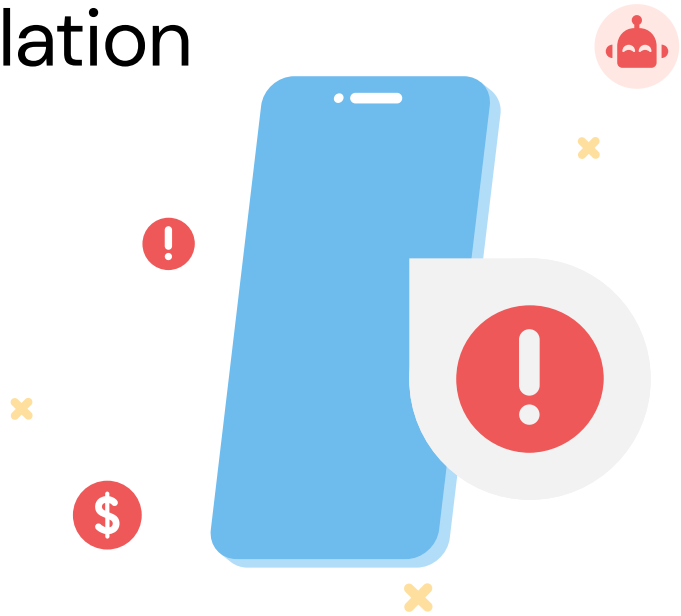
sinch

E-BOOK

Artificial Inflation of Traffic (AIT): a growing threat to the messaging ecosystem

What is Artificial Inflation of Traffic (AIT)?

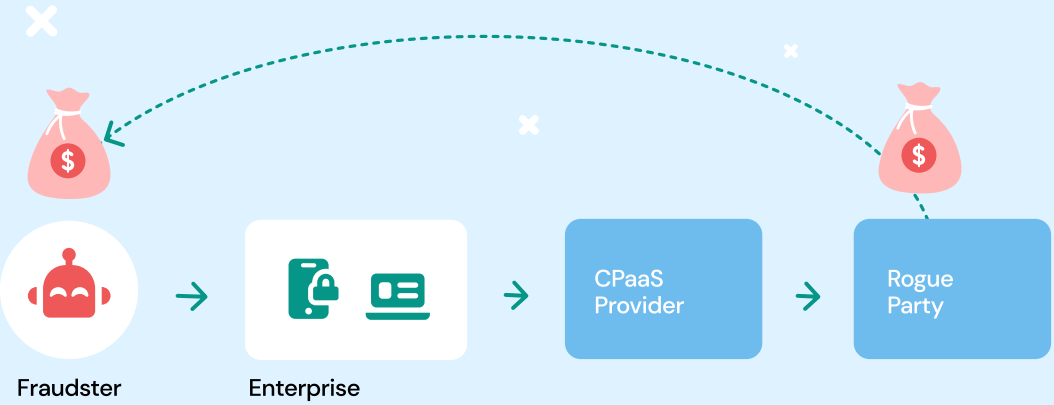


AIT is a type of SMS fraud that generates high volumes of fake traffic via mobile applications or websites.

According to recent Mobilesquared findings presented at the MEF Global Forum, the biggest threats to messaging in 2022 were grey routes, AIT, and SMS phishing – with AIT projected to take the lead in 2023.

A common AIT scenario looks something like this:

- A fraudster designs a bot to create fake accounts.
- The bot triggers a one-time passcode (OTP) SMS to mobile numbers.
- The fraudster partners with a rogue party to intercept the inflated traffic without actually delivering messages to the end user.
- Together, they claim the revenue, share the profits...
- ... and repeat the process to inflate revenues further or tamper with conversion statistics.
- As the owner of the application, you'll likely be stuck paying the bill as messages were delivered. It's common for fraudsters to inflate traffic to long-distance locations because international destinations with high delivery costs yield the most profit.



Common case: AIT exploits A2P SMS verification, where an OTP is sent to verify users phone numbers during the registration process.

Rogue party (SMS aggregator, mobile operator) conspires with a fraudster and the fraudster then takes a share of the profits while the enterprise incurs inflated A2P SMS cost without added value.

Why is AIT on the rise?

There are three main factors explaining the rise of AIT fraud:

- With increased A2P SMS costs, the profit potential of AIT is more and more attractive to fraudsters. And since the cost of SMS can be high, some will choose to use profits from AIT schemes to pay for legitimate SMS traffic.
- AIT is difficult to identify as it's not regulated under common SMS agreements and regulations. This means it can bypass MNO firewalls, because OTPs aren't considered spam.
- Parties could use fraudulent means to generate traffic to stay ahead of the competition and drive up their value in a crowded market.

How to spot AIT?

- Sudden increase of traffic to new destination.
- Unlikely geographical destination for the customer to send SMS to.
- Destination numbers are in sequential or nearly sequential order
- Changes or decline in conversion rates.

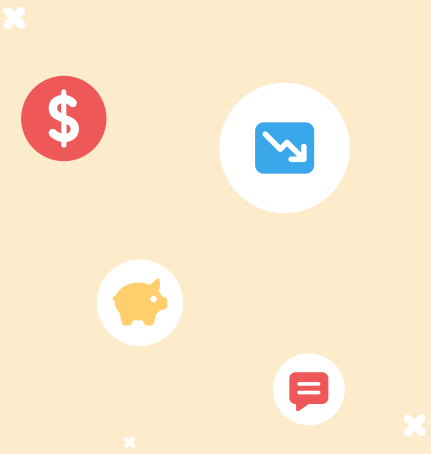
What's the real impact of AIT?

The primary impact is financial. There are significant profit losses associated with AIT fraud for enterprises. Twitter, for instance, is reported to have lost $60 million per year to AIT.

AIT fraud could go on completely undetected and become apparent only after comparing message volume delivery to projected returns.

Brand reputation could also be at risk as businesses could be perceived as illegitimate and non-compliant by their customers. If a user receives multiple OTPs that they didn't request, they'll likely question the business's integrity.

But businesses aren't the only ones standing to lose; AIT is an issue for the entire messaging ecosystem, threatening operators and message providers alike. With the rise of SMS rates and new regulation procedures, brands are starting to consider other channels. Mobile operators also risk losing A2P SMS revenue because brands are shifting to other authentication methods.

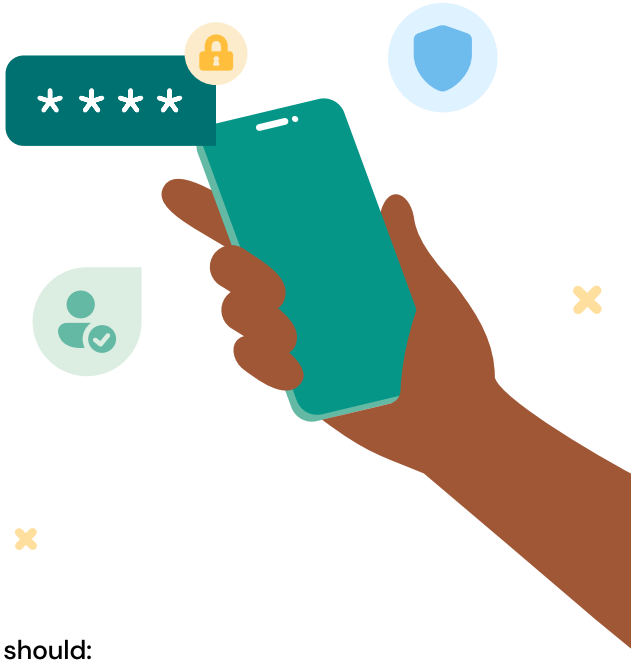


What can be done?

Although there isn't a specific playbook on fighting AIT, businesses can implement a few prevention and detection methods that can significantly reduce the number of fraudulent attacks:

- Monitor very large volumes of "out-of-place" outgoing messages: Add additional checks on IP, user, or device identifiers when a new user creates an account. This can help identify suspicious behaviors and take action before the fraudster has the chance to request a message be sent.

- Monitor conversion rates (CR) of OTP SMS: In many cases, perpetrators can't keep up with high CRs of AIT.

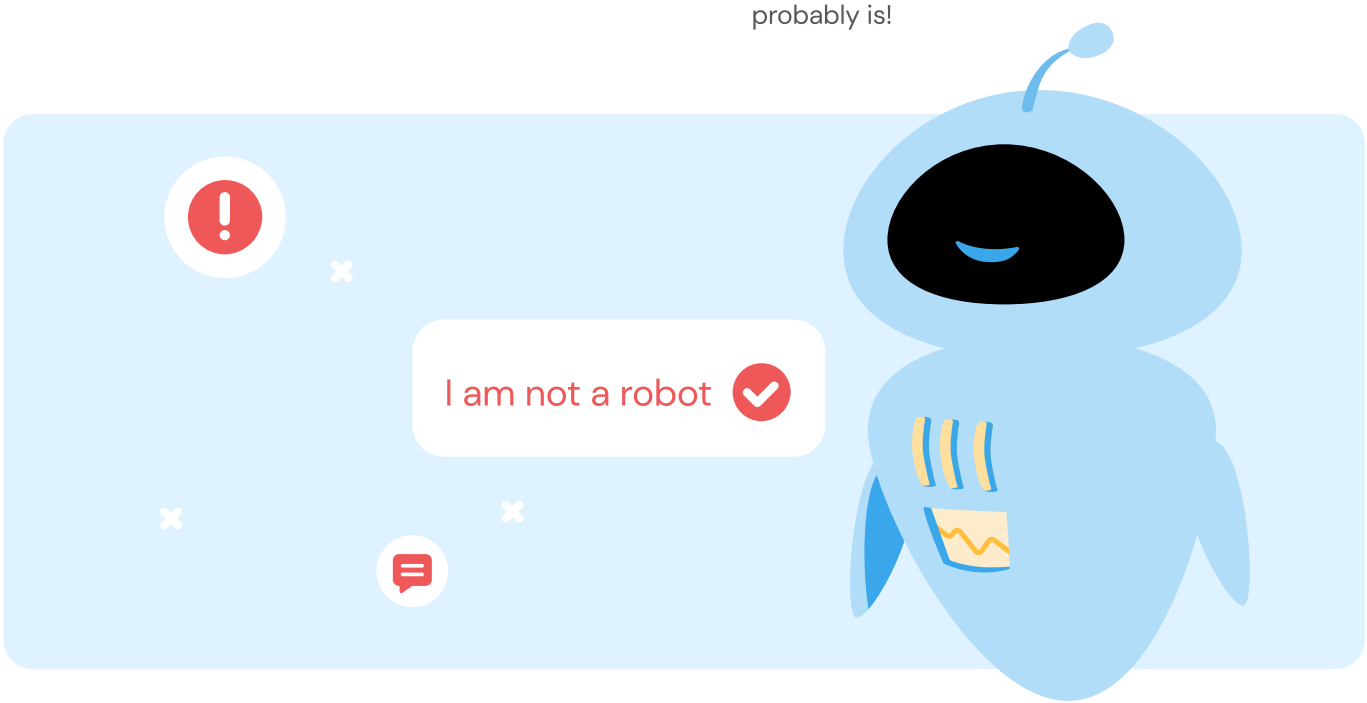


Businesses should:

- Limit the number of attempts to request SMS using the same IP address or device.
- Disable the option of sending messaging to unused destinations (most cases happen in countries where brands don't operate).
- Use CAPTCHA and similar tools to block bots.
- Use Sinch SMS Verification, which allows businesses to increase conversion and prevent fraud by monitoring their conversion rates in real-time to help identify AIT.

Operators should:

- Ensure legitimate usage of allocated ranges when leasing numbers and number ranges to third parties.
- Select only trusted and respectable partners for SMS traffic delivery to networks with enterprise customers to decrease the number of intermediaries between originators and subscribers.
- Be cautious of accepting over-ambitious revenue commitments from vendors seeking bespoke agreements. If it sounds too good to be true, it probably is!



How can Sinch help you address AIT?

As a cloud communications leader, Sinch is committed to following the highest standards for transparency and accountability. That's why we work with customers to reduce the risk of AIT:

- We monitor traffic to identify abnormal usage and inform clients if we detect it.
- We block detected AIT fraud on destination network level and MSISDN range level.
- We offer AIT detection as a part of Sinch SMS Verification.
- We contribute to a cleaner ecosystem:
  - Our routing strategy ensures fraudsters are excluded.
  - We uplift partner agreements to add AIT clauses.
  - We maintain a registry of high-risk destinations.
- We're also currently running an automatic fraud detection alerting system.

600 direct carrier connections to operators, actively monitor conversion rates.

Sinch is a Business SMS Code of Conduct Signatory under MEF's Trust in Enterprise Messaging (TEM)

We help accelerate market clean-up and educate business messaging solution buyers about the threats associated with fraudulent practices and poor procurement processes.

We also keep our chain of trust as short as possible, with over 600 direct carrier connections to operators, actively monitor conversion rates, and take a legal stance when we have sufficient evidence to inform our suppliers. Learn more about our fight against fraud in SMS.

Find out more at sinch.com