www.mitto.ch
info@mitto.ch

HOW MITTO PROTECTS AGAINST ARTIFICIALLY INFLATED TRAFFIC FOR SMS AND OTP

WHAT IS ARTIFICIALLY-INFLATED TRAFFIC?

SMS with OTP has been the most common authentication method globally for enterprises – A2P two factor authentication messages contribute to over 25% of SMS volume worldwide. But there is a disturbing trend of artificial inflated traffic (AIT) causing costs to rise and SMS traffic to fall short of its goals.

According to the Communications Fraud Control Association, telecom fraud costs have risen 12% in 2023, almost $39 billion lost to fraud. According to Juniper Research's recent report, Global Mobile Authentication Market 2023-2028, the rise of artificially inflated traffic, where enterprises pay for authentication or other SMS traffic for users that don't exist, is a key driver of increased SMS costs.

Artificial inflation of traffic scams can drain money from your company, especially if you send a high volume of SMS. In addition, this kind of traffic can ruin your brand's trustworthiness or create misleading engagement. You may think you have a lot of new users, but a big proportion of them could be fake. Enterprises with the largest user bases, such as big tech companies with millions or billions of users, will be affected the most.

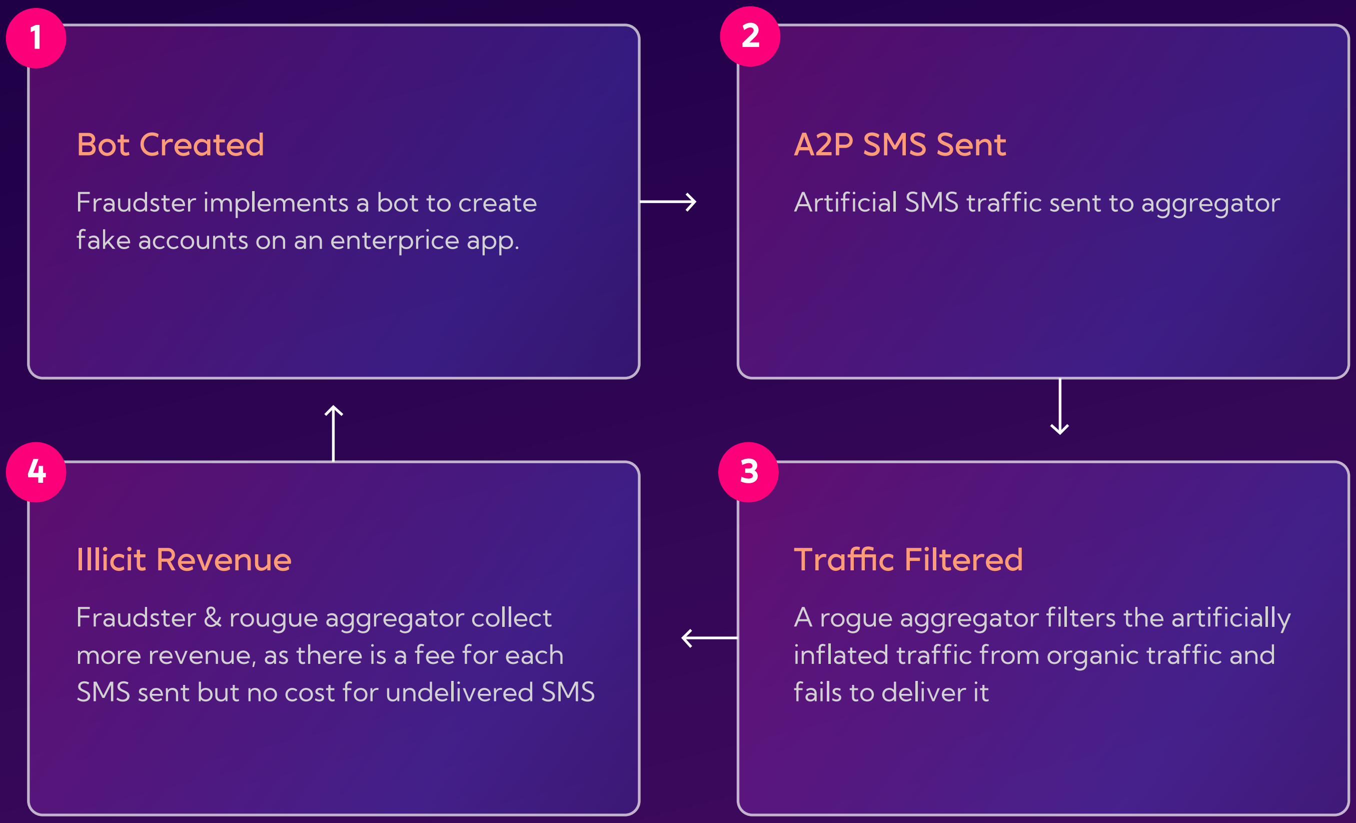
According to a recent report by the Mobile Ecosystem Forum (MEF), 60% of companies believe that AIT is increasing in frequency. In early 2023, one massive tech brand reported that it may have lost $60 million per year to bogus bot traffic. Enterprises are expected to spend $8.4 billion on messaging traffic that is not needed, an 80% increase from 2022. So how are these bad actors taking advantage of artificially-inflated traffic?

HOW ARTIFICIALLY-INFLATED TRAFFIC FOR SMS WORKS

One of the most common types of artificially-inflated traffic for SMS begins with fraudsters using bots to create fake accounts that require OTP. Since OTPs aren't considered spam by MNOs, MNO firewalls that protect against certain types of spam are bypassed.

By implementing AI, fraudsters can inflate traffic on a large scale. If a brand suddenly gets a huge amount of OTP traffic, there is likely an issue – unless there is a Taylor Swift concert pending! Be aware that AIT can present as a large-scale event, or a slow volume of fake traffic that incurs costs over time.

A COMMON AIT CYCLE



1

Bot Created

Fraudster implements a bot to create fake accounts on an enterprice app.

2

A2P SMS Sent

Artificial SMS traffic sent to aggregator

3

Traffic Filtered

A rogue aggregator filters the artificially inflated traffic from organic traffic and fails to deliver it

4

Illicit Revenue

Fraudster & rougue aggregator collect more revenue, as there is a fee for each SMS sent but no cost for undelivered SMS

HOW ARTIFICIALLY-INFLATED TRAFFIC FOR SMS WORKS

- ✓ Bots are created by a fraudster on apps with a weak registration process (or a lot of SMS A2P activity such as bank transactions)

- ✓ A fraudster may collaborate with a rogue SMS aggregator to identify and separate the artificial from organic traffic

- ✓ The rogue aggregator may suppress the delivery of the artificial traffic (SMS trashing), while allowing organic traffic to go through.

    - ✓ Though the rogue aggregator fails to deliver a portion of SMS messages, they charge the customer for these messages, thus receiving more revenue and reducing their costs by not sending on a percentage of the SMS traffic

    - ✓ The fraudster and rogue aggregator share the revenues, as there is a fee for each SMS sent

- ✓ OR the rogue aggregator allows the traffic to go through to meet unrealistic commitments about traffic volume they may have with an MNO

- ✓ The cycle is repeated

Since some AIT activity can mimic real customer behavior, we need careful monitoring, robust data, and strong industry experience to prevent AIT.

HOW MITTO PREVENTS ARTIFICIAL TRAFFIC FOR SMS AND OTP

Mitto proactively protects and defends its customers from artificially-inflated traffic. As the exclusive gateway for many operators, and as a service provider to many major enterprises, we have access to a plethora of data that other companies don't have about legitimate and illegitimate SMS traffic. With our real-time traffic monitoring, we have a unique ability to discover trends and can notice anomalies – for example, if we see rideshare SMS traffic in a place where that rideshare company doesn't operate, we know something's not right!

Based on our alerts, monitoring and data trends, we can detect suspicious activity and create fingerprints to prevent attacks and replicate successes. We keep a close watch on traffic trends of new suppliers with a special rate, and we can switch suppliers and block routes to reduce the volume of fraud. Here at Mitto, we constantly analyze a number of parameters such as volume spikes, DLR (delivery reporting) trends, velocity, destination, and number ranges, and use predictive analysis to continuously improve our ability to detect patterns of real and artificial traffic, and spot red flags.

For example, our knowledge of fraudulent number ranges using Global Number Range (GNR), Mobile Number Portability (MNP), and other proprietary data allows us to block illegitimate numbers in advance from being used. We can also identify and block non-reputable aggregators. We not only have a machine learning algorithm to prevent AIT fraud, we also have experienced and hands-on SMS routing experts who can monitor and block traffic, make sure traffic is consistent with where a brand operates, and minimize false positives.

DEPENDING ON CUSTOMER NEEDS, WE OFFER THE FOLLOWING OPTIONS:

1. Inform our customers immediately when we see any anomalies or fraud-related patterns happen, and give the customers the option to block problematic traffic.

2. Upon customer request, Mitto can manage blocking of problematic traffic on behalf of the customer

MITTO HELPS CREATE A SAFER MESSAGING ECOSYSTEM

We help you mitigate the danger of AIT in A2P SMS, and prevent revenue loss and hidden costs while allowing enterprises to maintain user trust and loyalty.

IF YOU'RE READING THIS...

... odds are you already know what AIT is. Don't take a chance on letting the problem continue. Improve your revenue stream and put an end to bad actors hurting your brand.

Contact Mitto Today