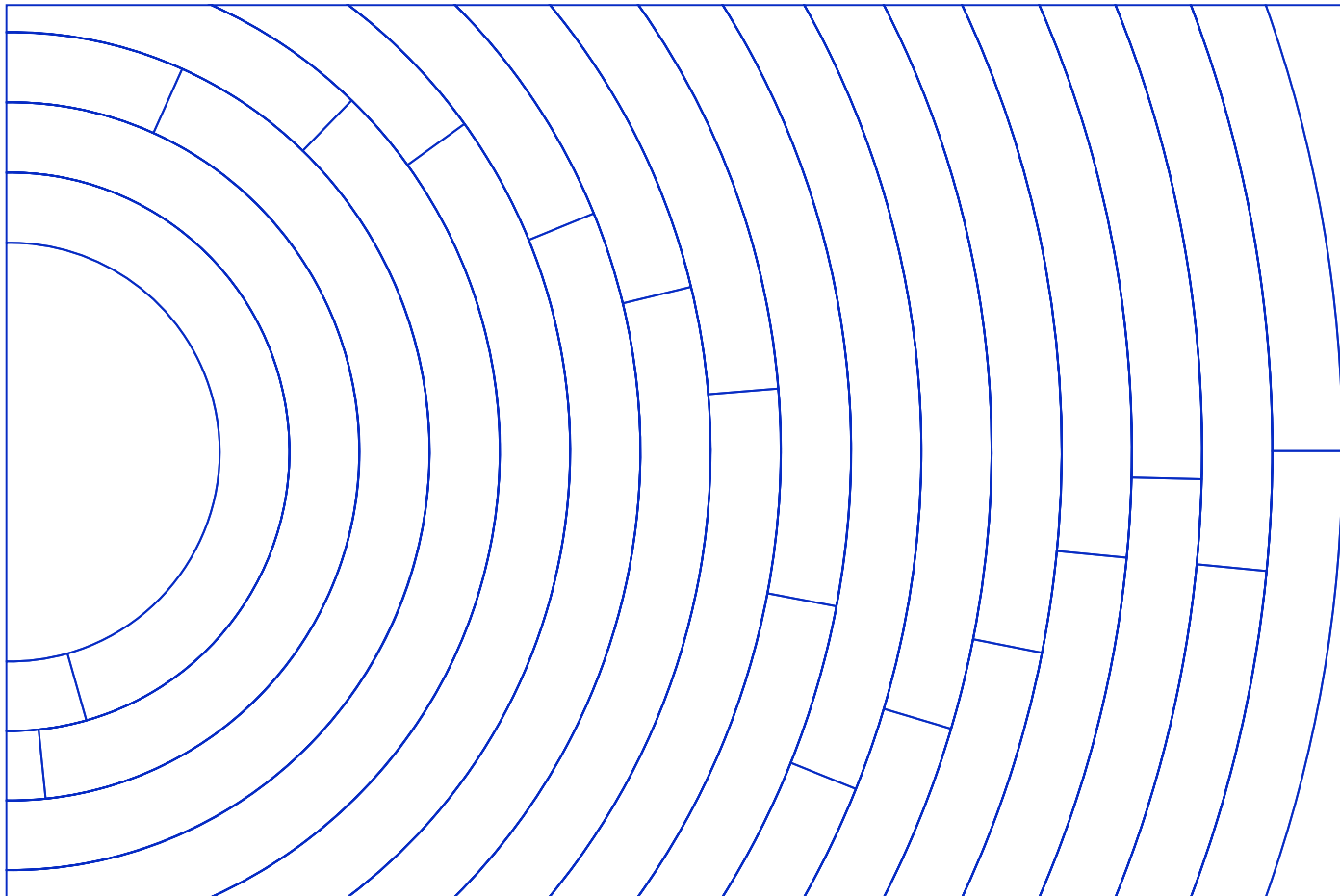


GUIDELINES FOR

Fraud Prevention



PRINCIPAL AUTHOR OTHER AUTHORS	DOCUMENT SHORT NAME	DATE OF LAST CHANGE	REVIEWED BY
GSC Fraud Prevention Workstream	Fraud Prevention Guidelines 2.0	September 2020	GSC Group Members

1. Purpose and scope

1.1 Purpose

The purpose of this procedure is to describe mitigations related to international Revenue share numbers and to set recommendations applicable between the operators. Identify main activities within the carrier to secure that unwanted voice traffic is stopped/ prevented at an early stage.

1.2 Scope

The procedure describes the responsibilities within the carrier and its partners to outline actions required to secure that the carrier acts like a Trusted partner for the interconnect partner.

1.3 I3Forum

I3Forum has published several documents that the carrier should use as source for information for the different types of fraudulent traffic in a more detailed manner.

2. Defining Fraudulent Voice Traffic

Fraudulent traffic includes, but is not limited to, traffic that the Carrier reasonably determines as:

- Calls terminated to repeating interactive voice responses (IVRs) or recordings platforms.
- Not routed for termination in the country of destination and/or to the owner of the number range.
- Involving numbers that are unallocated or unassigned at time of traffic.
- Machine generated, sequential, or simultaneous in nature.

Referenced to I3Forum fraud definition.

3. Fraud prevention activities within the carrier

3.1 Traffic monitoring

Network Operation Center within the carrier should monitor all voice traffic from and to ALL customers with the purpose of identify and stop fraudulent traffic.

3.2 Unallocated ranges

Carrier should only allow traffic to allocated ranges in the specific country code depending on the knowledge of the carrier and depending on the knowledge of the numbering plan.

All known unallocated ranges should be blocked at switch level.

3.3 Hijacked ranges

Carriers should have a Fraud Monitoring system internally to identify potential premium rate/ revenue share traffic. The carrier is responsible for the selection of vendors for a destination. If a selected vendor terminates traffic to hijacked ranges – the vendor needs to be informed and potentially removed from Routing.

3.4 Verification of ranges

Carrier should have access to a test call system to be able to test if a range is potential hijacked or controlled by an IPRN supplier.

Requirements for the test call system.

- Possible to choose different carriers towards a destination.
- Possible to set CLI to identify CLI based hijacking.
- Possible to make a recording of the call to secure evidence.

3.5 Wangiri Monitoring

Carrier should try to limit possibility to facilitate Wangiri calls – when detected this should be reported towards the Originating and terminating carrier.

If unwanted traffic is detected the sending party should be notified and blocked if applicable.

3.6 Detected fraudulent ranges

Number ranges that are detected to be related to International Revenue Share fraud should be blocked if linked to any fraud incidents.

Carrier has no obligation to terminate any suspected fraudulent traffic towards potential Revenue Share Numbers and should prevent traffic towards such destinations.

3.7 Alert follow up activities

If an alert has been triggered the Operator should investigate the reported ranges.

Unallocated ranges should be blocked ASAP after the investigation has been completed and customer should be informed.

Ranges defined to be fraudulent of nature like special ranges or reported Revenue share number ranges should be blocked if applicable.

Due to the potential call hijacking this needs to be dealt with in a careful process - a replacement of vendor in routing should also be validated. Test calls through other interconnects should be performed to verify if the ranges are terminated by other vendors.

All traffic streams that seem to be suspect should be investigated and stopped if required.

Procedures for stopping of payments related to a fraud incident.

[I3Forum document](#) Paragraphs 2.4 and 2.5 outlines the procedures. Operators should comply with these recommendations.

In the event a fraud incident has happened and the carrier has received a request that this incident will be reported to the Local Police and/or that a request of stopping of payment has been received the following activities needs to be performed by the carrier.

Process needs to be started as early as possible to secure that the payments are stopped in the full chain of suppliers that potentially can be involved.

Carrier will inform the supplier in routing as soon as possible after the event has occurred in written. The request shall contain a description of the traffic, amount and a time period for the event at the level the terminating operator should be able to verify the incident from their end - CDRs are shared by the sending party.

A request for additional information needs to be forwarded to the sending carrier in order to secure that the documentation are at a level that will support the withholding request.

The following requirements should be shared with the originating carrier for the official documentation or Police report.

Police reports shall contain at a minimum:

- Detailed explanation of the fraud incident
- Dates of fraudulent traffic
- Destinations involved –
- Total number of minutes affected
- Total cost of the alleged fraudulent traffic
- List of ALL Calling and Called numbers of the affected calls - can be included in the police report or separate CDR file mentioned in the Police report.

Amounts related to the incident can be masked before sharing with a partner.

In addition, a translated police report in English needs to be shared.

This information should be shared with the Receiving Party.

The customer (Sending party) shall pay for amounts referring to fraudulent traffic for which a credit note cannot be obtained from the supplier (Receiving Party).

4. Reference documents

4.1 External

- [I3Forum Fraud clause Link.](#)
- I3Forum Fraud Classification
- Binding Permanent Reference Document BA.20 Roaming Fraud Prevention Procedures
- GSMA PPC.01 Mobile Spam
- GSMA FF.21 Fraud Manual

5. Definitions

CONTROL

- Means of managing risk which can be of administrative, technical, management, or legal nature, e.g. policies, procedures, guidelines, practices, organizational structures or technical implementations. Control is also used as a synonym for safeguard or countermeasure.

FRAUD EVENT

- An identified occurrence of a situation indicating possible fraudulent activities.

FRAUD INCIDENT

- A single or a series of unwanted or unexpected Fraud Events that can or will have a significant probability of financial or revenue loss or possible reputational damage.

SERVICE FRAUD

- Fraud is perpetrated where process, control, or technical weaknesses are intentionally exploited, resulting in a financial or other loss.

IRSF

- International Revenue Share Fraud. Number ranges controlled by criminals either directly or indirectly by hijacking of ranges. For more details, refer to the IRSF definition in the Fraud Classification document of the I3F.