Arkose Labs | SOLUTION BRIEF

SMS Toll Fraud

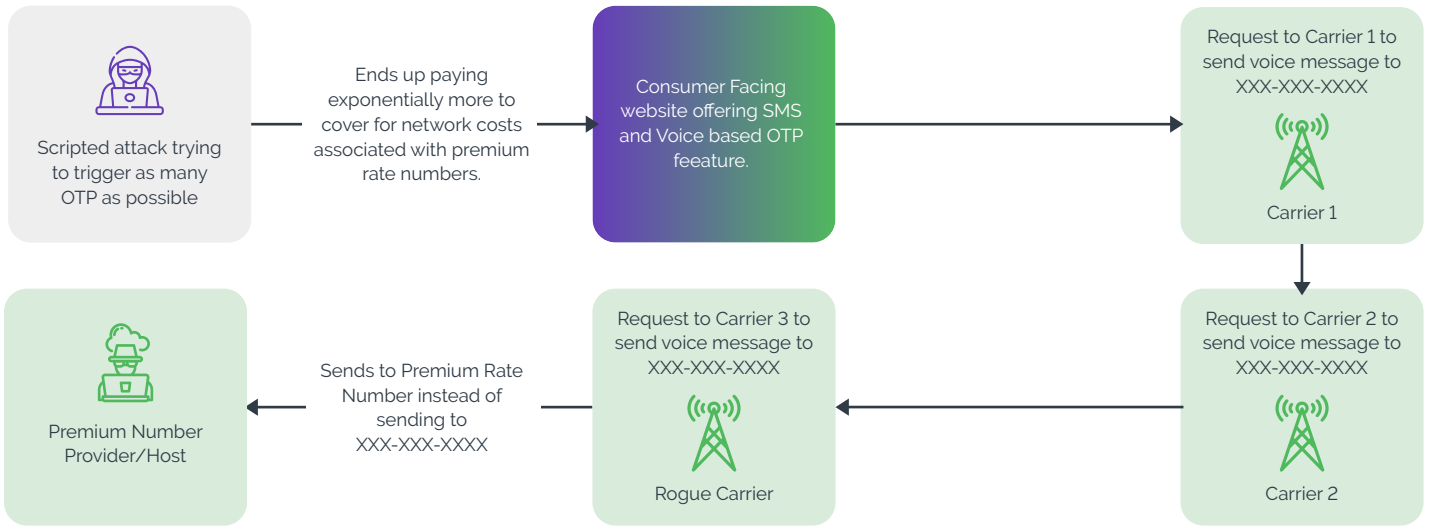
Arkose Labs protects businesses across major industries, including Fortune 500 companies, from SMS pumping and international revenue share fraud (IRSF)

SMS Toll Fraud:

A Rapidly Growing Threat Costing Businesses Millions in Hidden Charges

Digital businesses in diverse industries such as financial services, ecommerce, travel, technology, and others are suffering spiraling costs due to a form of attack called SMS toll fraud, also known as SMS pumping or international revenue share fraud (ISRF). This threat is a growing type of cybercrime in which scammers use automated attacks on digital touchpoints such as account registration, 2FA, and similar mechanisms to send large volumes of SMS messages to premium rate numbers and telecom networks. These fraudulent and expensive SMS transactions can net fraudsters and rogue telecom operators a per-message payout of $1 or more. At scale, these massively inflated charges can amount to millions of dollars a month in hidden costs to a digital business. One recent study showed that SMS toll fraud cost a collective $10 billion in 2021, up from $1.8 billion in 2013.

How it works



The steps of SMS toll fraud are:

1. An attacker initiates a manual or scripted attack on a webpage to trigger SMS-based OTPs. Attackers can opt for high-volume attacks or low-and-slow attacks.
2. The attacked app or website forwards the OTP request to a cloud communication provider.
3. The provider forwards the request to a telecommunications carrier. Multiple network providers spanning international territories are involved before the OTP can reach the intended consumer.
4. In that chain, a compromised carrier, colluding with an attacker, forwards the request to a “premium rate” number on a high-cost network. As a result, scammers exact an extortionate carriage fee, up to $1 or more per transaction.
5. The originating sender (in this case, the web site or app) must absorb the inflated costs, resulting in thousands or millions of dollars in hidden costs each month.

SMS toll fraud is difficult to detect. Don’t let this scam spiral into major unexpected costs to your business.

Arkose Bot Manager Stops SMS Toll Fraud

Arkose Bot Manager stops SMS toll fraud. Our adaptive technology tracks more than 125 data signals to detect malicious bots and block SMS scams in real-time. Our industry-first SMS Toll Fraud Warranty covers up to $1 million in telecom expenses if Arkose Bot Manager fails to defeat an SMS toll fraud attack on an Arkose managed service customer within the SLA.

- Robust defense preventing SMS toll fraud/IRSF
- Effective protection with superior user CX
- Strong partnership against SMS fraud attacks
- Warranty backed by top tier insurance carrier

Arkose Labs helps businesses save money and achieve a better return on investment by detecting bogus account sign-ups and malicious logins, and eliminating the persistent attacks on user touchpoints that trigger SMS messages and OTP verifications. Arkose Bot Manager protects against SMS toll fraud, reduces costs, and restores trust and confidence.

Trusted by the World's Leading Companies

Arkose Labs protects the world's leading brands in major industries such as financial services, ecommerce, travel, technology, telecommunications, and streaming media.

Microsoft · Adobe · chime · ROBLOX · zilch

Expedia · Sony Interactive Entertainment · EA

Real-World Results Stopping SMS Toll Fraud

Gaming Merchant Saved

$3 million

per month in fraudulent SMS charges

Social Media Company Saved

$450,000

per month in fraudulent SMS charges

"Arkose Labs has already saved customers millions in fraudulent SMS charges by stopping these attacks. Frankly, this type of warranty should be table stakes for any security vendor."

— Frank Teruel, Chief Financial Officer

The mission of Arkose Labs is to create an online environment where all consumers are protected from online spam and abuse. Recognized by G2 as the 2023 Leader in Bot Detection and Mitigation, with the highest score in customer satisfaction and largest market presence four quarters running, Arkose Labs offers the world's first $1M warranties for credential stuffing and SMS toll fraud. With 20% of our customers being Fortune 500 companies, our AI-powered platform combines powerful risk assessments with dynamic threat response to undermine the strategy of attack, all while improving good user throughput. Headquartered in San Mateo, CA, with offices in London, Costa Rica, and Brisbane, Australia, Arkose Labs protects enterprises from cybercrime and abuse.

Email:
demo@arkoselabs.com

REQUEST A DEMO