INTERNATIONAL INTERCONNECTION FORUM FOR SERVICES OVER IP

i3 FORUM
(www.i3forum.org)

Fraud classification and recommendations on fraud dispute handling within the international wholesale telecom industry for Voice services

Release 4.0 – April 2023

FOREWORD

According to surveys of CFCA, ACFE and ETNO the potential commercial loss due to fraud in telecommunication networks represents 2.22% of the Global Telecom revenues. I3F members assume that fraud entails an average commercial business risk in the amount of 1 % of their revenue.

As fraudulent activity impacting the telecommunications industry continues to grow with no signs of slowing down, it's no surprise that fraudsters are becoming increasingly skilled in exploiting international service providers, network operators and end users by using new technologies (eg. machine learning) and expanding to new telco services (eg. SMS).

The risk to Telecom Service Providers is twofold; firstly, there is a loss of revenue when the party that is abused while using the services is not able to pay for these; secondly and potentially far more damaging, is the reputational damage related to facilitating, carrying and making profits out of fraudulent and scam traffic.

Hence, i3F members focus on fraud detection and fraud prevention to minimize commercial loss for themselves, their partners and the consumers. This document describes the main fraud types relevant for the international service providers, detection methods and possible dispute actions.

Table of Contents

I. Acronyms

A&DM	Account and Dispute Management
ACFE	Association of Certified Fraud Examiners
ACD	Average call Duration
AIT	Artificially Inflated Traffic
ASR	Answer Seizure Ratio
CDR	Call Data Record
CFCA	Communications Fraud Control Association
CLI	Calling Line Identification
ETNO	European Telecommunications Network Operators' Association
FAS	False Answer Supervision
FMS	Fraud Management System
IPRS	International Premium Rate Services
IRSF	International Revenue Share Fraud
LCR	Least Cost Routing
OBR	Origin Based Rating
OBC	Origin Based Charging
PM	Product Management
Sec	Sec(urity) department
SLA	Service Level Agreement
TM	Traffic Management
VAS	Value Added Services

II. Definitions

Carrier	Refers to the wholesale carrier
Service Receiving Party	Refers to the wholesale carrier's customer, traffic sending party
Service Providing Party	Refers to the wholesale carrier's supplier, who provides the service
End Customer	Refers to the retail customer who receives the call
Retail Access Provider	Refers to the retail network operator
Call Initiating Party	Refers to the party that makes the call, typically a retail access provider's customer
Terminating Party	Refers to the number range holder on the far end of the call flow

1 Executive Summary

1.1 Introduction and definition

The objective of this document is to facilitate the development of controls and processes that can help improve the detection and prevention of fraudulent activity as well as limit the financial and reputational exposure for the international wholesale service providers and its partners. The present document focuses on voice telecom services.

It is the intent of i3Forum to promote consistency across the telecommunications industry and specifically amidst the international wholesale carrier community by providing guidelines and best practices for the development of controls against fraudulent activity in the international telecommunications voice services.

For practical purposes, within this document, fraud may be defined as the use of deception with the intention of obtaining a profit, personal data, avoiding an obligation or causing loss or damage to another party. For “fraudulent traffic” examples, more details are provided in chapter 4.3.1, aiming at describing the characteristics of such traffic.

1.2 Scope

This document provides guidance on handling fraud issues in the international wholesale market for voice services.

The guidance recommends a fraud dispute handling process that sets the process for reporting fraud cases as well the actions for resolution.

It indicates the recommended contractual clauses to frame the processes related to fraud and fraud disputes alongside the prerequisites to allow for payment withholding.

Fraud types described are considered to have the major impact on commercial revenue loss or are brand impacting. Chapter 3 contains a description of the main Voice fraud scenarios relevant for international wholesale carriers, the approaches to detect and to counter them alongside information on the dispute handling. Chapter 3, together with Appendix 1, provide detailed workflows to detect and remediate fraudulent traffic.

1.3 Basic Recommendations

The I3F group does not accept any level of fraud and is committed to ensuring that vulnerability exploitation is minimised. The I3F group calls for zero tolerance for fraud, so that any case detected or notified should be investigated and dealt with appropriately and diligently.

It is expected that the Carriers who are signatories to the GLF Code of Conduct and / or are members of the i3Forum, will adhere to the guidelines and principles of these two Bodies and cooperate to reduce fraud.

The anti-fraud strategy, which in its application is described in this document, encourages all parties to follow 4 recommendations:

Recommendation 1: Prevention

- Encourage education and awareness across the industry on anti-fraud through various media and conferences

- Know Your Customer
- Develop and maintain effective controls to prevent fraud
- Deploy and maintain technical measures to avoid or mitigate risk per fraud type
- Avoid using Carriers with a track record of terminating fraud into destinations / regions

Recommendation 2: Detection

- Continuous training of the employees involved in the sector that have sufficient knowledge about anti-fraud
- Share information for fraudulent traffic and destinations with the relevant Carrier peers
- Technical measures to avoid or mitigate risk per fraud type

Recommendation 3: Investigation, Handling

- Ensure that, if fraud occurs, a vigorous and prompt investigation takes place.
- Take appropriate actions as per contractual obligations, the i3Forum best practices and the relevant local legislation
- Adoption of standard contractual clauses addressing fraud as per i3Forum guidelines
- Take all reasonable actions to stop payment flows as per the i3Forum guidelines
- Take all reasonable actions to prevent further exposure from all parties

Recommendation 4: Monitoring, Evaluation

- Internally report fraud cases, analysis and follow-up to establish trends, bad actor's analysis, etc. in order to take subsequent and diligent actions to prevent fraud in the future.
- Review systems and processes to improve the prevention / detection of fraud

The document incorporates the GLF Code of Conduct in its entireness.

All information / data documented herein is periodically evaluated as effort to industry and ethics improvement.

2 General Information

2.1 Recommended workflow

The workflow proposed in this section aims at improving the efficiency with regards to fraud fighting by increasing the information that is shared within the ecosystem and helping carriers take timely actions to reduce fraud on their networks.

In general, it is recommended to have a clear process to monitor and detect fraudulent traffic behaviour. The fraud specialists will analyse suspicious traffic flows and potential fraudulent destinations or originations. If necessary, counteractive measures will be initiated as well (for example, traffic blocking and disputing fraudulent traffic).
This document describes in Chapter 3. different fraud schemes and the way to detect these while analysing the traffic patterns.

Information on the suspicious traffic flow and its details should be shared with both the upstream and downstream parties involved, where permissible, subject to anti-trust legislation, contractual and regulatory obligations and commercial constraints.

Two separate communications, one to the upstream party and another one to the downstream party, may be sent that should contain at least the following details:

- Timeframe related to the allegedly fraudulent traffic
- Suspected fraud scenario
- Selling destination involved in the allegedly fraud scheme
- Volume (minutes) related to the allegedly fraudulent traffic at that time
- CDRs of the allegedly fraudulent traffic

For greatest efficiency, it is recommended that a central defined email mailbox should be made available for external parties to communicate regarding fraud related matters.

Alongside external communication, fraudulent traffic related KPIs (fraud traffic volumes, number of disputes or disputes volumes, etc) should be included within management reporting.

3 Fraud

The voice services fraud scenarios relevant for wholesale Carriers are listed below:

3.1 Voice Fraud Scenarios

3.1.1 Call Hijacking

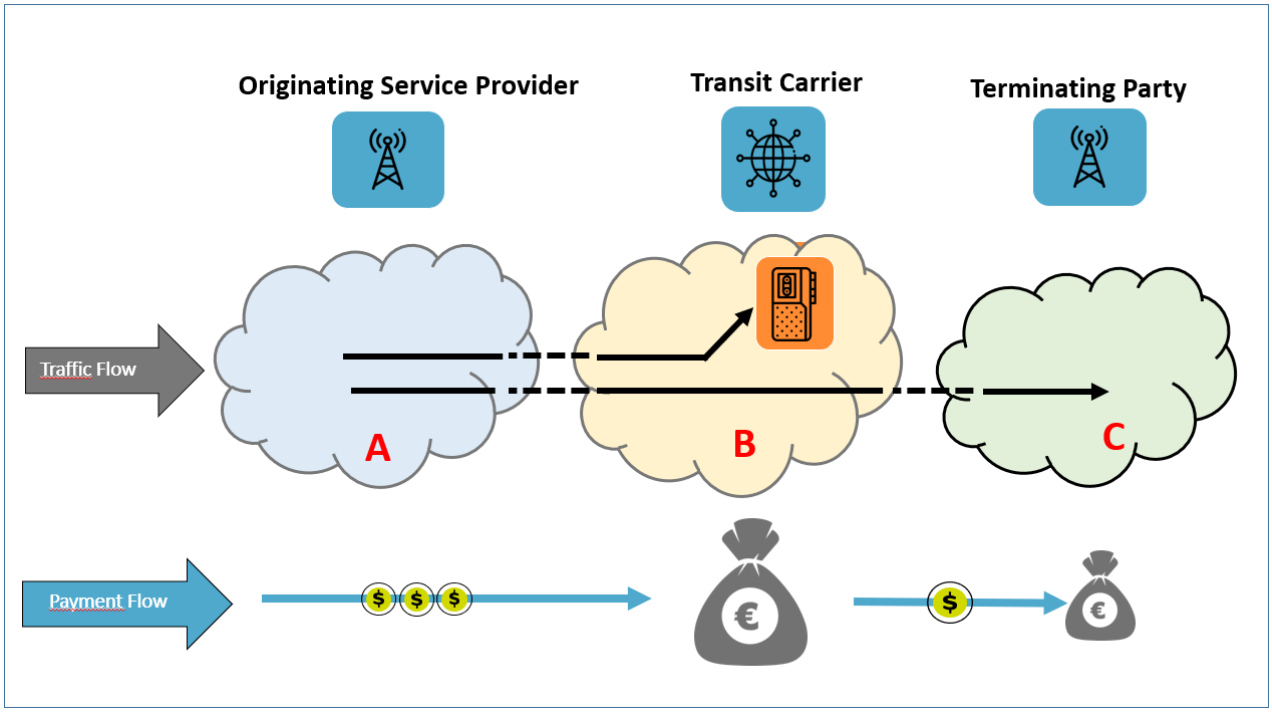


Figure 1: Call Hijacking

Description:

There are several scenarios where this technical approach is used to generate high fraudulent margins. Example one, the redirection of a percentage of normal customer traffic to a destination served by network C towards a recorded message that plays ringing tone followed by a message that aims to keep the customer online for as long as possible.
Example two, the scenario uses a similar technique, but involves the (mostly computer generated) pumping of traffic from a compromised PBX or mobile phone(s) for financial gain – that is called Artificially Inflated Traffic (AIT). The fraudster will ensure, through low pricing, that they are in route for a destination. Their partner generates high volumes of calls to these numbers which are all answered with long durations. Should this traffic be mixed in with other legitimate traffic to the destination, normal average reports of ALOC and ASR do not necessarily reflect the high answer rate. As end customers are not impacted, no customer complaints are received. The fraud generally comes to light when the high bill to the PBX owner triggers an investigation. The destination numbers used in this kind of schemes, vary from unallocated numbers, unassigned numbers, MSRNs. etc.

Issue:

The call hijacking combined with traffic pumping (AIT) results in high margins to the fraudulent Carrier coupled with a significant loss to the PBX owner or Retail Access Provider. An amount of traffic sent via this transit operator towards a terminating operator is affected in the case of call hijacking, as it is difficult to block particular numbers or number ranges, without impacting legitimate customer traffic.

- Fraudster:
  - The Carrier that hijacks the traffic gets a higher volume of chargeable calls and margin per minute.
- Intermediaries (unaware)
  - Not known in this case.
- Victim:
  - The Carrier and their wholesale partner (image, disputes, end customer complaints)
  - The originating party and its Retail Access Providers get invoiced for services they didn't use.

Approaches to detect:

- Comparing measured call duration with the expected call duration (ALOC: average length of call)
- Analysing the volume of charged calls in relation to the initiated calls (ASR: answer seizure rate) and compare it to the expected ASR.
- Detailed statistical analysis of the pattern and distribution of calls within the destination to identify the peak of activity to a relatively small and rarely dialled set of codes
- Analysing complaints of end customers
- The offered rate for termination is below the range of most other offered prices (market price)
- CLI testing tool: By using a CLI testing tool one can make calls to predetermined numbers to test numbers provided by or installed in the network of the Terminating Party (distant service provider) by the vendor solution provider. However, as the probes are not installed on unallocated numbers, this will rarely be successful in determining the fraud.
- Do test calls using the same A/B numbers via the suspicious Carrier. Benchmark same test call via the direct route.

Approaches to avoid the fraud:

- Change call routing to another Carrier instead of using a suspicious transit Carrier.

Information of dispute handling:

Given the position of a Carrier within the traffic chain, it is very difficult to identify hijacked destinations or traffic being short-stopped in real time.

Traffic patterns may also include similarities to the IRSF scenario (cf. 3.1.4.) and the details to be provided by the Service Receiving Party to support the dispute may also include End Customer complaints.

The scenario might be demonstrated or even proven by closely collaborating with the Terminating Party (destination network owner) and comparing the CDRs of the traffic issued by the Service Receiving Party and the CDRs of the Terminating Party.

3.1.2 False Answer Supervision

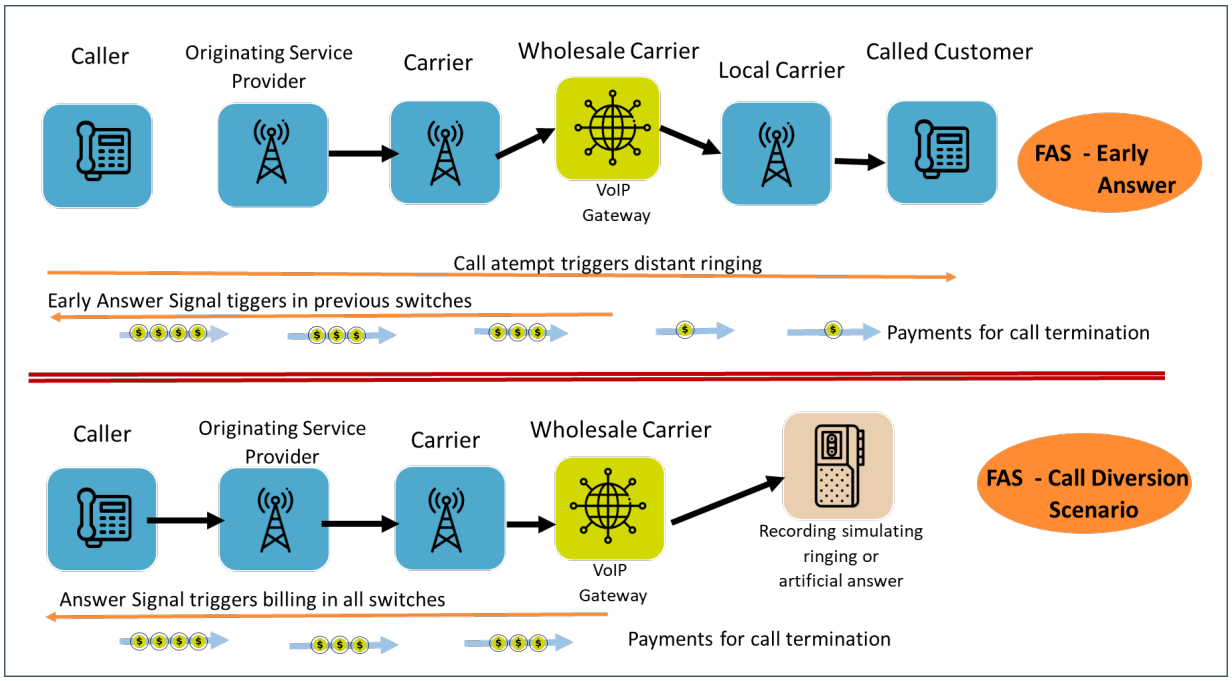


Figure 2: False Answer Supervision

Description:

There are two variants of this fraud. In both cases, a party in the traffic flow chain returns a false answer signal to the earlier Carriers in the chain, starting billing for all parties. In the early answer case shown above, the fraudulent party continues to try to establish the call, in which case, the caller pays for ringing regardless of whether the distant customer answers or not. In the second variant, call diversion, the fraudulent party routes the call to a recorded message that first plays a ringing tone, and then proceeds to a recording that mimics an answer and conversation – all with the intent of keeping the calling customer on the line and paying for the call for as long as possible.

Issue:

This is essentially a fraud against a wide range of calling customers. A call is charged before the service is actually established and conversation starts between the calling-party and the called-party, and hence the consumer pays more than contractually agreed. If the called party doesn't reply, the call is charged anyway. If the call is routed to an announcement, the consumer can pay for a significant duration, and may never be able to call the correct distant party, resulting in significant dissatisfaction. The consumer, especially if using a software client or calling card, will also notice the false charge and demand a refund from their service provider.

- Fraudster:
  - Fraudulent Carrier that starts charging for a call, although it isn't yet established. This can significantly improve their margins.
- Intermediaries (unaware)
  - Not known in this case
- Victim:
  - Service Providing Party and their wholesale partner (image, customer disputes)
  - Consumers pay for services they didn't use and may not even be able to connect to their distant number

Approaches to detect:

- Compare measured call duration via a Service Providing Party with the expected call duration
- Analyse if there are calls with short duration (5-20 sec.) which may be followed by repeat attempts between the same end customers.
- Analyse the answer delay (duration of call status “ringing”) to identify the distribution and pinpoint “machine-answered” calls
- Analyse the volume of charged calls in relation to the initiated calls (call seizure rate) and compare it to the expected distribution.
- Analyse complaints of Call Initiating Parties, especially calling card/OTT providers complaining about FAS
- Implement a probe-based FAS detection system based on sample calls to distant probes
- Implement a FAS detection system based on statistical call patterns analysis
- Once detected and confirmed, the Carrier will normally re-route the traffic to another Service Providing Party unless the current one is able to rapidly identify and resolve the issue in their own network
- False positives (ie suspecting FAS when the cause is an increase in answering machine terminations) must be rigorously identified to avoid penalizing an innocent supplier

Approaches to avoid the fraud:

- Small Service Providing Parties that are offering a wide range of destinations at a lower-than-normal price are prime suspects for this type of fraud, and so carefully checking Service Providing Parties on activation and closely monitoring their performance can help avoid the issue. This is discussed further in the i3Forum *Interconnection Form for International Voice Services*.

Information of dispute handling:

Although FAS is considered as one of the fraud scenarios, the recommended measures currently consist of informing the Service Providing Party and removing them from the route. A detailed process for detecting and removing FAS from international termination is included in Appendix 1 of this document.

Note:

The call diversion element of FAS is technically like the Call Hijacking Fraud detailed in section 3.1.1 as both involve the deliberate rerouting of a call to an announcement or recording rather than properly terminating to the called user. They are treated separately in this document because both the methods of detection and the steps taken once the fraud is identified are significantly different.

3.1.3 Call Stretching

Description:

Call Stretching is an inter-Carrier fraud type that occurs on international voice services. A fraudulent Carrier artificially inflates the duration of a call to be able to charge more money. The fraudulent Carrier illegally records the conversation during the call. As soon as the disconnect message is received from the terminating network – the fraudster plays back a fragment of the recorded conversation for the calling subscriber. People are normally unaware of this trick, so they try to interact with the voice they hear for some time before realizing that this was just a recording.

At this point, the calling party becomes really annoyed with the situation. Both the fact that the call was clearly overcharged and that a private conversation has been recorded.

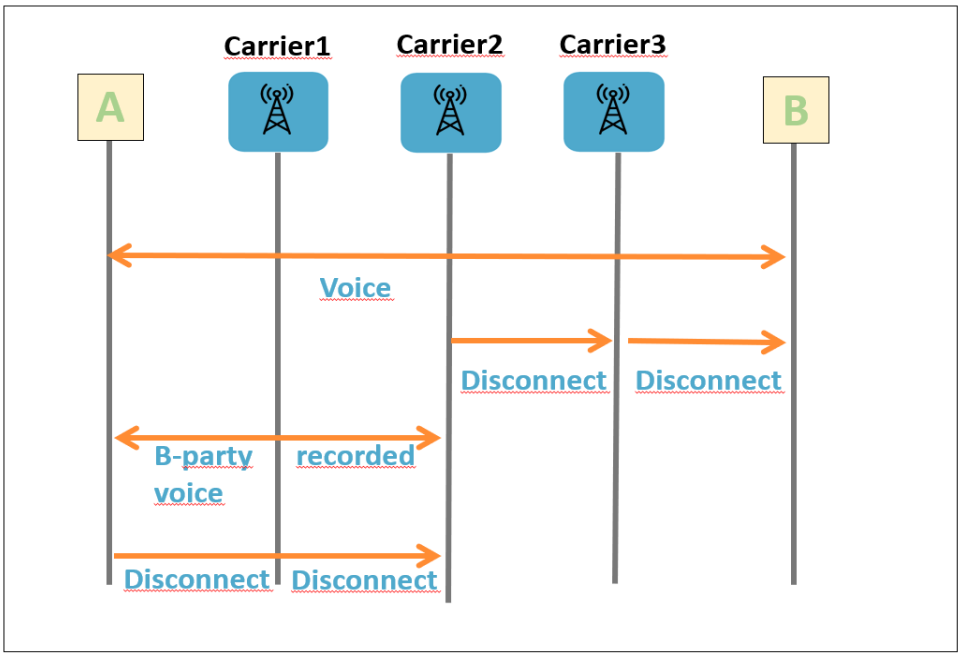


Figure 3: Call Stretching

Issue:

This is essentially a type of fraud against a wide range of calling customers. A call charging is defined once the call is disconnected. When tricking the calling party to stay in the line longer the fraudster increases the billing time and the benefit for himself.
At the same time, the fraudulent Carrier has certainly no outpayment for its Service Providing Party, as the official call was stopped as soon the called party hung up - and keep the respective proportion of the call as profit.
A customer will realize that the call was recorded which raises serious trust issues.

- Fraudster:
  - Fraudulent Carrier that prolongs the duration of the call by illegally recording and replaying part of the real conversation for the calling party. This can significantly improve their margins.

- Intermediaries (unaware)
  - Not known in this case
- Victim:
  - Service Providing Party and their wholesale partner (reputation, customer disputes, complaints).

- Call Initiating Party (retail customer) pay for services they didn't use and may even loose trust in telecommunication services.

Approaches to detect:

- So far no widely accepted methods are available for pro-active, online monitoring and effective screening of the phenomenon.
- Certain vendors claim their solution is capable to identify call stretching near real time, but it's not widely tested so far.
- Due to lack of available detection methods, typically carriers get to know about incidents by customer complaints.
- Once a Carrier got aware of an incident, it shall initiate action to improve its routing and eliminate call stretching.

Approaches to avoid the fraud:

a) Eliminate Service Providing Party from routing, who used downstream faulty Service Provider:
Carrier receives complaint → Start investigation:
   - Save the most detailed traces including signalling messages
   - Try to re-produce the event with the same conditions and record the RTP
   - Open TT with Service Providing Party and request to investigate the incident and ensure implementing safe routes
   - Remove Service Providing Party in case not satisfying feedback received

   Communication
   - Inform Service Receiving Party (customer) of the actions taken
   - Inform all parties involved internally to avoid the Service Providing Party used in the future

b) Track down the perpetrator
   - Once a case is reported, start to investigate from origin + destination ends simultaneously. This dual approach might be effective, by starting an investigation from both the sending and receiving party once a case has been revealed. So, both Carriers get routing information and may end up at a certain Carrier in the routing chain.
   - *Challenge:* confidentiality sections in the contracts might prevent carriers to reveal the identity of their wholesale partner if they don't give explicitly permission for it. That might block the process of getting to the perpetrator effectively.
   - *Solution:* might be to include law enforcement agencies (LEA) or regulators and try to get the identity information by exploiting their cross-border collaboration with fellow LEAs/regulators.

Information of dispute handling:

Although Call Stretching is considered as one of the fraud scenarios, the recommended measures currently consist of informing the Service Providing Party and removing them from the route. Due to its similarity to FAS, the detailed process for detecting and removing FAS from international termination is included in Appendix 1 of this document can be applied in this scenario as well.

3.1.4 Hacking of a customer Telephone System / Software Manipulation

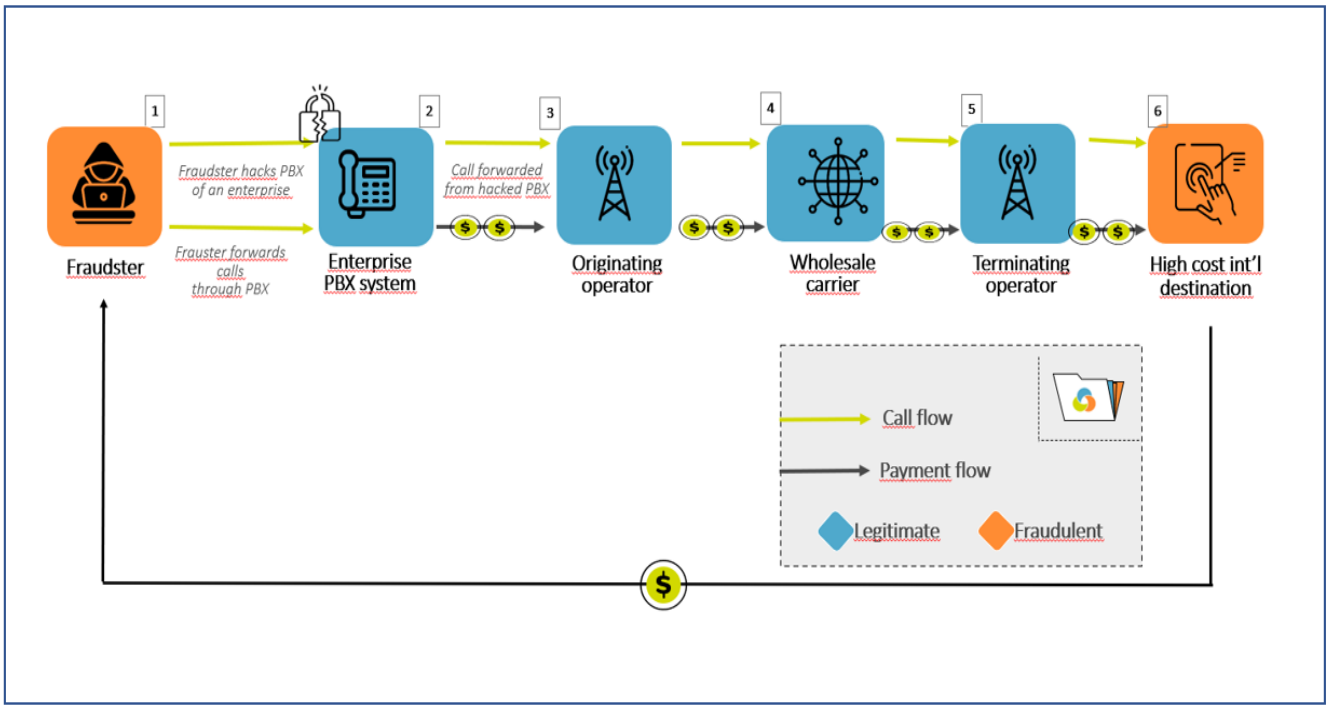


Figure 4: Hacking of Telephone System / Software Manipulation

Description:

An attacker tries different admin passwords to infiltrate a retail customer telephone system. If they get access, they establish a call-forwarding or a dial-thru to a high price destination. After that the attacker originates many calls to the infiltrated telephone system, usually from an IP based source to avoid detection, and the system forwards the calls to the expensive destination. In some other cases the attacker programs software which initiates calls automatically (AIT), avoiding the need to generate incoming calls. This has also been observed on mobile smart phone equipment infected with malicious software.

Relation to different fraud types and descriptions:

PBX hacking is considered a fraud access method and is observed in combination with different fraud types:

- AIT
- "Number plan misuse" in which national or international destination numbers could be used assigned to other providers or unassigned numbers could be used.
- "Call hijacking (or short stopping of calls)" and "international revenue share fraud (IRSF).
- Generation of calls to manipulated country-code-b-numbers

Issue:

The owner of the PBX/device normally isn't aware about the call forwarding / malicious software. This software will generate high usage that will normally result in very high amounts invoiced to the owner.

- Fraudster:
  - Attacker is able to make calls to particular destinations for free or at lower costs and he is able to offer them to others (call-through services) or profit from a revenue sharing approach with a premium rate service provider.

  - The Service Providing Party can charge the calls and increase its revenue (if actively involved in the scheme)
  - An owner of a VAS earns a fee per minute / call.
  - There is often a co-operation between the attacker and the Terminating Party / owner of the number (destination), for example, to launder money.

- Intermediaries (unaware)
  - The Terminating Party can charge the calls and increase its revenue.

- Victim:
  - The Carrier and its wholesale partners (image, disputes, use of capacity).
  - The Terminating Party/Service Providing Party who will have to devote resources to handle the fraud dispute (image, disputes, use of capacity)
  - The owner of the PBX receives an invoice for services they didn't want to use.
  - The owner of the PBX could become unreachable for their own customers and or could lose capacity due to a high load of manipulated calls (denial of service).
  - Retail Access Provider that may have to credit the stolen traffic to the PBX owner.

Approaches to detect:

- Analyse retail CDR (if high price destinations are often selected by a particular customer)
- Analyse wholesale CDR (if a particular high price destination is called unusually often). The Carrier could then inform the Service Providing Party of the potential issue.
- Analyse the duration of calls to high price destinations from a particular calling party number.
- Monitor destinations of known fraudulent traffic relative to existing and publicized number plans, traffic type, tariff models and possible extra white-and-deny-listing-functions (possibly derived from previous fraud cases).
- Retail customers monitoring their own usage actively, detect an abnormality and report then a complaint or a trouble ticket to their customer service or support point.

Approaches to avoid the fraud:

- Inform customers and the related service engineers about potential fraudulent usage of retail customer telephone system (there is a risk of the messenger getting poor feedback if the customer has already experienced misuse)
- Encourage customers, after raising awareness about the threats, to implement more stringent prevention measures such as access controls.
- Provide software updates which fix vulnerabilities within the telephone systems.
- Increase security of new telephone systems by password policies (such as password has to be changed before first usage, password has to be complex enough, etc).

Information of dispute handling:

It is reasonably assumed that, in a pure PBX hacking case where legitimate traffic is involved (eg. no AIT, IRSF or short-stopping involved), it's namely the Retail Access Provider's network and infrastructure security that should be questioned. In case of AIT, IRSF or short-stopped traffic is generated, the traffic can be subject to dispute.

3.1.5 IRSF (International Revenue Share Fraud)

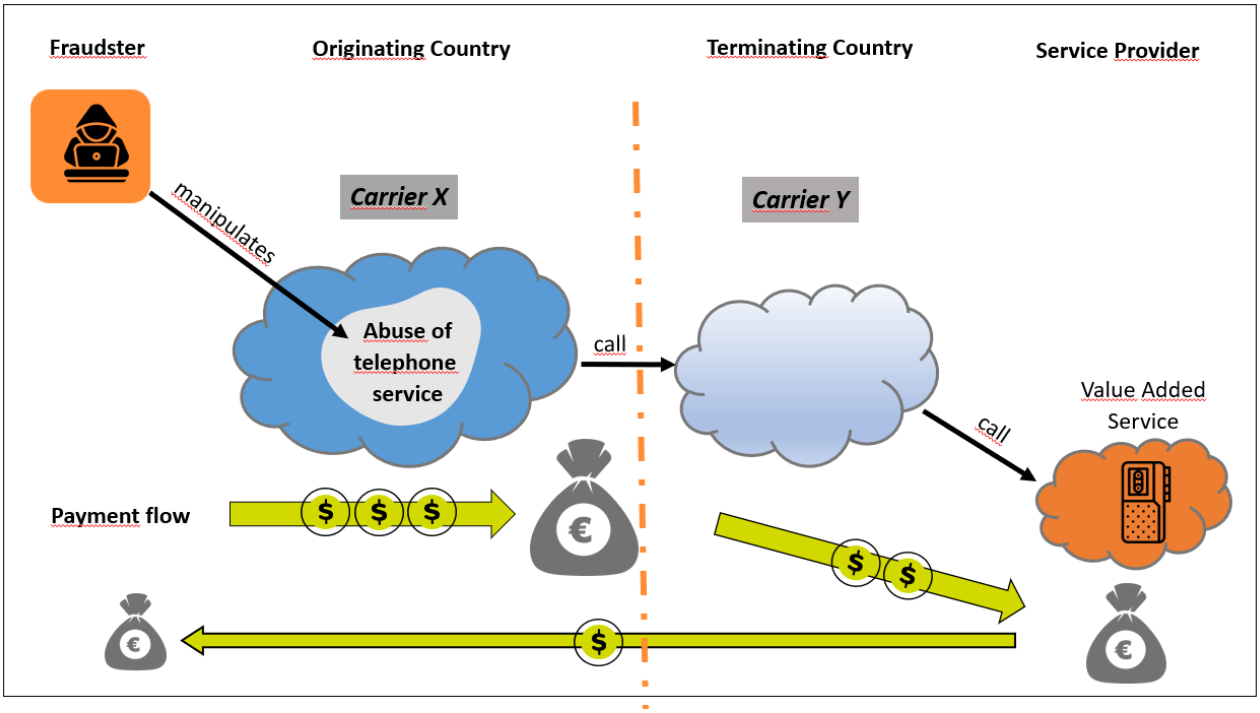


Figure 5: IRSF (International Revenue Share Fraud)

Description:

High revenue regular destinations (e. g. Cuba) and IPRS destinations remain extremely sensitive to fraud given the significant revenue that can be generated in a relatively short period of time.

Premium Rate Service is generally a service providing information, a specific service or entertainment, through calls to specific Premium Rate Service numbers that are charged at a high per minute rate. The resultant high revenue is shared by the number/network owner with the provider of the service.

Issue:

Premium Rate Services may end up being fraudulent through several mechanisms: the Service Providing Party fails to deliver the service promised or deliberately extends the length of the call via different methods or generates non-legitimate and artificially inflated traffic (AIT) using a variety of means, etc. In most cases a massive amount of traffic is generated by fraudsters in a short period of time and these same fraudsters will collect the revenue.

Fraudster:

- The party originating the calls in the originating network
- The Terminating Party (number range holder in the terminating network) can charge the calls and increase its revenue (if actively involved in the scheme)
- The content provider who operates International Premium Rate Service

Intermediaries (unaware)

- The Terminating Party and other Service Providing Parties in the chain can charge the calls and increase their revenue.

Victim:

- Retail Customer whose device (PBX, landline telephone or mobile) was compromised by hackers/criminals and used for initiating large number of calls towards typically exotic destinations or International Premium Rate ranges.
- Carrier and its wholesale partners (image, disputes, use of capacity)

- Retail Customer could become unreachable for their own customers and or could lose capacity due to a high load of manipulated calls (denial of service).
- Retail Access Provider that may have to credit the stolen traffic to the PBX owner.
- The Terminating Party (number range holder) operator who will handle the fraud dispute (image, disputes, use of capacity)

Approaches to detect:

It is difficult for a carrier to distinguish between legitimate Premium Rate Services traffic and fraudulent traffic. Indeed, a mere traffic increase does not constitute fraud itself as a push in the marketing campaign for a specific Premium Rate Service can generate visible traffic peaks.

Close traffic monitoring and abnormal traffic patterns can help identify IRSF.

Other elements that will help identify IRSF related traffic patterns:

- Sequential dialling pattern / machine generated profile:
- Example: calls occurring at same time and/or having the exact same interval between each or the calls (1 to 2 seconds interval). True Premium Services, even massive TV show traffic, does not have the same profile as machine generated /auto dialer traffic.
- Commonality of originating A-Numbers and/or Ranges
- Fake recordings
- When numbers are tested to determine if an actual service exists, in most instances you hear a fake "conferencing" recording to explain / mimic the simultaneous call traffic profile.
- ACD/ASRs that are completely disproportional /abnormal even for regular Premium Services, example 50 thousand minutes with ACD of 20 minutes, 98% ASR in a short period of time.
- Massive traffic volumes with the same A number can potentially indicate PBX hack (if the traffic was real conference calls, and/or TV oriented real Premium Services, then different A numbers would be visible).
- Any traffic origination that does not make sense given the existing options: for example, why would anyone in Canada dial an International Premium number when a domestic premium equivalent exists?

Approaches to avoid the fraud:

- Maintain a detailed and complete numbering plan with clearly identified PRS numbers/ranges.
- Close monitoring of the daily traffic and high usage reports can be the basis leading to reacting fast enough to stop significant financial impact.
- Strict company policy when opening Premium ranges in the carrier numbering plan.

Information of dispute handling:

The details as outlined in Chapter 4.2 (Fraud Dispute Principles) can be passed on by the Carrier to the next Service Providing Party down the chain to pass the dispute on; the objective is to withhold the payment (if possible, in consideration of national laws and as per i3forum guidelines) to the fraudster collecting the revenue at the end of the chain.

However, in most cases, disputing traffic and withholding payments is not enough and should be coupled with other actions taken by the telecom operator on which network the fraudulent traffic is originated. Tight SLAs with PBX customers, legal actions against local fraudsters.

3.1.6 Calls to manipulated country code B-numbers (to +CC 0 xyz)

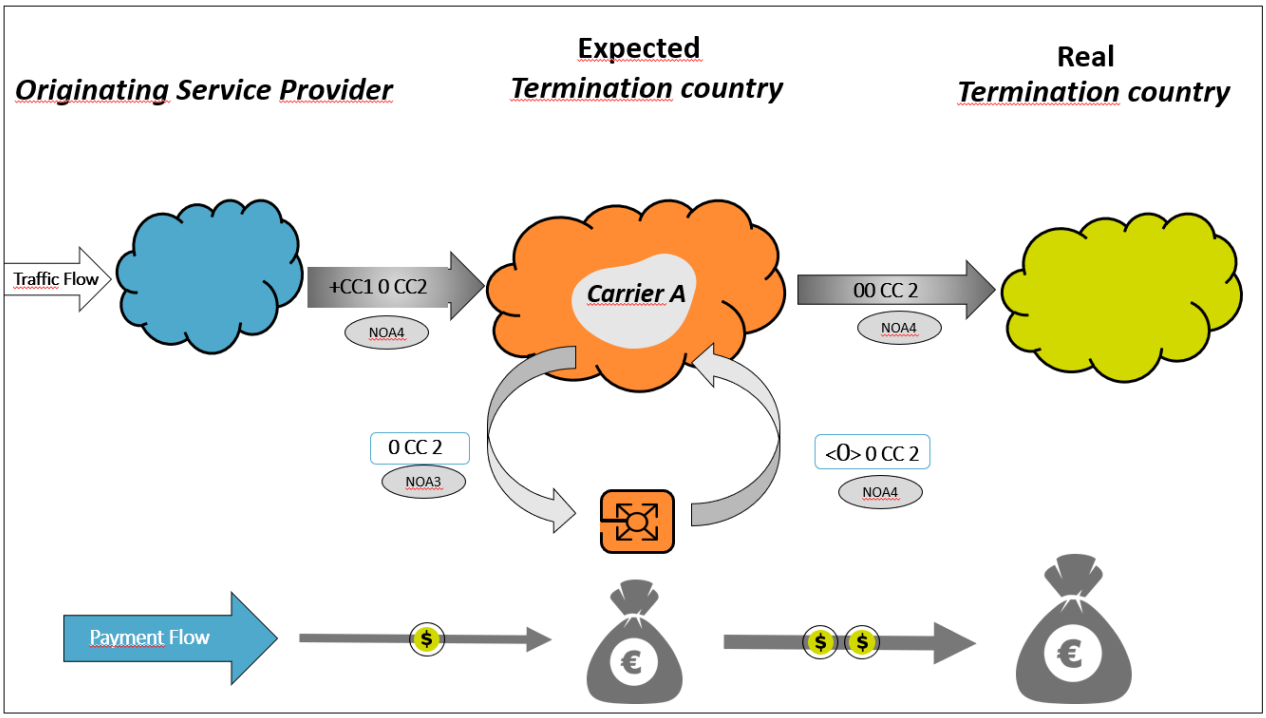


Figure 6: Calls to manipulated b-numbers (to +CC 0 xyz)

Description:

An Originating Service Provider sends a call with the prefix **+CC 0** (CC = Country Code), after that a further (additional) country code and a number. In this description, the two different country codes are marked, as follows: CC1 and CC2

+**CC1** 0 **CC2** XX YYY ZZZ

The number string starts with the country code of 'Carrier A', the call will be routed first to its international switching centre. It will handle the call as one which should be terminated within its country; therefore 'Carrier A' removes CC1 and starts to analyse further to determine where to terminate it inside the country. As the first remaining digit of the number string is '0', which normally is used to signify an international number format, the switch changes the handling of the call immediately (NOA3→ NOA4) and further determines that it is a call that should be terminated internationally to a distant 3rd country. As a result, instead of terminating in its home country, the call will be sent to a destination which is identified by the second country code (CC2) in the number string. For that reason, this type of fraud is called 'Double country code' scenario.

At most of the switch types, it is possible to program the equipment to avoid such cases, but this scenario might happen at certain types of switches due to technical restrictions or misconfiguration. It is also possible that in some countries, due to local number allocation rules - for example in Italy and in Sweden – service numbers can start with "0", so in these cases +CC 0 XXX YYY is a legitimate format.

The above scenario, where two different country codes are present in the number string is the most typical for the double country code type of fraud, and in those cases, CC2 is almost always an expensive destination. However, the fraud can also occur when the same CC is used within a number string, twice:

+CC1 0 CC1 XX YY ZZZ

In this case, operators, who are interconnected directly via bilateral interconnections, send each other traffic without indicating the others country code (Nature of Address 3 - National). In this case, a Service Receiving Party (customer) sends a Carrier a call with such format – where CC1 represents a 3rd country – the Carrier

will strip the first country code and send the call to its bilateral partner for termination. The Terminating Party will then still detect its own country code (the second CC1) and will terminate the call in-country, according to the actual number plan. In specific countries, where the mobile networks have a much higher termination rate, it is likely that the call will be terminated with a higher rate than expected, resulting in significant disputes between the partners.

Note: according to the recommendations of the i3F Technical working group, international codes should be prefixed with "+" instead of "00" or "011".

Issue:

Some Carriers deliberately manipulate the number string of the called number, by adding the home country code of 'Carrier A' (CC1) at the front of the string, to get charged a lower rate for a particular high-rate destination (CC2). The principle here - for the fraudster - is to select such countries where CC2 is significantly more expensive than CC1.

Therefore, the Originating Service Provider will receive an invoice from 'Carrier A' after a call termination in its home country, but at the same time 'Carrier A' will receive an invoice from the real termination country's operator. The difference between the two invoices causes the financial loss for Carrier A. The billing systems of 'Carrier A' record different services and prices, this probably will result in a dispute.

- Fraudster:
  - Call Initiating Party: might pay a lower rate for calls to expensive destinations
  - Retail Access Provider/Originating Operator: by committing this type of fraud:
    - it can offer to its customers low rates towards expensive destinations, therefore attract more calls
    - they don't change the retail price and leave it on a high, but realistic level, at the same time they don't have to pay the real termination fee, so they profit more as the volume increases

- Intermediaries (unaware)
  - The Terminating Party/Carriers can charge the calls and increase their revenue.

- Victim:
  - 'Carrier A': has a higher pay out for termination, than the revenue that will be received from the sending party
  - Probable consequence: a dispute will be raised because the billing system of 'Carrier A' detects different services and prices.

Approaches to detect:

- Sudden increase of traffic towards certain destination
- Switch configuration to automatically recognise such number formats /CC 0/
- Technical analysis of received call set up, call parameters and filtering out of unacceptable operational combinations, if they look doubtful. A allow-list based on the trusted and accepted own OPC (Originating Point Code) could offer such an analysis.

Approaches to avoid the fraud:

- Technical level:
  - At the international switches, put onto a deny-list all possible +CC0 country combinations - including Carrier A's home CC – as to avoid such traffic flowing unnoticed (exceptions: Italy, Sweden, Congo and Gabon)
- Commercial level: put a clause in the contracts, where it's clearly stated that:
  - It is not allowed to send traffic in such format and if carrier detects traffic at its switches with its home country code followed by a zero, then it's allowed for it to charge the customer such calls, according to the 'second country code'.
  - Modify the price/rate sheet to the carrier's customers which rates CC 0 at a very high rate (except for Italy and Sweden)

- Considerations:
    - In a normal ISUP case: if the international switching centre strips the +CC, it will assign a NOA NAT (Nature of Address: National) and it will not route the call to an international carrier, but as mentioned above, it still might happen due to technical limitations at certain switches
    - In case of SIP - if the SS7 logic of NOA is extended to the world of SIP - using the “+” sign on the SIP URI, such scenario will normally also not happen.

Information of dispute handling:

In such scenarios, the above-mentioned commercial clause forms a powerful reasoning to charge such calls according to the actual call flow and reject disputes raised respectively.

Example for commercial clause (CC means below the home country code of Carrier):

Blocking of +CC 0 in the Customers’ Network Switch

Service Receiving Party is not allowed to send calls where the called party number begins with 0 and the nature of address is 3 (National number). For the avoidance of doubt, if calls are sent to +CC 0, Service Receiving Party acknowledges that such calls might lead to routing failures or even termination of calls to other international destinations. In the latter case Carrier/Service Providing Party shall be permitted to invoice the Service Receiving Party according to actual destination and termination of the call, based on the applicable Price List of the Carrier/ Service Providing Party, if call set-ups have been made and call minutes have been recorded. Disputes will not be accepted for calls sent in this format.

3.1.7 Wangiri Fraud (Missed call campaign)

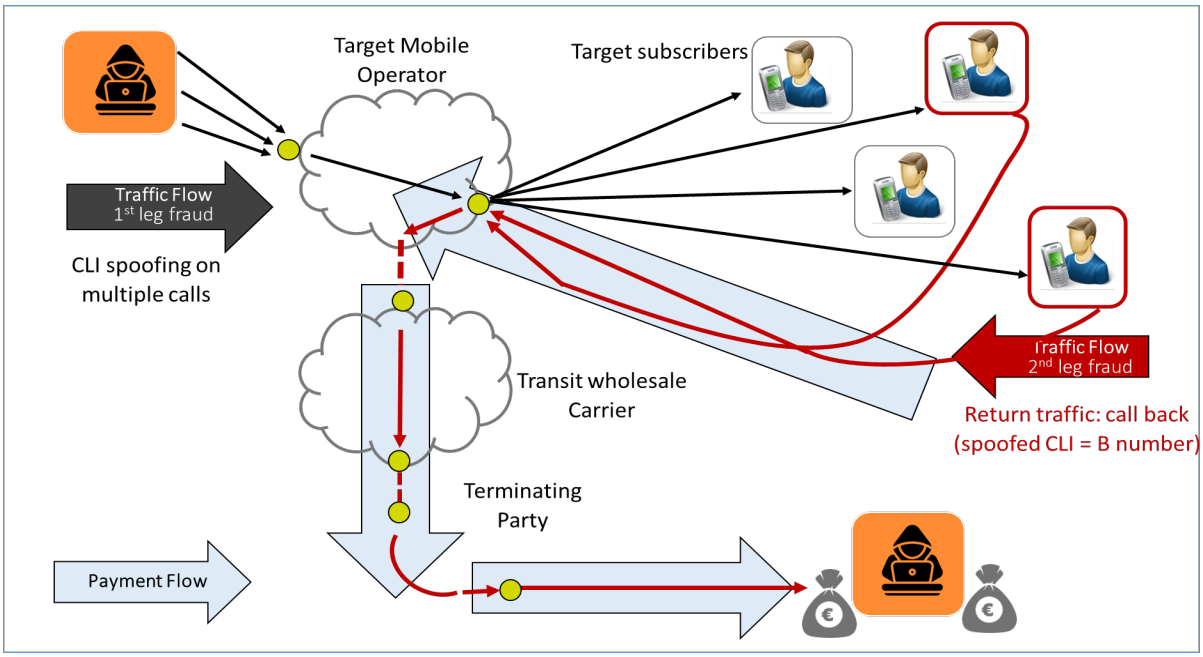


Figure 7: Wangiri Fraud

Description:

Missed call fraud campaigns and/or Wangiri fraud (Japanese term, as the fraud first occurred in Japan) is a Telecom fraud scheme based on CLI spoofing, spamming, deception and IRSF (International Revenue Share Fraud) and in most instances targets unsuspecting mobile end-users in a country and/or subscribers ('Target Subscribers') of a specific Mobile Operator ('Target Mobile Operator').

Customer Behaviour Manipulation:

The fraudulent party originates, via machine, calls to mobile customers (Target subscribers) in a specific country or operator (Target mobile operator).

Leg 1 of the Wangiri attack:
The fraudster has at its disposal the ranges of all the Target subscribers or a wide range of them. Their approach is to generate calls to thousands/millions of those customers (in some cases, it can reach 300 thousand calls per day), calling them and immediately hanging up/dropping the call after one or two rings. The fraud can also be supported by massive SMS spamming campaigns to the Target subscribers which achieves the same goal.

A manipulation is also done on the A-number field (the CLI), where the fraudster incorporates the same number for all calls, usually a hijacked number or a premium /high rated destination number on an International Premium Rate Service.

Leg 2 of the Wangiri attack:
The deception occurs as the unsuspecting Target subscriber notices the missed call or short SMS message and a proportion may decide to call back to see who had called them. When calling back, the Target subscriber will usually hear an adult oriented recording or lottery winning/gambling recording that serves as a pretext to keep the caller on the line for as long as possible.

Unknowingly, the Target subscriber is dialling an extremely expensive number for which he will be billed in his next invoice and almost certainly will dispute the invoice with the local target mobile operator.
In some cases, the Target mobile operator could be arbitraged if the international number range supporting the fraudulent activity has not been adequately rated in their customer rating systems.

Issue:

Not only leg 1 of the fraud scenario is troublesome, as it uses a large amount of capacity to destination that may not have significant available circuits, but the fraud is successful, in the eyes of the fraudsters, if only a small percentage of the Target Subscribers do call back.

The fraudster (often using VoIP) uses a variety of carriers for missed calls / SMS campaigns in leg 1 of the fraud scenario (they may send 10 thousand attempts to carrier A, 15 thousand attempts to carrier B, 5 thousand attempts to carrier C, etc.). There is minimal costs for the fraudster as the initial call is not charged (no answer) as most calls are disconnected before the target subscriber answers the call.

Even if the main wholesale carrier that transits the calls back to the fraudulent number range (leg 2 of the fraud scenario) has blocked the breakout, if the target mobile operator overflows its traffic to this destination to other wholesale carriers and if the return calls complete, they will still encounter fraud/issues. Thus, collaboration in the industry on this kind of fraud scenario is key to stop Wangiri fraud from escalating.

- Fraudster:
  - The service provider who operates (misused) International Premium Rate Services.

- Intermediaries (unaware)
  - The Terminating Party / Carriers (in the leg 2) can charge the calls and increase their revenue.

- Victim:
  - The Target customer (retail customer) who is tricked into a call back scheme

Approaches to detect:

- Monitor traffic to detect large streams from suspicious A-numbers: very low ASR or high volume of call attempts and very low ACD.
- Look for return traffic originating on the target mobile operator's network and intended to be sent to the suspicious A-numbers.

Approaches to avoid the fraud:

- Close traffic monitoring
- Timely information to the customer being potentially abused
- Barring of the fraudulent numbers in the mobile networks so that the leg 2 of the fraud scenario can never be completed and so the revenue is denied to the fraudsters.

Information on Dispute Handling:

For leg 1, there is no financial loss, so Chapter 4 (Disputes) should not apply.
For leg 2, the principles and requirements outlined in the Dispute Chapter (4.) should apply as per other fraud disputes.

3.1.8 OBC Spoofing (OBR Fraud or CLI Spoofing)

Definition

European legislation has imposed a lower termination rate for calls originated within EU. As a result, European carriers have created a paid model for fixed and mobile voice calls based on origin: the Origin Based Charging (OBC) principle or OBR (Origin Based Rating).

Issue

CLI spoofing and masking fraud has started to occur between international wholesale Carriers to benefit from lower rates. Since the price is based on origin, an increasing percentage of call networks without CLI has started to be forwarded, resulting in extra costs for the network forwarding the call without CLI. The target cost could be either very high, making the Retail Access Provider / Carrier uncompetitive, or very low, allowing fraudulent calls to take advantage of these prices (arbitrage). By identifying this trend, Terminating Parties internally began to detect and identify the various cases of NO CLI and Invalid CLI calls, as the detection of fraud for interconnection Carriers has become a necessity to avoid financial abuse.

Approaches to Detect

Similar CLI sanity check and CLI removal solutions as for Robocalls should be considered.

However, the detection of OBC spoofed calls is increasingly complicated as over the time the OBR fraud techniques have become more sophisticated whereby the inserted CLI is very difficult to detect as being a falsified CLI. And more frequently abuse is made of allocated numbers by what such fraudulent calls are not detectable by simple number validation checks, requiring more sophistic heuristics to recognize and block.

3.2 Abuse scenarios

3.2.1 Arbitrage

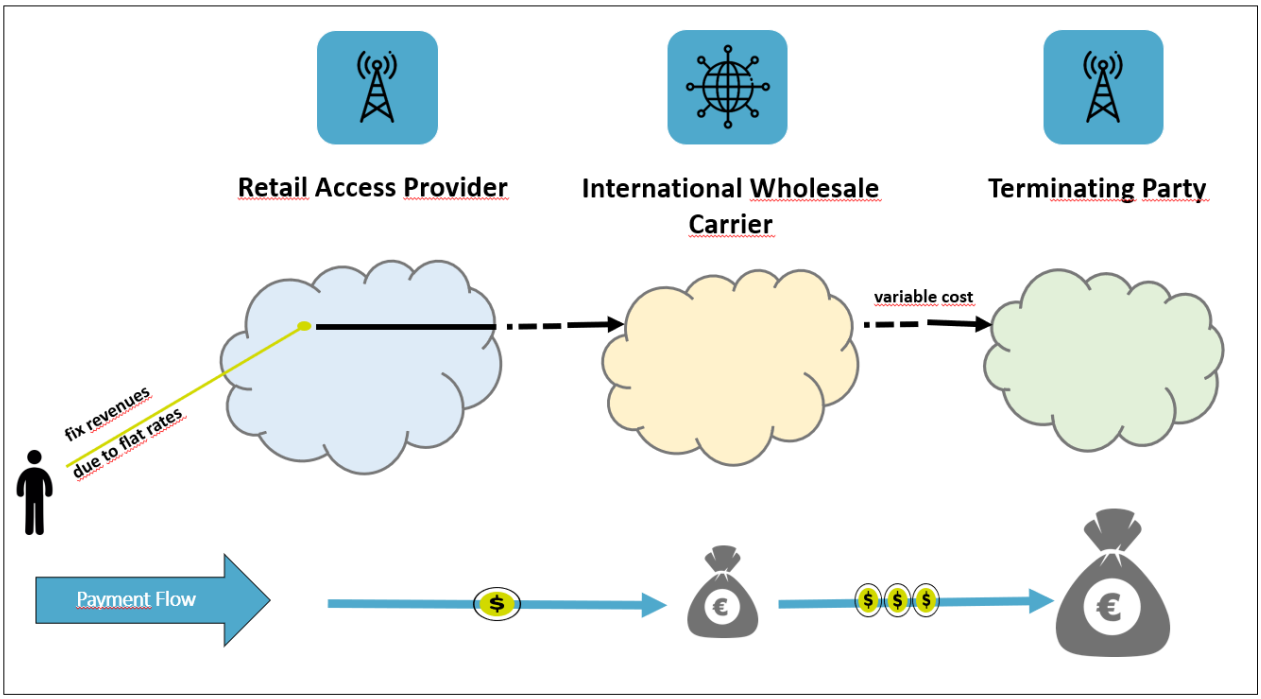


Figure 8: Arbitrage (flat rates)

Description:

An unlimited calling plan, or flat rate plan from a Retail Access Provider to a range of international destinations enables an arbitrage misuse potential, because the Retail Access Provider will have to pay the international Carrier on a per minute basis for each international call and may not be able to recoup the costs from the Call Initiating Party (retail subscriber).

In case of fraud, a lot of calls are made to generate revenue and the called party could be e.g. normal numbers in the terminating network, recorded message, an answering machine, a fictitious conference call or a chat room. Although the termination rates are quite low, a huge volume of minutes can mean a considerable commercial loss.

Fraudsters regularly scan the market seeking for loopholes in the operator's tariff plan that can be used to generate artificial inflated traffic, abusing the operator and sending massive amounts of traffic to the destination or set of destinations being sold below market value.

Issue:

A phone flat rate ensures fixed revenue for the Retail Access Provider and fixed costs for the Call Initiating Party (retail subscriber) . The price of the flat rate is calculated based on the average volume of minutes that the consumers normally make in the aggregate. If the volume of minutes is enormously high, the Retail Access Provider can't cover its costs for call termination. In case of fraud and misuse, calls are made in collusion with the Terminating Party intentionally to exceed the usage amount above the rated budget. Also, an often-temporary available new risk can exist after a change (and an increase) in a termination tariff. Similarly, a recently offered discount to retail customers can create the same situation.

- Fraudster / Winner:
  - Retail Customer: A high volume of calls and minutes to a particular destination are charged by a fixed price.
  - Carrier: High revenues depending on the high volume of incoming traffic

- Intermediaries (unaware)
  - The Terminating Party / Carriers can charge the calls and increase their revenue.

- Victim:
  - Retail Access Provider: The fixed incoming revenue will not cover the costs for call termination.

Approaches to detect:

- Analyse the CDR of all costumers with a phone flat rate to a foreign destination and check the monthly volume of minutes (heavy user analysis).
- Analyse calls with high durations to destinations covered by the flat rate and create a total view of input and output (calls, duration and costs) to detect when planned call budgets are exceeded.
- Monitor destinations of traffic relative to existing and publicized number plans, traffic type, tariff models and possible extra white- and deny-listing-functions (derived from previous fraud cases).

Approaches to avoid the fraud:

- Accurate retail pricing.
- Identification and blocking of high users.
- Introducing a volume limit for phone flat rates (e. g. 1000 minutes per month to higher rated destinations).
- Coordination between marketing and sales organizations to better assess the destinations that can be included in a flat promotional rate.
- Limit the calls to higher tariff destination numbers. It is also a good option to create a separate billing group for these calls outside the flat rate model.
- Block premium voice services technically which potentially could be covered by a fix price flat rate if the distant tariffs change.
- Start a destination number management based on existing and publicized number plans, tariff models, and possible white- and deny-listing-functions.
- Include a usage policy or usage conditions, in the offered flat fee contract to inform (end user) customers that service can be limited or that service could get cancelled in case of suspected or in case of found misuse.

Information of dispute handling:

Arbitrage abuses are the responsibility of the Retail Access Provider if the voice traffic which is sent are real (legitimate) calls.

The wholesale Carrier (Service Providing Party) routing the traffic should not accept any dispute due to retail arbitrage if the calls are legitimate. If the calls being sent are fraudulent calls under the definitions contained in this document (for example, artificially inflated or generated calls (AIT), IRSF fraud, number hijacking, etc), then the dispute should be handled under the normal fraud dispute guidelines.

3.2.2 Robocalls

Definition
A robocall can be defined as a phone call that utilizes computerization (for example, auto-dialer) to deliver a pre-recorded message(s) in high volumes, as opposed to calls placed individually by a live person. Robocalls are often associated with political and telemarking campaigns but can also be used for public service or emergency announcements. A good example of such emergency situations would be the recent COVID global pandemic.

Legality of robocalls/robocalling
The legality of a robocall will depend on the specific situation and will vary from country to country. Clearly, there are examples where robocalls can prove to be important, providing urgent or helpful information to individuals or more often, a group of people. Such examples would include medical appointment reminders, fraud alerts from banks or credit card companies, travel information etc.

An illegal robocall can be considered a call that is trying to sell something (e.g., a product or service) that has been received by a person without their consent and that has nefarious intent.

Issue - Illegality of robocalls/ robocalling
A robocall is one of many types of phone calls that are considered 'spam or scam', defined as irrelevant or inappropriate messages sent to many recipients who have not expressed any interest in receiving the message. Whilst not exclusively, robocalls differ from most spam/scam and telemarketing calls, primarily because they are 'auto-dialed' from a computer and deliver a pre-recorded message.

Lack of prior consent is what makes a robocall illegal. If the customer has not consented to receive a robocall and the robocall does not contain emergency or need-to-know information, the robocall is illegal.

Manipulating or 'spoofing' the caller ID for robocalling is also quite prevalent. This adds to the complexity of detecting 'robocalls' in practice because there are several legitimate scenarios whereby an originating number may be manipulated

However, spoofing the caller ID allows spam/scam callers to be more effective in their methods to get the customer to answer the phone. Spoofing allows spam/scam callers to place calls from phone numbers that appear to be in the same area code, to make believe they are receiving a call from their doctor's office, mechanic, or school

- Fraudster:
  - Call Initiating Party who originates the call and/or spoofs the caller ID.
- Intermediaries (may be unaware)
  - The Terminating Party / Carriers.
- Victim:
  - Target Customer (retail customer) who is tricked into accepting a call.
  - International Carriers may be compelled to break the laws in some jurisdictions to which send traffic because of the obligation to comply with the law in which the traffic originated

Approaches to Detect

For an international wholesale Carrier, it can be very difficult to distinguish between a 'legitimate robocall' passing its network, as opposed to a malicious robocall intent to cause harm or financial loss. Differing regulators have tried to mitigate fraud and robocalls by protecting customers in their own jurisdictions.

A robocall can be initiated any point of the world, even with a collaboration with a fraudulent Carrier, spoof the originating CLI and target local customers in a different country. Due to the falsified CLI, the call appears to be from a local or regional number.

The following table (status per mid 2022) demonstrates that the CLI detection solutions in different countries and regions are quite diverse and not inter-operable over the international interconnect.

The three main solution approaches in the various countries can be classified as follows:

1. CLI Validation Solutions – in these solutions the CLI is either cross-checking the CLI with the signature (STIR/SHAKEN), verifying the CLI against the number plan and number length, or by preventive removal of the CLI from the international call setup.
2. Roaming Status Checks – this solution applies to terminating calls when the CLI of a mobile user is checked against its roaming status. The status is checked either between national operators or using CAMEL to verify the status of the mobile user in the outbound visited mobile network.
3. Vetting Process – here the incoming traffic is monitored for specific call patterns that can be associated with Robocall, Wangiri, and other scams. Fines can then be imposed on carriers that carry through such unwanted traffic.

Please note that different implementation variants of the same solution approach co-exist (like how STIR/SHAKEN is implemented in the US/Canada versus France) can be complementary to each other (like a roaming status check may refine the effect of a CLI validation check.

It should be realized that sending calls over separated trunks and the use of call signing solutions such as STIR/SHAKEN do not protect against fraud within or a network prior to a sending operator's network (garbage in – garbage out). However, the identity of the sending network will be known for traceback and reconciliation actions.

Mobile status checks offer real-time and effective per call detection and blocking capabilities against spoofed Robocalling mobile CLI numbers of subscribers not roaming abroad. As these solutions do not work for fixed numbers, they should be seen as a supplement to CLI validation checks.

	1. CLI Securing Solutions		2. CLI Validating Solutions		3. Roaming Status Checks		4. Vetting Process Traffic Statistics	Call Blocking Policies
	STIR/SHAKEN	CNAP	CLI Sanity Checks	CLI Removal	National	International		
US	US/Canadian version	N.a.	N.a.	N.a.	N.a.	N.a.	N.a.	No
Canada	US/Canadian version	N.a.	N.a.	N.a.	N.a.	N.a.	N.a.	No
France	French version	N.a.	N.a.	N.a.	N.a.	N.a.	N.a.	Yes
Australia	N.a.	N.a.	Industry Code C661	N.a.	N.a.	N.a.	N.a.	Yes
Belgium	N.a.	N.a.	CLI guidelines BIPT	N.a.	N.a.	N.a.	N.a.	Yes
Latvia	N.a.	N.a.	CLI guidelines NRA	N.a.	N.a.	N.a.	N.a.	Yes
Norway	N.a.	N.a.	Regulation and Nkom	N.a.	N.a.	N.a.	N.a.	Yes
UK	N.a.	N.a.	CLI guidelines Ofcom	Under study	Under study	Under study	N.a.	Yes
Finland	N.a.	N.a.	Guidelines Traficom	If CLI not trusted	Based on API call	N.a.	N.a.	Yes
Poland	Under study	N.a.	CLI guidelines UKE	N.a.	Based on API call	CAMEL triggering	N.a.	Yes
Germany	N.a.	N.a.	For specific CLI ranges	If CLI not trusted	N.a.	CAMEL triggering	N.a.	No
Saudi Arabia	N.a.	N.a.	N.a.	N.a.	Based on SS7 ATI	N.a.	N.a.	Yes
Oman	N.a.	N.a.	N.a.	N.a.	Based on SS7 SRI-SM	N.a.	N.a.	Yes
China	N.a.	N.a.	N.a.	N.a.	N.a.	N.a.	Realtime monitoring	Yes
Ireland	Under study	N.a.	Under study	Under study	Under study	Under study	N.a.	??
India	N.a.	Under study	N.a.	N.a.	N.a.	N.a.	N.a.	No

As a result of this diversity of solutions, which is unlikely to be resolved by global standardization, trusted CLI information in one country is lost when the call terminates in the other country.

Approaches to avoid and possible counter measures for carriers

As previously referred to, the use or deployment of robocalls is not illegal and to some Operators/Carriers viewed as legitimate business. However, and clearly recognized, consumers and increasingly regulators see such traffic as unsolicited and an intrusion into personal lives. As such for Operators and Carriers who want to minimize (and even irradicate) this traffic, detecting and distinguishing 'real or genuine' calls can be complex and difficult.

The following steps can be considered in any strategy to tackle this issue:

i) Data analysis or a fraud management system (FMS) to look for triggers or indicators in traffic profiles, typically calls that are of such a frequency or ultra-short duration that they simply could not have been humanly made. Additionally, the use of AI software could help here.
ii) Consider partitioning 'known or trusted' traffic that may be 'robotic' in nature, for example contact center traffic from known retail sources.
iii) Maintain close review of known and expected robocall type traffic for any unexpected change in traffic profile.
iv) Implement the use of 'Do not originate' (DNO) and other openly available data to block traffic from previously identified 'spam sources'.
v) Consider the implementation of technical solutions as indicated above, considering any cost or regulatory implications. Note that new solutions are constantly developed
vi) Greater customer evaluation through applying "know your customer" (KYC) principles to identify "high risk" customers and Know Your Traffic (KYT) principles to identify 'high risk' traffic

Information of dispute handling:

In most cases both Carriers and Terminating Parties get know about robocalls in a re-active way, either by some post event analysis or a complaint from its end user or customer. This carrier or operator then identifies up the chain who sent this traffic and the information of suspected robocalling is passed up the chain.

In such cases, it is typically not about a traditional dispute situation (volume of financial dispute), where the disputing party is seeking a financial compensation, but rather a strong request for the identified sending party to make steps to exclude such type of behavior from its traffic (for one single robocall or several identified robocalls). That practice is in use in the US and in Canada, when robocalls are reported. International Carriers, who expressed commitment to collaborate pro-actively in identifying the source of such calls, need to work together with the above country's regulators to find the source of those calls and make sure, they will not route such traffic in the future.

3.2.3 Insolvency of a service provider and or of another operator

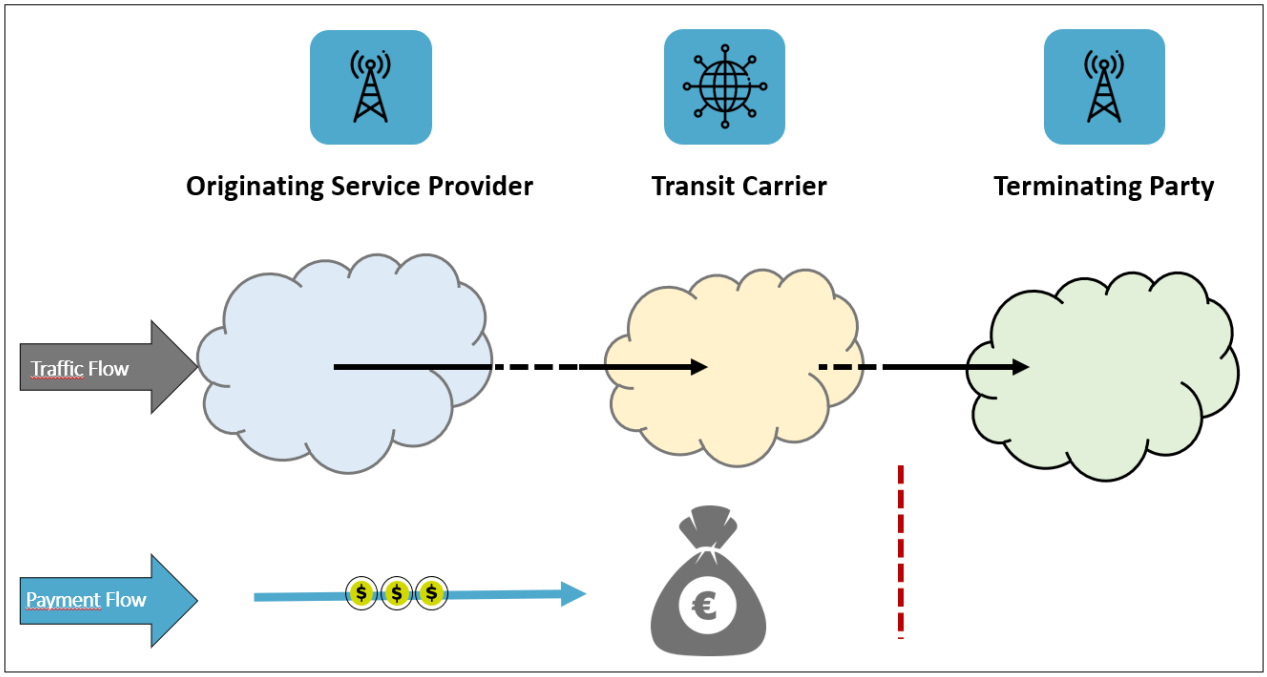


Figure 9: Insolvency

Description:

A Carrier sends a lot of traffic, although it knows that it is insolvent, and it won't be able to pay the termination fees. It offers the lowest rates for termination services in the whole market, so that it gets a lot of traffic from other Carriers and gains high revenue for a short period.

Issue:

Terminating Party gets a lot of traffic from Transit Carrier, without being paid afterwards, due to its insolvency.

- Fraudster:
  - The Carrier that becomes shortly insolvent, generates further revenue from its customers
- Intermediaries (unaware)
  - not known in this case
- Victim:
  - The Service Providing Party doesn't earn the expected revenue, because the insolvent Carrier is not able to pay the invoice, but they still must pay the downstream operators

Approaches to detect:

- Check and verify all orders and company details, preferable periodically and check of received case alerts or other warning information is found.
- Monitor changes of the regular use such as the traffic increases suddenly
- Set up an alert for news about an impending insolvency of a carrier in the current portfolio.

Approaches to avoid the fraud:

- Bank guarantee
- Payment in front (Prepayments)
- Credit check (regularly)
- Decrease the payment period / optimize the dunning process

3.2.4 Call Selling (traffic brokering)

This fraud scenario is also known as traffic brokering or SIMbox usage.

Description:

In the call selling scenario someone sells international LCR (Least Cost Routing) on the market and instead of using a legitimate Carrier / route to terminate the calls they use the Terminating Party's SIMs to create a GSM gateway (stolen, obtained via fake identity, etc.) or use a line obtained fraudulently (eg. subscription fraud, clip-on fraud) and route the calls via the Terminating Party at no or very low cost (below market rate in all cases).

Call selling operations usually serve specific communities (for example, ethnic populations through call shops).

Issue:

The Terminating Party is abused and will, in most cases, bear the costs (revenue loss) of the call selling operation. In case of clip-on fraud as the primary case, it is the subscriber that will bear the cost of the operation.

- Fraudster:
  - SIM Box operator /Call Selling broker
- Intermediaries (unaware)
  - International wholesale Carriers can charge the calls and increase their revenue.
- Victim
  - Terminating Party (number range holder) in the termination country, as they can't collect international termination fee and just receive national interconnect fee (which is significantly lower) or not even that

The Carrier in such scenario will receive and transmit abnormal traffic streams from its Service Receiving Party (customer).

Approaches to detect:

- Suddenly abnormal traffic patterns from the customer.

Approaches to avoid:

- There is not much to be done on the Carrier side except for performing close monitoring of the daily traffic.

Information of dispute handling:

If no IRSF or number hijacking are involved (and can reasonably be proven), the Carrier transiting the traffic should not be penalized for such fraud. Disputes based on this fraud scenario should not be accepted by the wholesale community.

3.2.5 Call Short-stopping

Definition:

Call short stopping can occur when a Service Providing Party/Carrier arranges with another Service Providing Party/Carrier to route calls to a geographic number in an alternative terminating country, the call does not terminate in the country owning the numbering series.

Short stopping has both legal and illegal types, depending on the legislation.

If there is no agreement from either the Call Initiating Party (subscriber) or in country Terminating Party to the traffic being terminated in the terminating destination; the traffic should be considered as illegal. This situation would result in other forms of fraud described in the document (for example call hijacking, IRSF ...).

Information of dispute handling:

Given the position of a Carrier within the traffic chain, it is very difficult to identify traffic being short-stopped in real time.

Traffic patterns may also include similarities to the IRSF scenario (3.1.5.) and the details to be provided by the Service Receiving Party to support the dispute may also include retail subscriber complaints.

These details might be sufficient to demonstrate to the Service Providing Party that there is collaboration between the originator of the traffic and the party finally hijacking the numbers. The scenario might finally be demonstrated or even proven by closely collaborating with the Terminating Party (destination network owner) and comparing the CDRs of the traffic issued by the wholesale Service Receiving Party and the CDRs of the Terminating Party (destination network owner).

A dispute under such circumstances could be justified and would follow the same scheme as for the IRSF fraud (3.1.5.).

4 Disputes

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

1. Origin of the traffic: subscription fraud, SIM theft, SIM cloning, SMS spamming, roaming fraud, PBX hacking, wangiri, etc.
2. Traffic/content: Artificial Inflation of Traffic (for example via auto-dialler equipment or by falsely answering calls), no actual content, etc.
3. Destination of the traffic: number range hijacking, traffic short-stopping, etc

Retail Access Providers can be hit by a wide variety of fraud scenarios and, given the market reality, more and more disputes get to the international wholesale Carrier community.

Despite that, in some cases there is no justification for disputing such traffic to the carrier. However, in some other cases, disputing fraudulent traffic to the carrier transiting/terminating the traffic may be justified.

4.1 Basic assumptions

Disputing and withholding payments to the carrier could in some instances be justified but should not become automatic. The final intention is to financially impact the fraudsters and not just cover for the revenue loss from compromised security and push the financial responsibility for that to the supplier.

A specific portion of traffic sent by an operator could be disputed with the carrier terminating the traffic, given that the payment to the suppliers in the chain will result in the fraudsters being paid (rewarded) for fraudulent traffic.

1. The intended outcome of i3 Forum practices is to prevent financial reward to the fraudsters.
2. Only the portion of traffic which can be shown as fraudulent should be considered disputable. Please refer to the fraud types described further in the document.
3. Suppliers should be notified that a fraud has occurred 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 payment flows corresponding to the alleged fraudulent traffic
4. The evidence/records (claim) substantiating the potentially fraudulent traffic needs to be shared within a reasonable amount of time as defined in Contract Fraud Clauses (4.3.2 – 4.3.5), and as required by the appropriate laws/regulations. Otherwise, payment should be released to avoid holding any carrier hostage.
5. 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.
6. The outcome of the investigation period may require the release of funds for payment from/to all carriers in the chain where it is not possible to permanently deny payment to the suspected fraudsters.
7. Operators are responsible for securing their networks from exposure to fraudulent traffic/use and should be prepared to fulfill their financial responsibility to downstream suppliers unless payment is denied to the fraudsters.
8. The minimum threshold (disputed value) to accept/refuse disputes due to fraud is suggested to be agreed by the parties in their contract.
9. If, for any reason, the carrier is not able to withhold the payments from the downstream players, the liability remains with the originating customer. Carriers agree to follow this process on a best effort basis.
10. In case of suspicion of fraud, the carrier always has the option of blocking fraudulent traffic independently of its customer (subject to contractual obligations).
11. If a carrier receives a credit note from their supplier, then they are required to pass it on to their customer.

4.2 Fraud Dispute Principles for International Wholesale

The customer remains liable for the traffic sent.

The prerequisite to raising disputes due to fraud is that the sending party has to provide the supplier with the details below (in English).

- CDRs

Fraud case description based on CDR analysis. Through the CDR analysis, the disputing party must explain the fraudulent nature of the traffic.

- Police or other law enforcement authority document containing:
    a. Date of fraud
    b. Name of victim (or company) that suffered the financial loss
    c. Destination
    d. Volume of minutes
    e. The English translation of this document

If the dispute opening party can prove that traffic did not reach the intended destination network (e.g.: by checking with the number range owner to verify whether they received the traffic or not), then a dispute could be raised with the supplier due to non-delivery of service. This should be proven with an official declaration from the terminating network. In this case, a police report may not be necessary.

4.3 Fraud Contract clause

i3Forum elaborated a recommendation for a contract clause (4.3.1 - 4.3.5) that focuses on fraud related disputes and their resolution. The goal of this chapter to help industry players to create a clear and straightforward environment to handle any fraud related dispute. The essence of the below wording is based on real life experience and indicate best practices for fraud dispute handling.

We encourage Carriers to amend their existing contracts with the below chapters and promote to their counterparts to act similarly, so each carrier will have the same approach for a fraud dispute process.

4.3.1 Definition

"Fraudulent traffic includes, but is not limited to, traffic that the Carrier reasonably determines as: (i) calls terminated to repeating interactive voice responses (IVRs) or recordings platforms; (ii) not routed for termination in the country of destination and/or to the owner of the number range; (iii) involving numbers that are unallocated or unassigned at time of traffic; (iv) machine generated, sequential, or simultaneous in nature."

4.3.2 Liability & Payment rules

"Each Party is responsible for and pay all expenses associated with all billing, collection, and provision of customer service activities in connection with calls originated by its customers. No payments due hereunder are contingent on payment due to either Party from its own customers. Neither Party is obliged to obtain a credit note for the supply of a Carrier Service for which the other Party could not collect the corresponding amount with its end user (e.g. in the event of insolvency or fraud).."

4.3.3 Right to suspend service

"The Service Providing Party may suspend terminating traffic to or from certain dial codes / numbers in the event that it suspects or has likely evidence of fraudulent use of such traffic."

4.3.4 If fraudulent traffic is detected

This part of the fraud clause clarifies that despite the liabilities defined in point 5.3.2, it remains possible to open fraud disputes under certain conditions.

*"If fraudulent / suspected fraudulent use of traffic occurs, the Service Receiving Party shall **notify** the Service Providing Party of such traffic before the invoice for such traffic period is received. The CDRs must be accurate and contain only the alleged fraudulent traffic and they must be provided together with the fraud traffic notification.*

*The fraud **dispute** shall be officially opened by the Service Receiving Party against the invoice received from the Service Providing Party.*

*Notwithstanding anything to the contrary in the [contract dispute resolution clauses], the following **information must be provided** by the Service Receiving Party (disputing Party) before the due date of the invoice relating to the alleged fraudulent traffic:*

i., a case description (in English) of the Fraudulent Traffic

ii. a criminal complaint or report from a public authority 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."

4.3.5 Credit note handling principles

"In case of fraudulent traffic disputes, the Service Providing Party will use commercially reasonable efforts to obtain a credit note from its suppliers regarding the fraudulent traffic. The Service Receiving Party must pay for amounts referring to fraudulent traffic for which a credit note cannot be obtained from the Service Providing Party's suppliers."

5 Call Barring Response Code

i3Forum recommends using RC 603 to identify ranges blocked due to fraud.

Based on the existing 3GPP TS 29.165 version 10.4 section 12.101.1 states that “The Response Code (DECLINE) including a Reason Header field shall be supported at the I-NNI for this purpose”. The response code 603 is mapped in the ISUP Release Cause 21.

Ref. to the i3F published White Paper “*Mapping of Signalling Protocols ISUP to/from SIP, SIP-I*”; annex B, page 16.

6 Appendix 1: FAQs

1. Is the report supporting a fraud dispute only valid if it is from a police force?

   No, the report can be from the police, or another relevant law enforcement agency.

2. Why is it necessary to submit a report from the police, or law enforcement agency, to support a fraud dispute?

   Carriers need to be sure that the originating customer is aware that a dispute was raised, and that any credits will be passed on to them if the dispute is successful. It is also important that law enforcement agencies are aware that the crime has been committed.

3. Must the law enforcement report be written in English?

   English is recommended, to reduce the chances of the report being rejected by upstream suppliers who might not have staff who are fluent in other languages.

4. If a dispute meets all the requirements recommended by the i3Forum, then is my supplier obliged to issue me with a credit for the disputed traffic?

   No, carriers can only pass on a credit to their customer if they receive a credit from their upstream supplier, or if they absorb the financial loss themselves. Members of i3Forum and GLF are committed to spreading good practice in the industry and will act in good faith to maximize the chances of passing on credits from suppliers, including favoring the selection of suppliers who comply with the i3F guidelines.

5. Is it good practice to exclude suppliers who have carried fraud traffic in the past?

   Not necessarily. Fraud has to occur before it can be detected, therefore all suppliers have some fraud traffic in their network before it can be blocked. The source of some frauds are on the originating customer network (e.g. IRSF, Wangiri). Whereas some frauds are the fault of the supplier network (e.g. call hijacking, FAS). So it is important to understand the type of fraud, to decide if the supplier was at fault. It is also important to consider how quickly a supplier detected and blocked the fraud traffic, and how co-operative they were in handling disputes.

7 Appendix 2: Process for identifying and resolving FAS issues with suppliers

Definitions:

False Answer Supervision (FAS) is a growing problem for the International Telecommunications Industry and can be found in the call routing structure to many global destinations – anything with a termination rate of more than a cent or two is potentially profitable for someone falsely answering calls. FAS manifests itself in several forms described below in greater detail but generally falls into two major groups. They are:

Call Diversion: Fraudulent call routing with answering by a recorded message and
Early Answer: Manipulation of call durations by providing an answer signal in the signaling path in advance of a true answer by the called party.

Call Diversion FAS is perceived as a major problem for all users as the call is intercepted by a downstream supplier and answered by a machine – the call is never answered by the desired called party. Instead, the caller is enticed to remain on the line and increase the cost of the call by playing a recording that can simulate ringing and then appear to be answered by the called party. Some recordings are cleverly produced, can be in the language of the called country, and can generate calls of 4-5 minute duration. Once the caller realizes that this is not going to be a successful call, their repeat attempt often encounters the same treatment, resulting in complaints to, and refunds by, the originating service provider.

Early Answer FAS also results in an extended duration of the call, and charges for unanswered calls, but the caller is generally connected to the called party if they answer. Callers are often unaware that FAS has occurred unless they are using a prepaid card or service that provides immediate feedback on the charge for each call.

Purpose of this document:

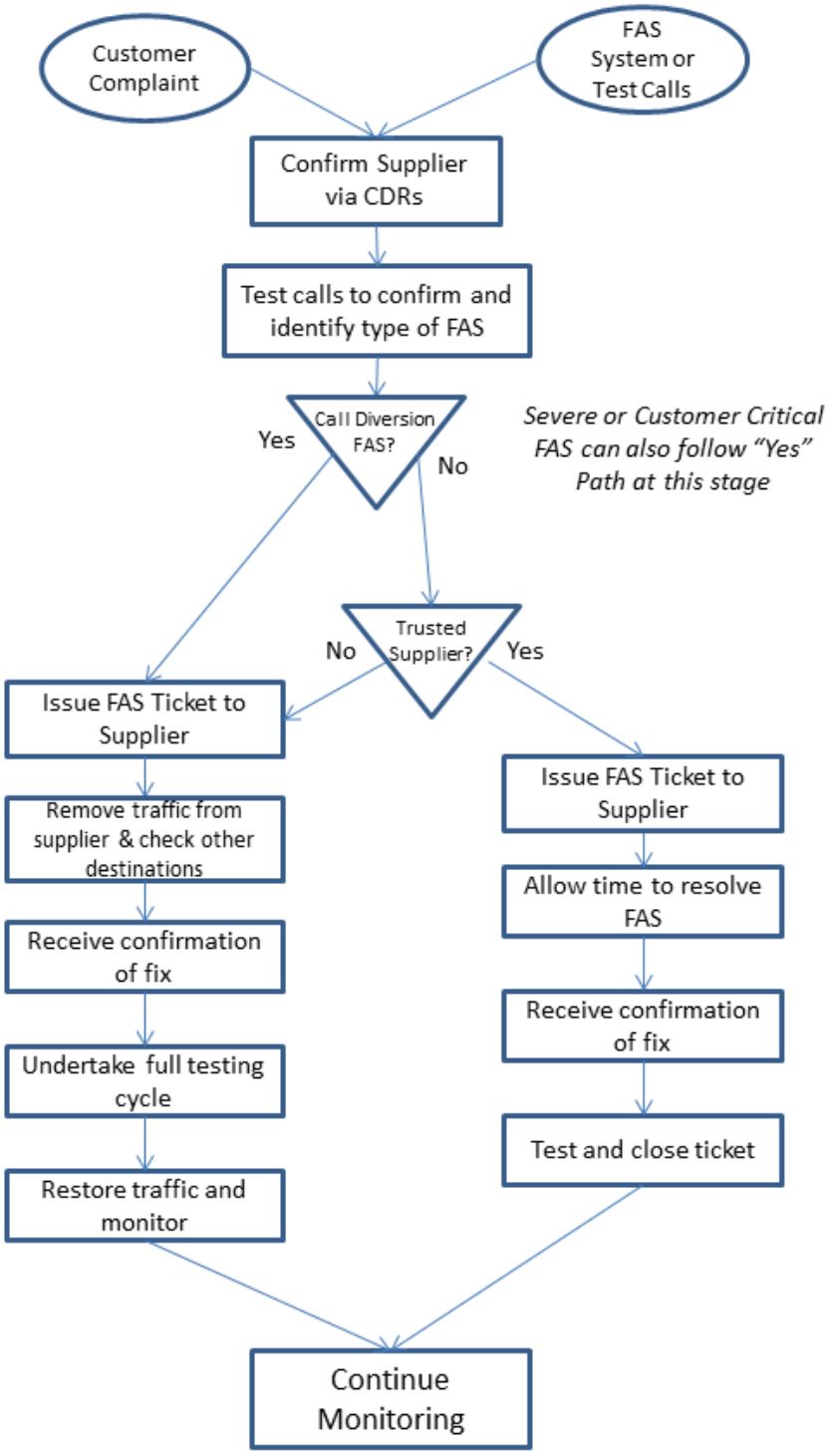
The process defined in this document is intended to enhance the ability of carriers to quickly determine the true source of the FAS problem and resolve that issue without creating quality problems for the calling customers and their service providers. Besides the obvious quality of service benefits, the capability to identify FAS problems correctly and quickly will result in fewer instances of lost traffic from customers that may otherwise shift traffic away from a problem supplier rather than troubleshoot the real cause of the issue.

In this document, the first carrier identifying the problem is referred to as the “Originating Carrier” and the carrier in the routing is referred to as the “Supplier.” The traffic is often coming from other service providers that are referred to as the “Originating Service Provider” or “Originating SP” as necessary.

For the purpose of this process, a “Trusted Supplier” is a carrier that the Originating Carrier believes is unlikely to be the source of the FAS issue directly AND has efficient and effective systems and processes in place to rapidly identify and resolve the true source of FAS following receipt of a trouble ticket.

FAS Detection and Remediation Process

The process recommended for detecting and removing FAS from the supply chain is fully described in this section. A graphical overview of the process follows below. The remainder of this section describes a step-by-step approach to resolving the issue.



Outline Process for FAS Remediation

Step 1 – Identification of problem supplier

FAS is normally detected by one (or more) of three processes:

1. An originating service provider (SP) may open a trouble ticket with the originating carrier identifying a "Quality problem" with associated call details needed to trace the call through the network.
2. Internal reports or analysis systems may highlight a problem destination/supplier.
3. Test calls being originated through various suppliers to test destination probes may find cases of

falsely answered calls.

If the problem has been reported by an originating SP, the carrier will use any provided call details with the incoming trouble tickets to trace the calls through their network to the supplier who accepted those specific calls for termination.

Internal reports are often developed to identify poor quality in the supply chain, and, more specifically, False Answer Supervision. These usually highlight lower than normal call duration, or higher than normal call connection rate for suppliers and are also used to pinpoint which supplier is likely to be providing false answers. As the providers of FAS get more skilled, such simple reports which rely on longer term averages can be fooled to such an extent that FAS that is intermittently applied or applied for a few hours and then moved to another destination will rarely be found by these internal reports.

The second option is to deploy advanced software systems to identify the suppliers that are “intelligently” applying FAS with the aim of avoiding detection. By applying detailed statistical analysis of the call records, looking for small changes in the distribution of, for example, call answering delay, a statistical system can find almost all types of FAS with a high degree of accuracy. In addition, it is often possible to identify the calls that have been falsely answered, which can help any subsequent disputes either by the customer or with the supplier.

Finally, test call sending systems can be used to identify the specific supplier that handled the test call proven to be falsely answered. These systems normally work by originating a series of preplanned test calls via each supplier to the main destination around the world. The test calls are destined for probes that have been installed in the distant networks, and, as an example, a difference in time between when the originating system sees the answer signal compared to the timestamp issued by the probe for the same call, can identify a false answer. These systems provide a positive confirmation of FAS but can only be used for networks and destinations where probes have been installed.

Having identified the supplier and destination that is believed to be causing the issue, the next step is to confirm the diagnosis. The carrier’s NOC will either initiate an automated test call pattern to that destination via that supplier, or, more likely, make several manual test calls to sample telephone numbers in that destination. Sample numbers can be found from recent calls that successfully terminated, or from an internal record of test numbers such as those assigned to hotels or fax machines. For an adequate sample, it is recommended that 10 test calls be made to the problem destination, and if three or more calls are falsely answered, the destination can be confirmed as FAS. If possible, the NOC should identify the type of FAS (Call Diversion or Early Answer) as this can help determine the severity of the problem to customer service. This can easily be achieved via manual test calls, and an automated test call that has been answered, but was never received by the distant probe, is likely to be call diversion FAS.

If the identified supplier has developed a reputation for being involved in FAS troubles or is a smaller and/or new wholesale carrier, it is often beneficial to look at other destinations currently in route to that supplier. Suppliers who are deliberately providing FAS will normally falsely answer calls on multiple other destinations as well, or switch the FAS from destination to destination in an attempt to avoid detection.

Note: *Be aware that more sophisticated FAS suppliers may be aware of the source details of test calls made by the NOC and may route those calls differently – either to a working route or to “fast busy”. If this behavior is identified, it may be necessary to originate test calls with a different CLI to avoid this false routing. In addition, such FAS suppliers may switch the FAS from destination to destination to avoid creating obvious patterns that will trigger internal alarms and be visible in reports. Test calls to those suppliers may be successful even though it was clear from the trouble tickets that they had previously been falsely answering the calls.*

Step 2: Traffic Removal

Experience shows that False Answer Supervision is rarely (if ever) introduced by an established international carrier. If FAS is detected in the routing to such a carrier, it will be because of an issue with a supplier in their routing plan. To avoid penalizing your supplier for the actions of others, it is recommended that a two-tier approach to FAS resolution is adopted, by developing a list of key Trusted Suppliers that have efficient systems and processes and therefore should be given time to find the true source of the fraud issue.

The originating NOC should follow local processes to determine the action to be taken to remediate the FAS

problem. The choice of action may be a responsibility of the NOC or may require confirmation by the commercial routing team, but the basic steps are:

1. If the supplier is a Trusted Supplier, then traffic should remain in place unless:
    a. The FAS type is determined to be Call Diversion to an announcement or;
    b. The FAS has been detected in a Premium High Quality routing plan or:
    c. The Originating Service Provider(s) and their customers are being significantly impacted by the issue
2. If the supplier is not a Trusted Supplier, then traffic should normally be removed from the routing

The “fast response Trouble Ticket process” when traffic remains on its original routing is:

1. Open a trouble ticket with the Trusted Supplier specifically identifying the problem as FAS. An example format is included in Annex A.
2. Provide the dialed digits of the test numbers that have been proven to be FAS
3. Provide the time stamps (and time zone) of the test calls to allow easy identification of the problem supplier
4. Provide the nature of the FAS problem – call diversion or early answer
5. Provide an estimate of the time available for troubleshooting before the traffic to that destination will be removed. This time period will normally be relatively short for high levels of call diversion FAS which, if uncorrected, are bound to result in the loss of that traffic from the entire carrier chain. It is recommended that low levels of Call Diversion FAS should be identified and removed by the Trusted Supplier within four (4) hours of the initial trouble ticket. Early Answer FAS should be identified and removed within eight (8) hours. These timings may also be affected by the sensitivity of the customer complaining, the destination and the percentage of false answers.

Where traffic is being removed from its routing, the process is:

1. Open a trouble ticket with the supplier specifically identifying the problem as FAS. An example format is included in Annex A.
2. Provide the dialed digits of the test numbers that have been proven to be FAS
3. Provide the time stamps (and time zone) of the test calls to allow easy identification of the problem supplier
4. Provide the nature of the FAS problem – call diversion or early answer
5. Identify that traffic has been removed until the issue has been resolved and the service retested.

Step 3: Trusted Supplier Responsibilities

On receipt of the FAS trouble ticket, the Supplier will quickly identify the wholesale carrier in their routing plan that carried the calls proven to be FAS. This is normally achieved through analysis of their own CDRs using the extra information provided by the originating carrier in terms of their specific fraudulently answered calls and timestamps.

Once the problem wholesale carrier has been identified from the CDRs, the NOC should undertake the same test call sending pattern described above to confirm the FAS. If it is not confirmed, the NOC should respond back to the originating carrier with this “Fault Not Found” result. It is possible that the FAS supplier is no longer in a distant carrier’s routing plan, or that the supplier has temporarily disabled the FAS to avoid detection. It is recommended that a watch is maintained on the supplier for that destination if a negative result is obtained.

If the test calls demonstrate FAS, it is recommended that the NOC follow local procedures to decide if to immediately remove the supplier from the routing plan or provide the information to their commercial routing team for a decision. In either event, the originating carrier should be advised of status as they may still choose to remove the traffic themselves if they believe the trouble to be severe.

Step 4: Originating Carrier Responsibilities to resolve the Fraud Issue

Up to this point in the process, a carrier will generally follow the steps above of locating and identifying the source of FAS and issuing a trouble ticket regardless of the relationship with the downstream supplier.

As described above, local processes will determine whether the traffic should remain in place until the issue is quickly resolved by a Trusted Supplier or the traffic will be rerouted (or blocked).

If the Trusted Supplier in the FAS routing responds that the problem has been identified and the suspect carrier is being removed from routing, the originating carrier can close their trouble ticket once it is confirmed that traffic is being handled properly. As traffic has continued to flow through the investigation, no further routing action is needed.

If the delay in taking action is deemed to be too long, or the problem is causing customer issues, then the originating carrier will remove the supplier from routing to that destination until advised that the problem has been permanently resolved. In this case, the supplier is advised of this as an update to the trouble ticket. Once the distant supplier responds to the ticket with advice of a resolution, the process is recommended to diverge again, depending on the nature of the supplier involved:

1. Trusted Supplier – rapidly confirm that the trouble has, in fact, been resolved and restore the traffic as quickly as possible to its original routing via that trusted supplier. This is in recognition of the acceptance that the real issue was with a downstream wholesaler, not the trusted supplier.
2. If the supplier is a not a Trusted Supplier, it is recommended that careful testing and/or discussion with the supplier be undertaken before restoring the traffic. The NOC is trying to confirm that the FAS has been fully resolved and not simply turned off for a while. Repeated trouble tickets to the same supplier are an indication that this is their response to any trouble tickets raised. At some point, internal processes may point to ceasing the relationship with this wholesaler.

Step 5: Management Reporting

It is normal for a summary of FAS trouble tickets to be created for internal management review. It would help the i3Forum Fraud Group to have a better understanding of the scale of FAS related trouble tickets. If possible, the carrier should maintain a monthly record of FAS trouble tickets opened, split between Trusted Suppliers and other carriers. It is not necessary to identify the specific carriers involved, by name, as this information is normally commercially confidential. The purpose of sharing this information with the i3Forum Fraud Group is for statistical purposes rather than to assess the involvement of any individual carriers.

Annex A

Trouble Ticket Format/Required Information

Although each carrier has their own system for issuing a trouble ticket to other carriers to raise issues, certain data elements must be present to support the full implementation of this process. An example ticket is outlined below:

Issuing Carrier Name: Carrier A
Ticket issued to: Trusted Supplier B
Ticket ID Number: aaacccnnn
Ticket Time Stamp: 08:32 UTC 1 October 2012

Subject: False Answer Supervision FAS on Country: Region Destination

Details: We have identified that calls are being falsely answered using an early answer methodology on traffic you are terminating to the above destination. Example CDRs and time stamps are included below. In accordance with our agreement, we may need to remove traffic from this destination with effect from 12:32 UTC on 1 October 2012 unless we hear from you that the issue has been resolved.

Please respond with updates to allow us to take appropriate action.

Example CDRs proved to have been falsely answered:

93 79123456 – 07:31 UTC 1 October 2012
93 79157456 – 07:34 UTC 1 October 2012
93 79184456 – 07:35 UTC 1 October 2012
93 79192456 – 07:38 UTC 1 October 2012
93 79184456 – 07:42 UTC 1 October 2012

Trunk Group/Service: Supplier B Premium
VoIP Prefix: 94627#

Please respond with updates, referencing Ticket ID aaacccnnn to:

John Smith
+1 703 555 1212
NetworkOperations@CarrierA.com