i3Forum

INTERNATIONAL INTERCONNECTION FORUM FOR SERVICES OVER IP

Fraud classification and recommendations on fraud dispute handling

Release 1.0 – October 2023

1 SMS Fraud Disputes for AIT Fraud

Fraud can be committed on several levels, impacting many telecom parties and generating considerable losses overall:

1. Origin of the traffic: subscription fraud, impersonation, SMS spamming, malware in mobile devices, platform hacking, SIM farms, SMS reseller apps, etc.
2. Traffic/content: Artificially Inflated SMS Traffic (for example via bots), no actual content (or fraudulent content), fake OTP traffic, etc.
3. Destination of the traffic: number ranges hijacked, traffic short-stopped (such as SMS traffic trashing, fake delivery), fake number ranges, etc

Enterprises (Brands) and Retail Service Providers can be abused by a wide variety of fraud scenarios and more and more SMS fraud disputes get to the international wholesale carriers, emulating the existing process stablished for Voice fraud disputes.

It is important to note that in some cases there is no justification for disputing and withholding payments to the suppliers carrying the traffic down the chain. However, in other cases, disputing fraudulent SMS traffic and negating financial benefit to the direct supplier and the subsequent suppliers in the chain carrying or terminating the traffic may be justified, the ultimate goal being to have a negative financial impact on the fraudsters responsible for the fraud.

1.1 Basic assumptions

All parties in the SMS delivery chain must work together to identify, alert, mitigate, and eliminate AIT fraud (details to be included in the Fight SMS Fraud GLF Code of Conduct).

Disputing SMS fraudulent traffic and withholding the payments to the Supplier helps to mitigate future cases of AIT fraud, in accordance with clause 1.2.2. If payments were stopped in all cases, this would eliminate the incentive for conducting AIT fraud going forward.

The final intention is to financially impact the fraudsters and not just cover for a revenue loss due to compromised platforms or poor security controls.

1. The intended outcome of i3 Forum guidelines is to prevent financial reward to the fraudsters.
2. Only the portion of traffic which can be shown as fraudulent should be considered disputable.
3. The SMS fraud dispute process is only applicable for the following SMS fraud types: SMS Artificial Inflated traffic (AIT), as described in section 1.3.

4. The suppliers should be notified of the alleged fraud case as soon as it is noticed so that they can put measurers in place to stop payments whilst the investigation continues. The Supplier should use reasonable efforts to stop the payment flows corresponding to the alleged fraudulent traffic.
5. The evidence/records (claim) substantiating the allegedly fraudulent traffic needs to be shared within a reasonable timeframe as defined in the Contract Fraud Clauses (1.3). Otherwise, any payment should be released to avoid holding any innocent carrier hostage.
6. Legal/regulatory requirements may supersede voluntary industry practices in determining what evidence/records are required to deny payment and may require in-country legal and/or regulatory action.
7. The outcome of the investigation may require the release of funds for payment to all suppliers in the chain where it is not possible to permanently deny payment to the suspected fraudsters.
8. The originating service providers or Enterprises are responsible for securing their platforms, processes and networks from exposure to fraudulent traffic/use and should be prepared to fulfill their financial responsibility to the downstream suppliers unless payment is denied to the fraudsters.
9. The minimum threshold (disputed value) to accept/refuse disputes due to fraud is suggested to be agreed by the parties in the Master Agreement ruling their relationship.
10. If, for any reason, the carrier is not able to withhold the payments from the downstream players, the liability remains with the originating service provider or Enterprise. The carriers agree to use reasonable efforts to follow this process.
11. When possible, in case of suspicious traffic, and subject to contractual obligatons, the carrier may block the suspicious traffic.
12. If a carrier receives a credit note from the supplier(s) carrying the fraudulent traffic, the corresponding revenue is issued as a credit note to the Sender.

1.2 Fraud Disputes

1.2.1 Fraud dispute principles and conditions

The Sender remains liable for the traffic sent. Despite this liability, it remains possible to open fraud disputes under certain conditions.

The Sender should notify the Carrier/Aggregator of the allegedly fraudulent traffic before the invoice for such traffic period is received or no later than 30 days after the routing of the traffic.

The fraud dispute shall be officially opened by the Sender against the invoice received from the Carrier/Aggregator.The prerequisite to raising disputes due to fraud is that the Sender must provide the Supplier, at minima the details below in English. These details must be provided before the due date of the invoice relating to the alleged fraudulent traffic.

- Fraud case description:

  Fraud case description based on EDR analysis. Through the EDR analysis, the disputing party must explain the fraudulent nature of the traffic. The EDR set must be accurate and contain only the alleged fraudulent traffic and they must be provided together with the fraud traffic notification.

  Any additional information related to the traffic originator that shows suspicious or fraudulent behavior (eg suspicious IP address behavior, suspicious user behavior pattern, sign up process not complete, etc).

  A strong indicator of fraudulent behavior may be the lack of messages terminating on the destination network (I.e messages not arriving/submitted to the destination country MNO).

- Criminal complaint or report from a law enforcement authority (ie police report) or a document issued by a Public authority confirming that (criminal) investigations have been initiated by the respective Authority in the country of traffic origination and showing the fraudulent nature of the traffic. This document should acknowledge:
  a. Description of the fraud
  b. Date(s) of the fraud (mandatory)
  c. Name of the victim (person or company) that was abused and suffered the financial loss
  d. Destination(s) of the fraudulent traffic (mandatory)
  e. Volume of fraudulent SMS (mandatory)
  f. The English translation of this document in case it is established in a different language (mandatory)

1.2.2 Credit notes handling principles

In case of fraudulent traffic disputes, the Carrier/Aggregator will use commercially reasonable efforts to obtain a credit note from its suppliers regarding the fraudulent traffic. The disputing party must pay for amounts referring to fraudulent traffic for which a credit note cannot be obtained from the Carrier's / Aggregator's suppliers.

1.3 Definition of Artificial Inflated Traffic (AIT) on SMS

i3Forum has elaborated a recommendation that focuses on fraud related disputes and the resolution of these in case of Artificial Inflated Traffic (AIT),The goal of this chapter is to help define AIT traffic as well as understand the main use-cases.

Artificial Inflated Traffic (AIT), occurs when a party generates automated messages to fake, invalid or legitimate numbers with the intent to financially defraud other parties in the chain, between the sending party to the destination mobile network.

AIT can be used for both Person-to-Person (P2P) SMS traffic and Application-to-Person (A2P) traffic.

The impacted parties and fraud definition differs in both P2P and A2P use-cases

1.3.1 Definition of AIT fraud in the use-case of Application to Person SMS

Artificial Inflated of Traffic (AIT), occurs when a party generates messages to fake, invalid or legitimate numbers with the intent to:

- Artificially force an originating Enterprise to send A2P SMS :
  - either to a legitimate user of that Enterprise who did not accept to receive A2P SMS from the originating party
  - or to a destination that is not a legitimate customer of that Enterprise
- Artificially force and defraud an originating Enterprise to pay a downstream vendor (SMS aggregator or MNO) for the artificially generated A2P SMS traffic.

AIT contributes to the forced transfer and cascading of money from the sending Enterprise being defrauded to the downstream fraudster that artificially generated the traffic as they can control and collect the revenue of traffic to the destination numbers.

In general, A2P international traffic involves higher revenues and represents most of the AIT fraud when compared with domestic traffic. In 2023, the artificial generation of One-Time-Password SMS is the most straightforward and most used mechanism to generate AIT A2P fraud. However, AIT A2P applies more largely to any mechanism that enables a fraudster to force an Enterprise to send an SMS that was not requested by a legitimate user of that Enterprise with a legitimate intent.

Use-cases (these are two examples, not an exhaustive list) aimed at cascading money flows from the sending Enterprise down the A2P supplier chain:

- A fraudster logs out and logs back into an APP or website, which triggers and forces the App/website to send an authentication OTP codes via SMS. This process can be automated and scale via programable bots.

- A fraudster creates fake accounts and registers a mobile number to services that trigger A2P SMS notification of some sort, for instance, many restaurants with online reservation websites offer a confirmation via an A2P SMS.

1.3.2 Definition of AIT fraud in the use-case of Person-to-Person SMS

Artificial Inflation of Traffic (AIT), occurs when a party generates messages to fake, invalid or legitimate numbers with the intent to:

- Artificially force an originating MNO Mobile subscriber to send P2P SMS to a number of another MNO destination.
- Artificially force an originating MNO Mobile subscriber and its MNO to pay a downstream vendor (a P2P SMS aggregator and/or another MNO) for the artificially generated P2P SMS traffic.

AIT contributes to the forced transfer and cascading of money from the sending Mobile user and its MNO being defrauded to the downstream fraudster that artificially generated the traffic which it can control and collect the revenue of traffic.

AIT with P2P involves sending SMS toward expensive destinations such as premium number ranges or an expensive destination country as a whole. Often, this expensive P2P traffic is found in international P2P.

Use cases (these are a few examples, not an exhaustive list) aimed at cascading money flows down the P2P supplier chain:

- A fraudster infects mobile devices with malware that generates P2P SMS traffic from the mobile device toward expensive numbers, without the consent or knowledge of the end-user
- A fraudster generates SMS traffic by using SIM farms where the SIMs are acquired at advantageous commercial conditions with a unit cost per SMS lower than the wholesale cost charged to send SMS towards premium number ranges.
- A fraudster generates A2P traffic using the sender ID of a premium phone number and creates content that incentivizes the mobile user to reply to this SMS, which will create a high-cost P2P SMS from that mobile user towards the premium number destination.