**INTERNATIONAL INTERCONNECTION FORUM FOR SERVICES OVER IP**

**i3 FORUM**
(www.i3forum.org)

# Fraud classification and recommendations on dispute handling within the wholesale telecom industry

# Release 3.0 - May 2014

## FOREWORD

According to surveys of CFCA, ACFE and ETNO the potential commercial loss due to fraud in telecommunication networks represents 0.5% to 5% of operator's revenue. I3F operators assume that fraud provides a commercial business risk in the amount of 1 % of their revenue.

Hence, i3F operators focus on fraud detection and fraud prevention to minimize commercial loss for itself, its partners and the consumer. The specific focus of I3F in the context of fraud prevention is the impact of the move of the industry to IP interconnections. This document describes the main fraud types, detection methodology and possible dispute actions.

# Table of Contents


**I. ACRONYMS ..... 4**

**1 MANAGEMENT SUMMARY ..... 5**

**2 GENERAL INFORMATION ..... 6**

**2.1 Recommended workflow ..... 6**

**3 DISPUTES ..... 7**

**3.1 Basic assumptions ..... 7**

**3.2 Fraud Dispute Principles for International Wholesale ..... 8**

**4 FRAUD ..... 9**

**4.1 Fraud Scenarios ..... 9**
4.1.1 Call Hijacking ..... 9
4.1.2 False Answer Supervision ..... 11
4.1.3 Hacking of a customer Telephone System / Software Manipulation ..... 13
4.1.4 IRSF (International Revenue Share Fraud) ..... 15
4.1.5 Calls to manipulated b-numbers (to +CC 0 xyz) ..... 17
4.1.6 Wangiri Fraud (Missed call campaign) ..... 20

**4.2 Fraud-like Scenarios: Abuse scenarios ..... 22**
4.2.1 Arbitrage (retail flat rates) ..... 22
4.2.2 Insolvency of a service provider and or of another operator ..... 24
4.2.3 Call Selling (traffic brokering) ..... 25
4.2.4 Call Short-stopping ..... 26

**5 CALL BARRING RESPONSE CODE ..... 27**

**6 APPENDIX 1: PROCESS FOR IDENTIFYING AND RESOLVING FAS ISSUES WITH SUPPLIERS ..... 28**

# I. Acronyms

| | |
|---|---|
| A&DM | Account and Dispute Management |
| ACFE | Association of Certified Fraud Examiners |
| ACD | Average call Duration |
| ASR | Answer Seizure Ratio |
| CDR | Call Data Record |
| SLA | Service Level Agreement |
| CFCA | Communications Fraud Control Association |
| CLI | Calling Line Identification |
| CARRIER | Wholesale carrier |
| ETNO | European Telecommunications Network Operators' Association |
| FAS | False Answer Supervision |
| IPRS | International PREMIUM Rate Services |
| IRSF | International Revenue Share Fraud |
| PM | Product Management |
| Sec | Sec(urity) department |
| TM | Traffic Management |
| VAS | Value Added Services |

# 1 Management Summary

The following documentation provides guidance on handling fraud issues in the international wholesale market for voice services.

It should be the basis for contractual clauses with suppliers referring to defined fraud types and prerequisites with the target of blocking payment flows which enrich the fraudulent party.

Generic fraud scenarios have been described and they are responsible for a considerable commercial loss. Chapter 4 contains a description of the main fraud scenarios, approaches to detect and to avoid a particular fraud scenario and information on the dispute handling. Chapter 4, together with Appendix 1 provides detailed workflows to detect and remediate fraudulent traffic.

Within a carrier, different departments take the responsibility to analyse traffic flows regarding fraud destinations and to initiate counteractive measures if necessary (e.g. blocking of a fraudulent destination).

# 2 General Information

## 2.1 Recommended workflow

Fraud specialists will analyse traffic flows and potential fraudulent destinations or originations. If necessary, counteractive measures will be initiated by the other teams as well (i.e. traffic blocking and dispute fraudulent traffic).
Information should be sent to both the upstream and downstream parties involved about the suspicious traffic flow. For greatest efficiency, it is recommended that a central defined email mailbox should be made available to other carriers. Two separate communications should be sent that could contain at least the following details:

- Timeframe
- Selling destination
- Volume (minutes) at that time

. In addition, a key element to any dispute due to fraud is respecting the deadlines and timeframes set by the carrier's procedures to avoid adding complexity to the case by breaching the commercial terms of the agreements in place.

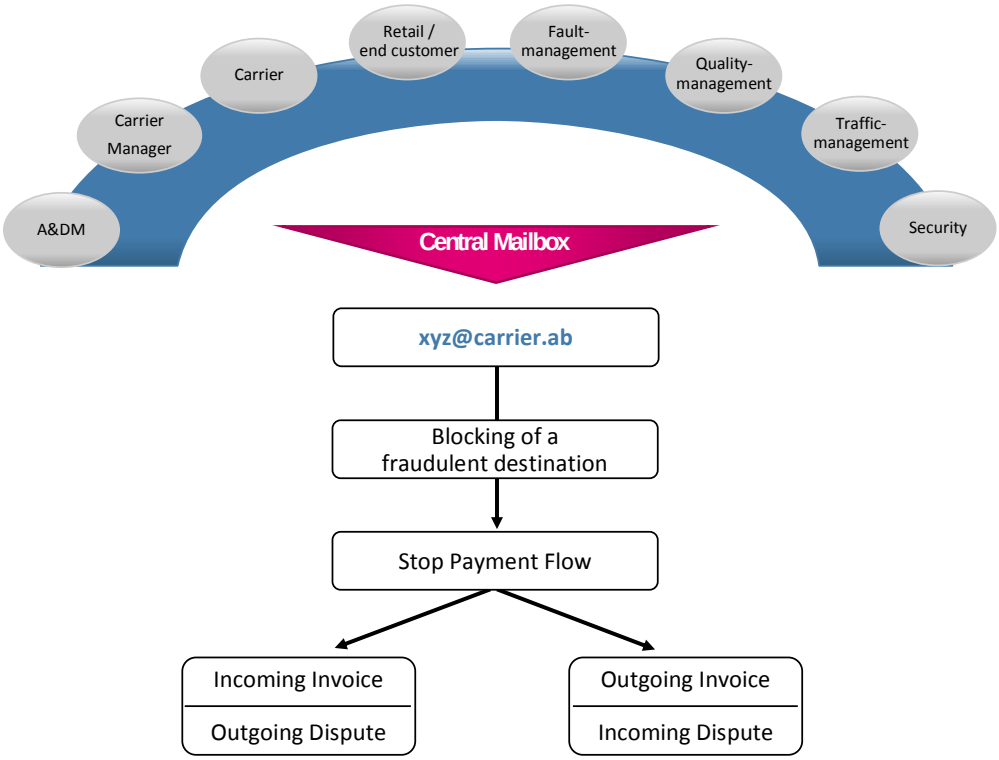



*Figure 1: What to do in case of fraud*

# 3 Disputes

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

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

The operators can be hit by a wide variety of fraud scenarios and, given the market reality; more and more disputes get to the 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.

The top 5 fraud loss categories reported by operators to CFCA in 2011 were:

- $4.96 Billion (USD) – Compromised PBX/Voicemail Systems
- $4.32 Billion (USD) – Subscription/Identity Theft
- $3.84 Billion (USD) – International Revenue Share Fraud
- $2.88 Billion (USD) – By-Pass Fraud
- $2.40 Billion (USD) – Credit Card Fraud

Amongst these, the top growing fraud schemes affecting telecom operators are PBX hacking and IRSF (IRSF will indeed typically be a secondary fraud originated eg. by a subscription fraud).

## 3.1 Basic assumptions

Disputing and withholding payments to the carrier could in some instances be justified, but should not become a reflex, if 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 carrier.

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 for fraudulent traffic.

- The intended outcome of i3 Forum practices is to financially impact the fraudsters. Taking the carrier hostage by denying or withholding payment indefinitely is not recommended.
- Only the portion of traffic which can be shown as fraudulent should be considered disputable, should the payment be denied. Please refer to the fraud types described further in the document.
- The evidence/records (claim) substantiating the potentially fraudulent traffic need to be shared within a reasonable amount of time (e.g., 30 days) and as required by the appropriate laws/regulations, otherwise payment should be released to avoid holding any carrier hostage.
- Legal/regulatory requirements as well as private commercial agreements 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.
- The outcome of the investigation period (e.g., six months) 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.
- Operators are responsible for securing their networks from exposure to fraudulent traffic/use and should be prepared to fulfil their financial responsibility to downstream suppliers unless payment is denied to the fraudsters.
- The threshold (disputed value) to accept/refuse disputes due to fraud is suggested to be the threshold indicated in the general financial terms in the interconnect contracts (i.e. 1% or 2%).
- If, for any reason, the carrier is not able to withhold the payments from the downstream players, the liability remains with the retail operator. Carriers agree to follow this process on a best effort basis.

- In case of suspicion of fraud the carrier always has the option of taking action independently of its customer.

## 3.2 Fraud Dispute Principles for International Wholesale

The customer remains liable for the traffic sent.

The sending Party may suspend sending traffic to certain dialling codes / numbers and may not pay the incurred charges for traffic that has already been sent to such dialling codes / numbers, if such traffic involves fraudulent behaviour or action of the terminating Party or terminating Party's service providers/end user or other carrier(s) interconnected to the terminating Party and if the prerequisites are met as described in chapter 4 “Fraud”. Without limiting the generality of the foregoing, the foregoing right applies especially to fraudulent use of dialler devices or manipulation of telecom equipment (such as unauthorized implementation of call forwarding) causing the sending Party, service providers, other interconnected carriers(s) or any of such parties' end customers to send traffic and thus using the Services without their consent.

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

- CDR analysis
- Fraud description based on CDR analysis
- Official fraud letter from the operator
- Official document, issued in the name of the customer company by one of the customer Chief Officers, stating that the operator has not been paid or has had a loss (quantified) for the specific portion of traffic that is disputed
- Police or other law enforcement authority report

# 4 Fraud

Fraud scenarios which account for a considerable commercial loss are listed below. Besides the information about the particular fraud scenario, approaches to detect and avoid them are stated as well. Especially in case of arbitrage issues the borders between regular wholesale business and fraud are vague. There are manifold hybrid forms of several fraud scenarios as well, but this chapter contains only generic fraud scenarios.

## 4.1 Fraud Scenarios

### 4.1.1 Call Hijacking

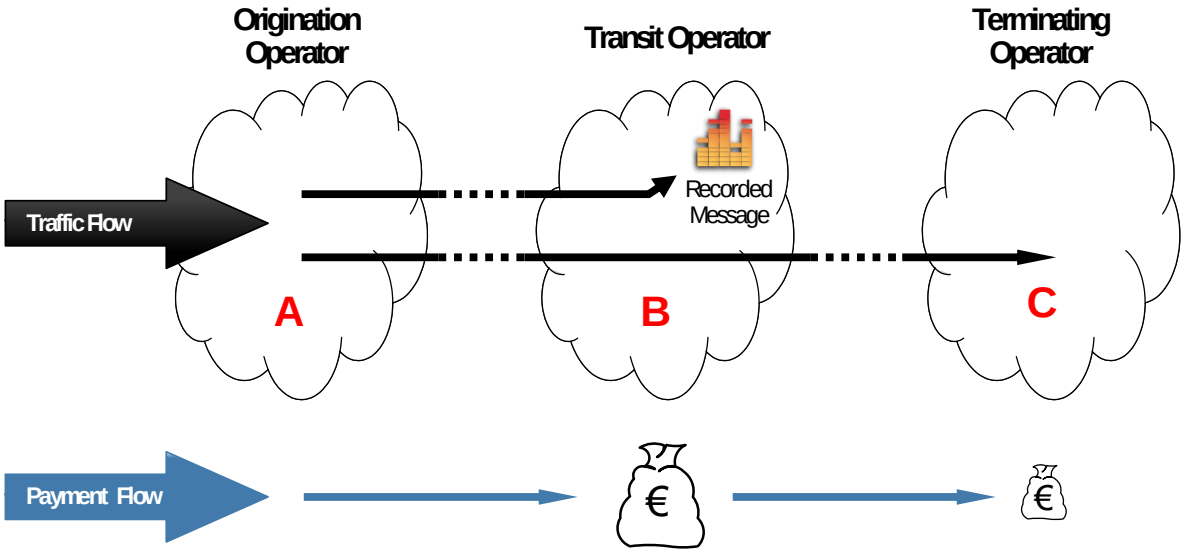



*Figure 2: Call Hijacking*

**This fraud scenario is also called, number plan misuse, non-legitimate destinations.**

**Description:**

There are two main scenarios where this technical approach is used to generate high fraudulent margins. The first involves 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. This scenario of fraud against the end user is more fully defined in section 4.1.2 – False Answer Supervision.

The second scenario uses a similar technique but involves the pumping of traffic from a compromised PBX or mobile phone(s). The fraudster will ensure, through low pricing, that they are in route for a destination, and will choose some unallocated numbers in the destination network. Their partner generates high volumes of calls to these unallocated numbers which are all answered with long durations. Other carriers who happen to get these calls will either fail them as “number unallocated” or return a route advance signal which simply causes the traffic to go to the fraudulent supplier. 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.

Relation to other fraud types and descriptions:

- This fraud scenario is sometimes also called "number plan misuse" in which national or international destination numbers are assigned to other (incorrect) provider or are unassigned numbers and used for fraudulent purposes.
- Call hijacking or call short stopping is also observed in combination with fraud scenarios such as “Misuse of (retail) customer systems” (pbx or ip-pbx) and or “misuse of (retail) customer equipment” (mobile smart phone or mobile USB stick with rogue dialler software), possibly followed by call forwarding misuse or roaming misuse.

**Issue:**

The FAS scenario is discussed in section 4.1.2. The call hijacking combined with traffic pumping results in high margins to the fraudulent carrier coupled with a significant loss to the PBX owner or retail/mobile service 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 customer traffic.

- Winner:
  - Operator that hijacks the traffic gets a higher volume of chargeable calls and margin per minute.
- Loser:
  - Carrier and their wholesale partner (image, disputes, end customer complaints)
  - End Customers and retail service 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 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.

**Approaches to avoid the fraud:**

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

**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.

Traffic patterns would be similar to the IRSF scenario (cf. 4.1.4.) and the details to be provided by the operator to support the dispute would also include end customer complaints.

These details might be sufficient to demonstrate to the carrier 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 destination network owner and comparing the CDRs of the traffic issued by the wholesale customer and the CDRs of the destination network owner.

A dispute under such circumstances could be justified and would follow the same scheme as for the IRSF fraud (cf. 4.1.4.).

### 4.1.2 False Answer Supervision

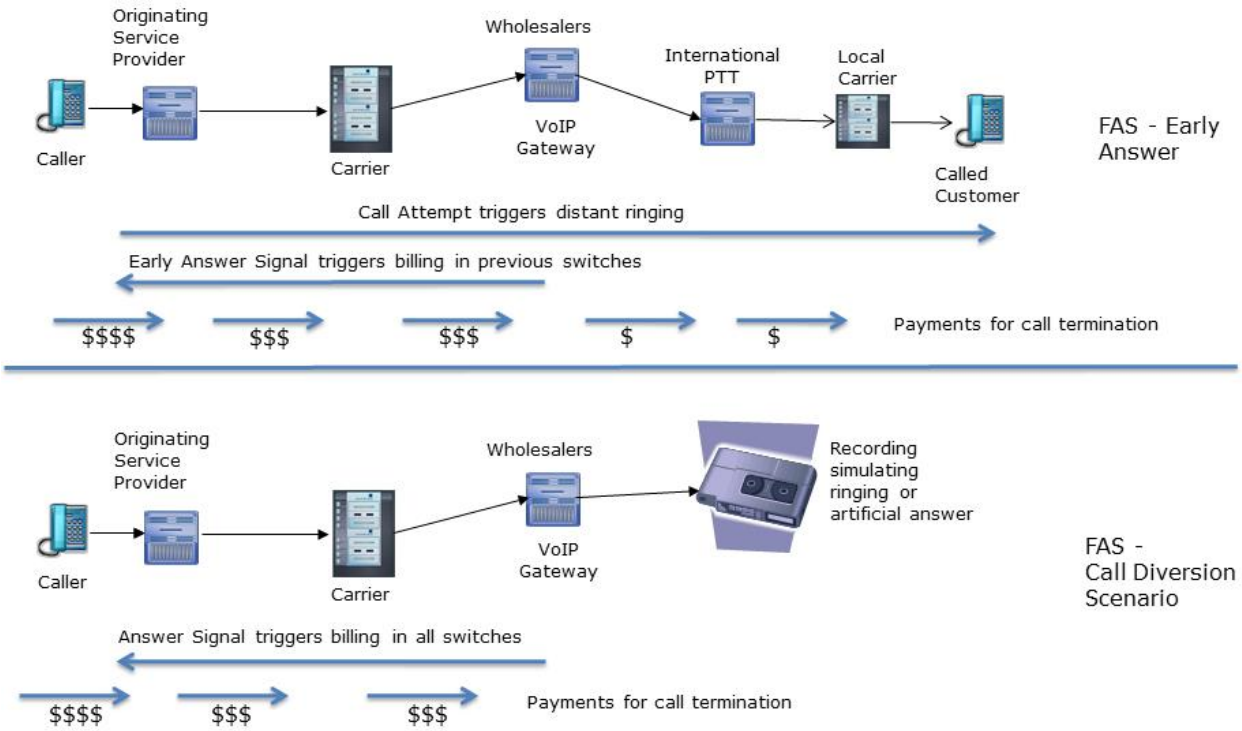



*Figure 3: False Answer Supervision*

**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.

- Winner:
  - Fraudulent carrier that starts charging for a call, although it isn't yet established. This can significantly improve their margins.
- Loser:
  - Service Provider 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 supplier 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 end customers, 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 supplier unless the current supplier 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 suppliers 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 suppliers 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 supplier and removing the supplier 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 similar to a the Call Hijacking Fraud detailed in section 4.1.1 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.

### 4.1.3 Hacking of a customer Telephone System / Software Manipulation

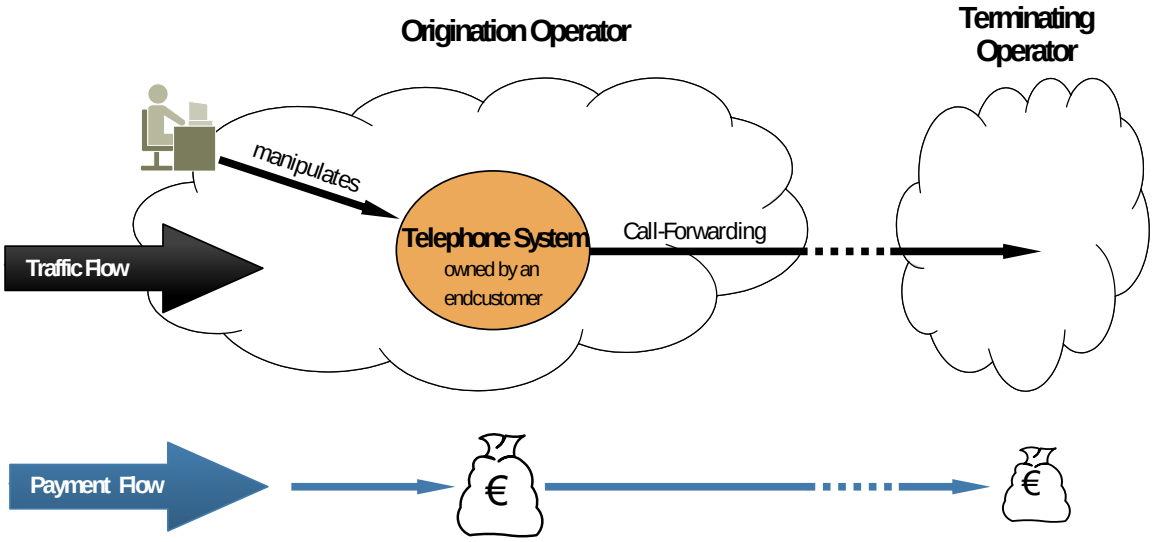



*Figure 4: Hacking of Telephone System / Software Manipulation*

**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, avoiding the need to generate incoming calls. This has also been observed on mobile smart phone equipment infected with malicious software.

**Relation to other fraud types and descriptions**:

- This fraud scenario is observed in combination with:
  - "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).

**Issue:**

The end customer 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 end user.

- Winner:
  - 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 terminating operator can charge the calls and increase its revenue.
  - An owner of a VAS possibly earns a fee per minute / call.
  - There is often a co-operation between the attacker and the termination operator / owner of the number (destination), for example, to launder money.
- Loser:
  - Carrier and its wholesale partners (image, disputes, use of capacity)
  - End Customer gets an invoice for services they didn't want to use.
  - End 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 Service Provider that may have to credit the stolen traffic to the PBX owner.

**Approaches to detect:**

- Analyse retail CDR (if high price destination 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 Provider 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-blacklisting-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.

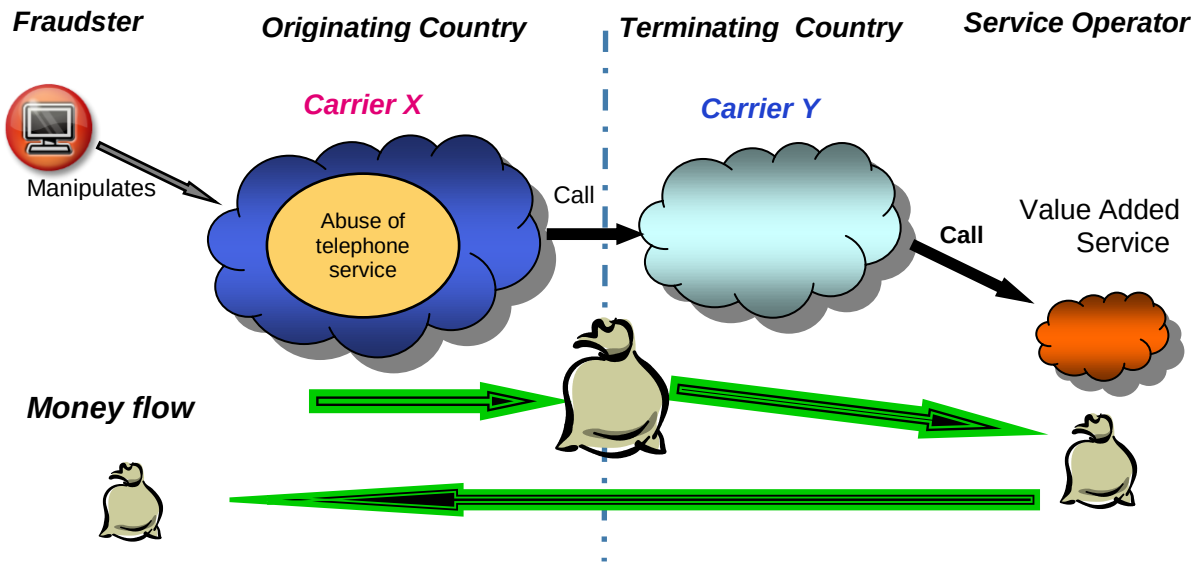
**Approaches to avoid the fraud:**

- 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 (e.g. no IRSF involved), it's namely the operator's network and infrastructure security that should be questioned. As such, the supplier terminating the traffic should not accept any dispute due to PBX hacking.

### 4.1.4 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 provider fails to deliver the service promised; the service provider deliberately extends the length of the call via different methods or; the service provider generates non-legitimate and artificially-inflated traffic 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.

**Approaches to detect:**

Generally speaking, 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 dialing pattern / machine generated profile :
  Example: calls occurring at same time and/or having the exact same interval between each or the calls (i.e. 1, 2 sec 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 actually tested to determine if an actual service exists, in the vast majority of instances you hear a fake "conferencing" recording in order to explain / mimic the simultaneous call traffic profile.

- ACD/ASRs that are completely disproportional /abnormal even for regular Premium Services, example 50k 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 actually 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, i.e. why would someone in Canada dial an International Premium number when a domestic premium option/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:**

In this scenario, and as long as the operator can demonstrate to the carrier that there is collaboration between the originator of the traffic and the party finally terminating the traffic, the dispute might be justified.

The following details should be delivered by the operator:

- CDR analysis
- Fraud description based on CDR analysis (in English)
- Official fraud letter from the operator (in English)
- Official document stating that the operator has not been paid or has had a loss (quantified) for the specific portion of traffic that is disputed (in English)
- Police or other law enforcement authority report (preferably in English)

These details could then be passed on by the carrier to the next supplier down the chain to pass the dispute on; the ultimate goal being to withhold the payment (if possible, in consideration of national laws) 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 SLA's with PBX customers, legal actions against local fraudsters … From A to Z, every actor in the chain needs to take its own responsibility.

### 4.1.5 Calls to manipulated b-numbers (to +CC 0 xyz)

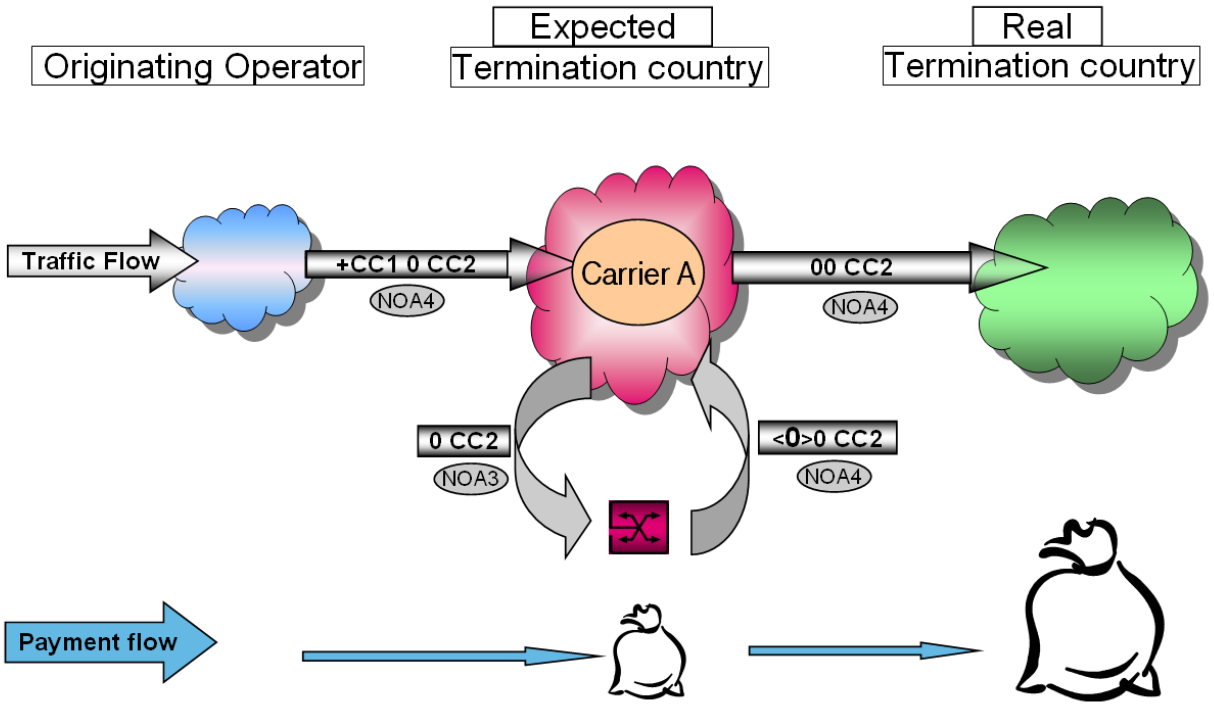



*Figure 5: Calls to manipulated b-numbers (to +CC 0 xyz)*

**Description:**

An Originating Operator 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 as 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 customer sends an operator a call with such format – where CC1 represents a 3rd country – the operator will strip the first

country code and send the call to its bilateral partner for termination. The Terminating carrier 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 WS, 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 Operator 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 results in a dispute.

- Winner:
  - End customer: might pay a lower rate for calls to expensive destinations
  - 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
- Loser:
  - 'Carrier A': has to pay out more for termination, than will receive from customer
  - Probable consequence: 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 white list on the basis of 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 black 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, than 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*

Customer 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, Customer acknowledges that such calls might lead to routing failures or even termination of calls to other international destinations. In the latter case [CARRIER] shall be permitted to invoice the Customer according to actual destination and termination of the call, based on the applicable Price List of [CARRIER], provided that call set-ups have been made and call minutes have been recorded. Disputes will not be accepted for calls sent in this format.

### 4.1.6 Wangiri Fraud (Missed call campaign)

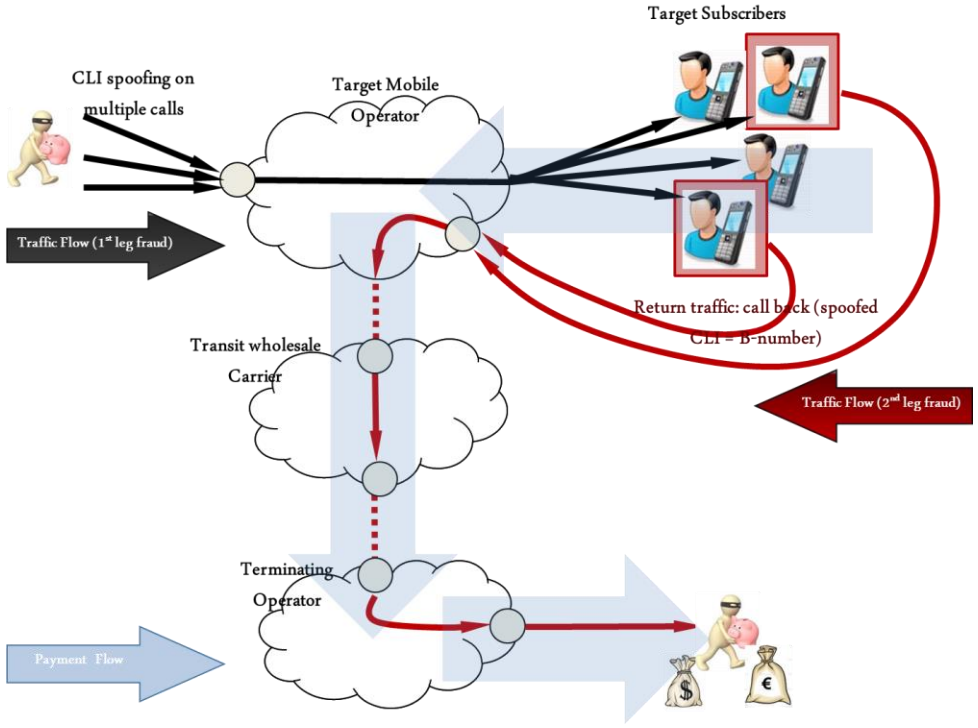



*Figure 6: Wangiri Fraud*

**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 given 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).

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 K/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.

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 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 is the 1st leg of the fraud scenario 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 call/SMS campaigns in the 1st leg of the fraud scenario. (i.e. they can send 10k attempts to carrier A, 15k attempts to carrier B, 5k attempts to carrier C, etc.). There are few costs to the fraudster as the initial call is not charged (no answer) as the majority of calls are disconnected before the Target Subscriber actually answers the call.

Even if the main wholesale Carrier that transits the calls back to the fraudulent number range (2nd leg 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 nonetheless. Thus collaboration in the industry on this kind of fraud scenario is key to stop Wangiri fraud from escalating.

**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 to be terminated on 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 2nd leg of the fraud scenario can never be completed and so the revenue is denied to the fraudsters.

## 4.2 Fraud-like Scenarios: Abuse scenarios

### 4.2.1 Arbitrage (retail flat rates)

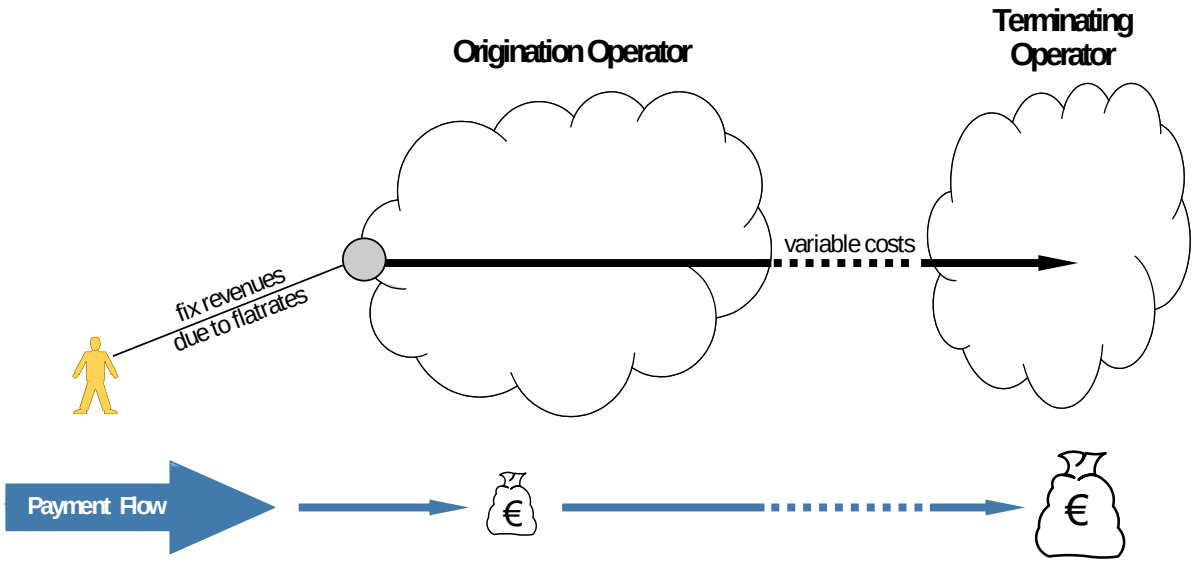



*Figure 7: Arbitrage (flat rates)*

**Description:**

An unlimited calling plan, or flat rate plan from a retail service provider to a range of international destinations enables an arbitrage misuse potential, because the retail SP 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 end customer.

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 inflation of traffic, abusing the operator and thus sending massive amounts of traffic to the destination or set of destinations being actually sold below market value.

**Issue:**

A phone flat rate ensures fixed revenue for the operator and fixed costs for the end customer. 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 operator can't cover its costs for call termination. In case of fraud and misuse, calls are made in collusion with the terminating operator 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.

- Winner:
  - Retail Customer: A high volume of calls and minutes to a particular destination are charged by a fixed price.
  - Wholesale Partner: High revenues depending on the high volume of incoming traffic
- Loser:
  - Carrier Retail: The fixed incoming revenue can't 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 blacklisting-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 blacklisting-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:**

Retail arbitrage abuses are the sole retail operator's responsibility, which should be the only liability in this case.

The wholesale carrier routing the traffic should not accept any dispute due to retail arbitrage unless IRSF or number hijacking can be demonstrated.

### 4.2.2 Insolvency of a service provider and or of another operator

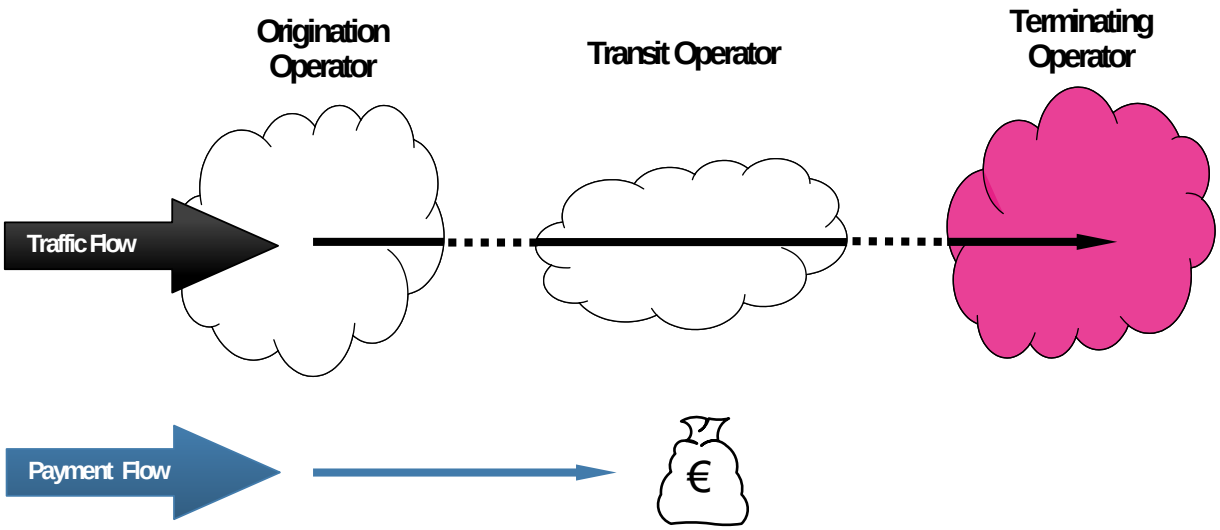



*Figure 8: Insolvency*

**Description:**

A carrier (transit operator) sends a lot of traffic, although it knows that it is insolvent and it won't be able to pay the termination fees. The transit operator 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 operator gets much traffic from a transit operator, without being paid afterwards due to the transit operator's insolvency.

- Winner:
  - Carrier that is shortly insolvent generates further revenue from its customers
- Loser:
  - Carrier Wholesale doesn't earn the expected revenue, because a carrier is not able to pay the bill and still has to pay the downstream operators

**Approaches to detect:**

- Check and verify all orders and company details, preferable periodically and in 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

### 4.2.3 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 on the market and instead of using a legitimate carrier / route to terminate the calls they use the operator 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 operator at no or very low cost (below market rate in all cases).

Call selling operations usually serve particular communities (e.g. ethnic populations through call shops).

In this case, and as long as there is no IRSF or number hijacking involved, the carrier terminating the traffic should not be penalized for such fraud. Disputes based upon such scenario should not be accepted by the wholesale community.

**Issue:**

The terminating retail SP 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.

The carrier in such scenario will receive and transit abnormal traffic streams from its 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:**

As long as 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.

### 4.2.4 Call Short-stopping

.
**Definition**:

Call short stopping can occur when a service provider/operator arranges with another service provider/operator 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 subscriber or in country operator 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 (eg. call hijacking, IRSF ...).

# 5 Call Barring Response Code

I3 Forum recommends using RC 603 in order to identify a destination blocked due to fraud.

On the basis of 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: 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:**

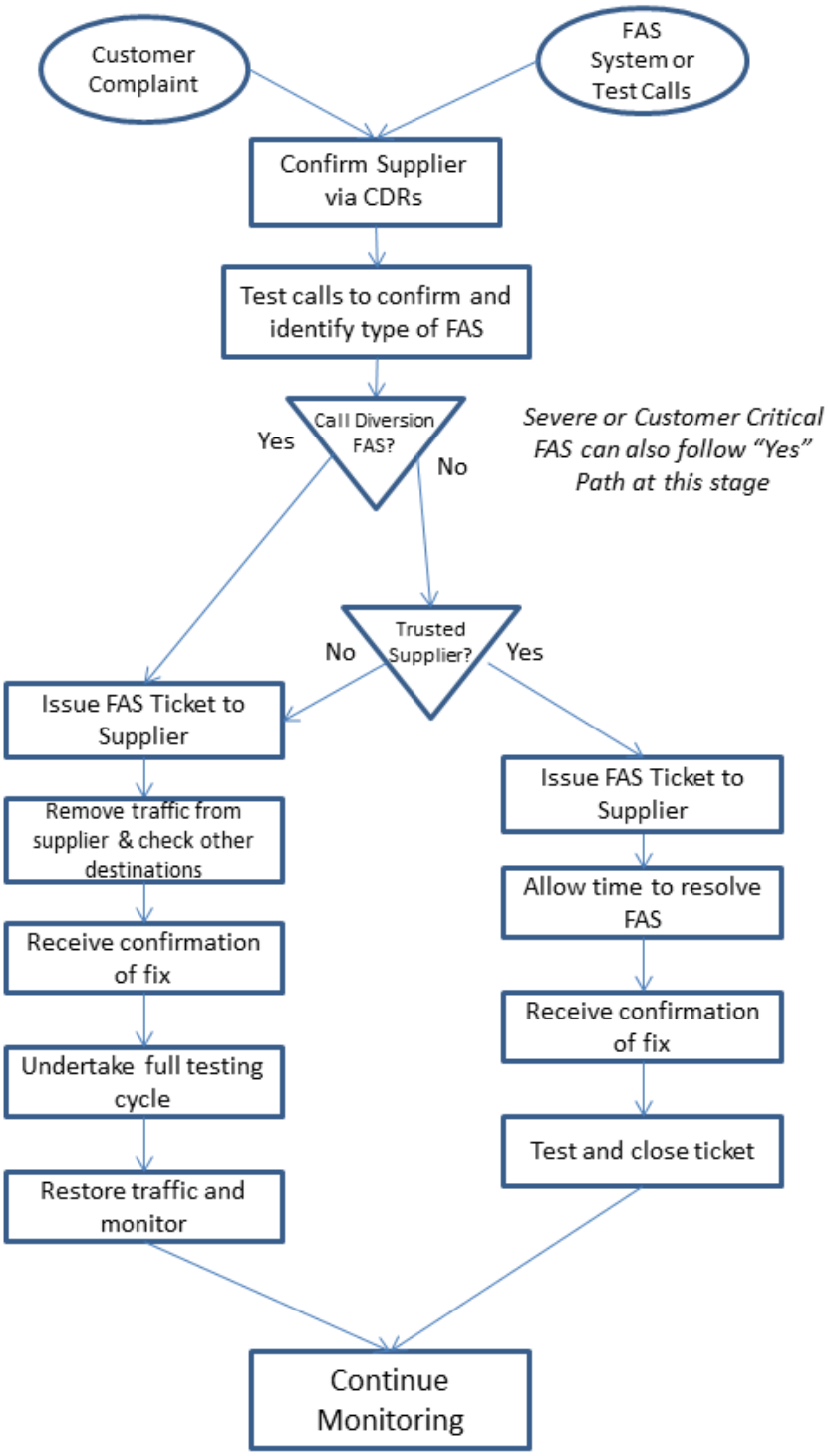
The process defined in this document is intended to enhance the ability of carriers to quickly determine the true source of the FAS problem and resolve that issue without creating quality problems for the calling customers and their service providers. Besides the obvious quality of service benefits, the capability to correctly and quickly identify FAS problems 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