protected by the Arkose Titan platform are seeing dramatic results against AI-powered SMS fraud.

- During a 60-day period in late 2025: Saved customers over $12.3 million in prevented SMS fraud losses
- Geographic Reach: Actively defending against coordinated attacks from 43 countries

Industry-Leading Case Studies

Global Payments Leader: After attacks quadrupled year over year and fraudsters evolved tactics continuously—from basic bots to machine learning solvers to human fraud farms—a prominent fintech implemented Arkose Labs protection and achieved:

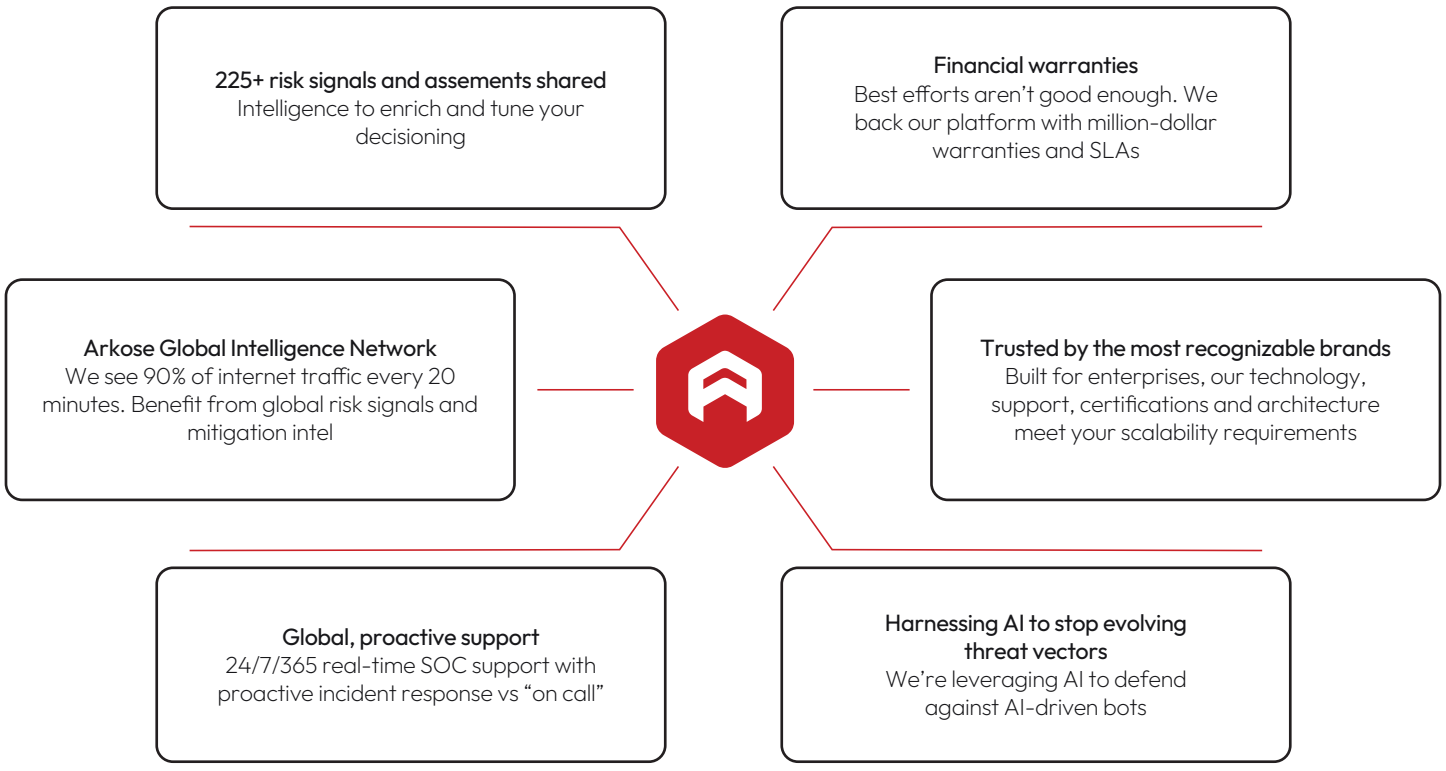
- $3.7M estimated annual savings from reduced SMS fraud
- 70.2% immediate reduction in overall SMS volume within just 3 days

Gig-Economy Leader: The company faced millions in losses as attackers used bots to trigger OTP verifications at scale through premium-rate SMS fraud. The challenge was unique—its customer base was extremely sensitive to friction, making aggressive verification difficult to achieve without harming legitimate users. After implementing Arkose Labs protection:

- Realized $2.5 million in annualized savings from SMS toll fraud
- 99.5% of legitimate traffic passed through unchallenged and zero customer complaints

Cybersecurity Leader: SMS fraud attacks exploited a feature so aggressively that the enterprise made the decision to completely remove this valuable customer acquisition tool from its website. After implementing Arkose Bot Manager protection, the company successfully restored the SMS invite flow and brought back the customer acquisition channel.

The Arkose Labs Advantage



Proactive Defense

Our Global Intelligence Network data consortium enables real-time intelligence sharing across our customer base, creating a unified defense against coordinated AI-driven attacks. Dedicated threat-hunting and disarmament through our ACTIR team proactively identifies emerging AI agent tactics before they scale, while our 24/7/365 SOC actively monitors for new attack patterns and meets all cyber and privacy regulations.

This real-time threat and response visibility provides actionable intelligence for downstream security decisioning, ensuring your team has the transparent risk signals needed to make informed decisions. We combine pioneering technology that proactively identifies attackers using behavioral analysis with proven scale—trusted by the world's largest B2C and global brands, including two of the top three banks. This comprehensive approach is backed by our industry-leading $1M warranty per event for SMS fraud and cyberattacks.

Don't Wait for Your CFO to Sound the Alarm

With AI accelerating SMS fraud to unprecedented levels, the question isn't whether you'll be targeted—it's how much you'll lose before you act. SMS fraud is theft with receipts, visible as hard line items on your telecom invoices. The money lost this month funds the fraudsters attacking you next month. Unlike other security investments that involve theoretical risk reduction, SMS fraud ROI is immediate and measurable.

Are you ready to stop writing checks to fraudsters? To see how Arkose Labs can protect your organization from SMS toll fraud, schedule a call with an expert today.

BOOK A DEMO

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.