Arkose Labs
PROVEN ACCOUNT SECURITY

Sharing Economy Giant uses Arkose Device ID to identify SMS toll fraud

Arkose Device ID uncovered 31,000+ malicious traffic sessions, equating to an estimated SMS toll fraud cost of $9,000+ over a two-week period. This translates to an estimated $200,000+ in annual savings when mitigation is in place.

OVERVIEW

A global online marketplace and major player in the sharing economy with 150 million users across 200+ countries was facing challenges with sophisticated SMS abuse. Its existing security measures weren't detecting low-volume fraud seamlessly blending with legitimate traffic. Already using Arkose Bot Manager for volumetric automated bot attacks, the company approached Arkose Labs for help mitigating this threat to platform integrity. Not only did Arkose Labs help identify hundreds of suspicious devices engaging in SMS abuse, but the team also uncovered 31,000+ malicious traffic sessions. It's likely that most of these originated from humans or human fraud farms. Arkose Device ID frustrated these bad actors by providing the sharing economy company with rich device identification data to take targeted action against this hard-to-catch fraud.

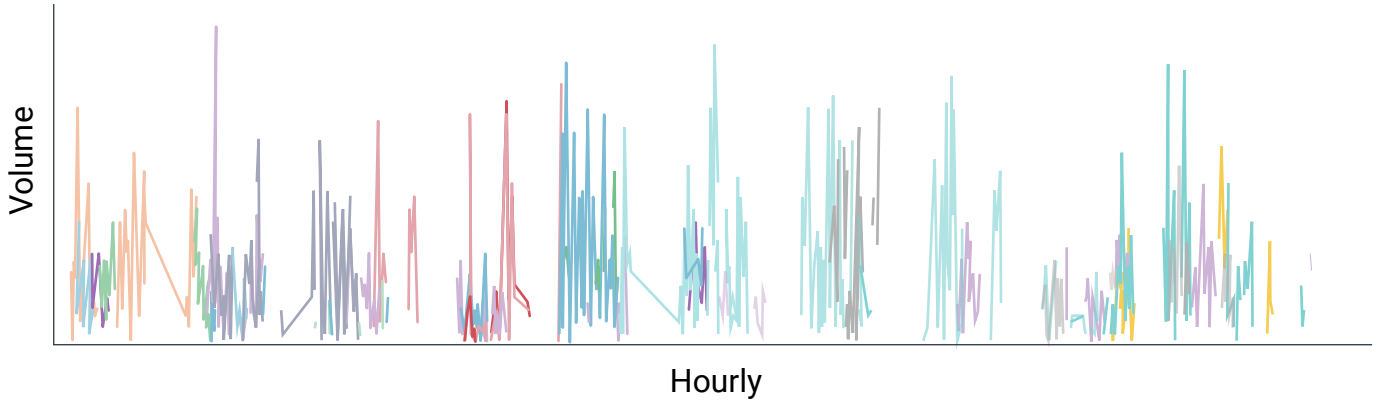
THE BUSINESS PROBLEM

The attack type that this customer was experiencing targeted SMS workflows. SMS toll fraud is a scheme where fraudsters exploit one-time password (OTP) that use SMS verification, triggering SMS messages to premium rate numbers controlled by colluding telecom carriers who share the profits. Merchants are unknowingly charged excessive fees for these SMS messages, often resulting in hundreds of thousands or even millions of dollars in losses.

The data strongly appeared to be coming from real people, rather than bots. These could be individuals operating alone, or most likely, human fraud farms: organized operations where workers are hired to manually conduct fraudulent activities that bypass automated security measures, often operating from physical facilities in countries like Cambodia with dozens or hundreds of people working in shifts on devices connected to the internet.

This kind of human-initiated fraud is notoriously hard to detect, because technology cannot always discern the intent behind the way that devices are being used. In order to pull out the fraudulent activity, the company needed visibility to the data so they could gather and analyze it.

The company wanted a strong device identification solution that could be implemented into the SMS flow whenever a user requests a one-time password (OTP). The business had an internal solution for device identification in use, and had also worked with other vendors in the past, but continued to struggle with mitigating their specific challenge.



ABOVE: A line graph showing suspicious SMS one-time password (OTP) request patterns across devices (represented by different colored lines). Each line shows multiple OTP codes being requested per hour per device, demonstrating "low and slow" attack behavior that mimics human-scale activity.

THE SOLUTION

The approach with **Arkose Device ID** is to give customers the rich data that they would need to recognize specific devices. By identifying known and recognized devices, this solution gives companies the chance to reduce challenges for good users, while detecting suspicious activity before it escalates.

The Arkose Labs team implemented **Arkose Device ID** and used identifiers to provide deterministic signals, then provided the data directly to the customer to give it full visibility into fraudulent traffic in its SMS flow.

Taking action against fraud can be a double-edged sword if not handled carefully. The Arkose Labs approach is to gather strong and reliable risk signals and share those with the customer. Arkose Labs puts the keys to anti-fraud strategy in customers' hands by providing rich, contextualized device data and allowing them to choose which actions to take.

DEMONSTRATED RESULTS

Analysis of data over a two week period shows that since the implementation of **Arkose Device ID** on the customer's OTP flow, there were 724 unique devices which were sending an OTP request more than ten times within 24 hours. Since this behavior is irregular, it is possible to deem these devices abusive.

Drilling down, the analysis revealed **31,452** total attempts to request an OTP coming from these devices during this period, and in most cases, these human-initiated requests were verified. One device in particular sent 140 requests in a single hour: a high volume that suggests a human fraud farm was responsible for the attack. Many of the devices sending the most requests were from Egypt, while others were from the U.K., Singapore, Pakistan and Poland. Many of these countries are known hotspots for SMS toll fraud.

Catching these types of attacks is critical for businesses, so that they can choose which approach to take. By using Arkose Device ID alongside Arkose Bot Manager, the customer has access to the detailed data it needs to take action against expensive SMS toll fraud attacks.

SCHEDULE CALL WITH AN EXPERT