International Interconnection forum for services over IP
(i3 Forum)

(www.i3Forum.org)

Source: Workstream "Fraud"

Keywords: Fraud

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

(Release 1.0) April 2012

FOREWORD

According to surveys of CFCA, ACFE and ETNO the potential commercial loss due to fraud in telecommunication networks makes 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 and its partners. The specific focus of I3F in the context of fraud prevention is the move of the industry to IP The present documentation describes several fraud cases and possible dispute actions.

Table of Contents

I. List of Figures

II. 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 a guidance to handle fraud issues in the international wholesale market for voice services.

It could be the basis for contractual clauses referring to defined fraud types and prerequisites with the target in withholding payment flows.

The sending Party may suspend sending traffic to certain dialling codes / numbers and will not pay the incurred charges for traffic that has been already 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 3.2 and 4. 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.

Generic fraud scenarios have been described and they are responsible for a considerable commercial loss. Besides a description of every single fraud scenario chapter 4 provides approaches to detect, approaches to avoid a particular fraud scenario and information on the dispute handling.
Furthermore chapter 4 contains information about workflows to detect fraudulent traffic.

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).
Eight different parameters have to be analysed to ensure a best possible detection of all common fraud scenarios.

2 General Information

2.1 Recommended workflow

In the case of a suspicious fraudulent traffic, a central mailbox could be contacted.

Fraud co-workers like Product Management will analyse traffic flows and potential fraudulent destinations or originations. If necessary, counteractive measures will be initiated by the fraud co-workers 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. Two separate communications should be sent that could contain at least the following details:

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

The customer remains liable for the traffic sent. In addition, a key element to any dispute due to fraud is respecting the deadlines and timeframes set by the carriers's procedures to avoid adding complexity to the case by breaching the commercial terms of the agreements in place.

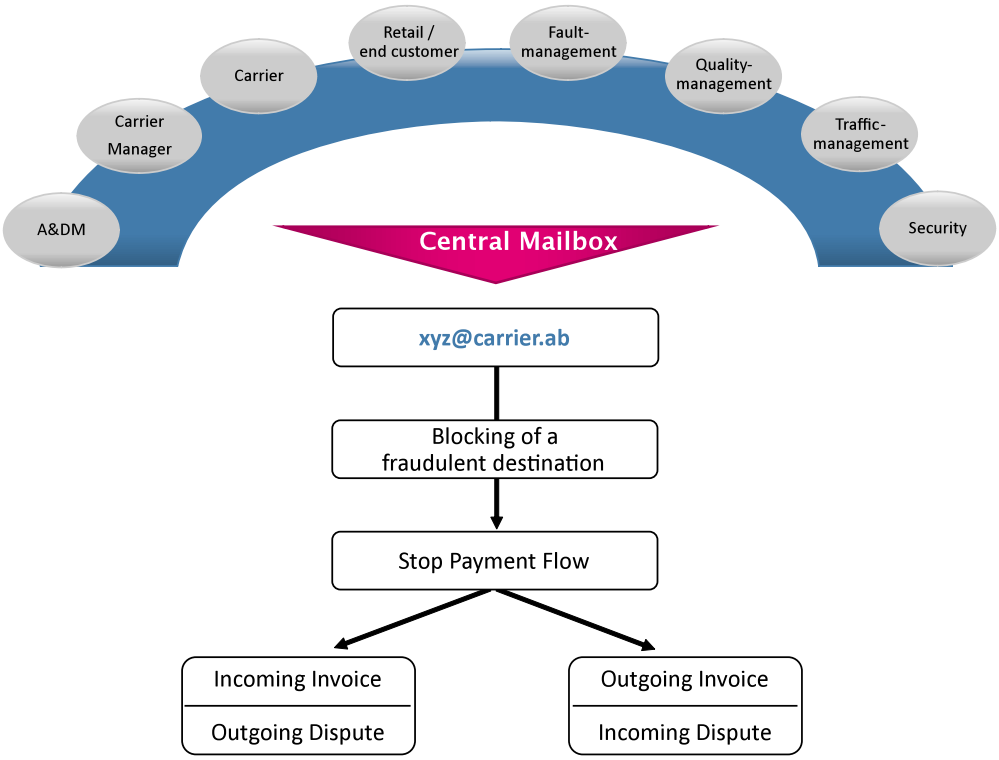

Figure 1: What to do in case of fraud

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), 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 actually hit the fraudsters and not to just cover for the revenue loss and push responsibility to the carrier.

A specific portion of traffic sent by an operator could be considered as “disputable” to the carrier terminating the traffic, as by issuing the payment to the suppliers in the chain the fraudsters will eventually be paid for non-legitimate traffic.

- The intended outcome of i3 Forum practices is to impact the fraudsters. It is not recommended to take the carrier hostage by denying or withholding payment.
- 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.
- Carriers 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.
- Each carrier will determine the respective threshold (disputed value)to accept/refuse disputes
- If, for any reason, the carrier is not able to withhold the payments, the liability remains with the retail operator.
- In case of suspicion of fraud the carrier always has the option of taking action independently of its customer.

3.2 Elements outlining fraud

The prerequisite to accepting disputes due to fraud: 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

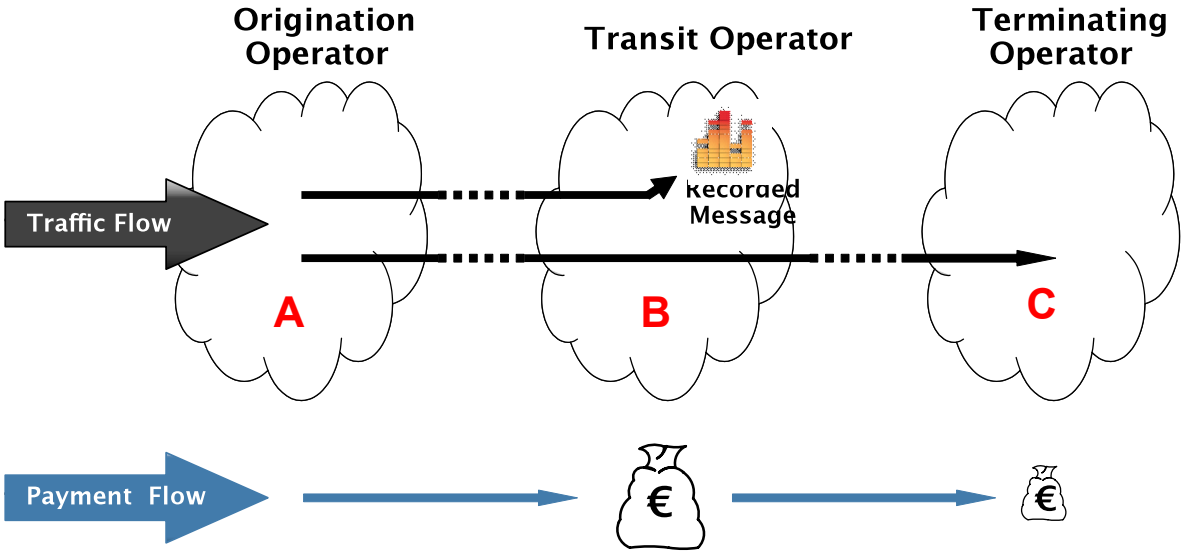

Figure 2: Call Hijacking

This fraud scenario is also known as: Blueboxing, call short stopping, number plan misuse, non-legitimate destinations.
Description:
A certain percentage rate of the calls which should be terminated in network C is intentionally routed to a server with, normally, a pre-recorded message by transit operator B. The caller will never reach the legitimate called party. Transit operator B charges all calls at the rate committed and has nearly 100% margin on all calls which are routed to the recorded message. The transit operator offers low prices and due to that it gets much traffic. All in all the traffic towards a transit operator that hijacks calls increases, because an end customer initiates a further call after he ran on a recorded message.

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 stick with rogue dialler software), possibly followed by call forwarding misuse or roaming misuse.

Issue:
A call initiated by a consumer terminates (for example) on a recorded message or on an imitated answer signal tone and the consumer doesn’t get the demanded service but the call will be fully charged by the network operator anyway. The whole amount of traffic sent via this transit operator towards an terminating operator that is affected by call hijacking in the case of call hijacking, so it isn’t effective to block particular numbers or number ranges.

- 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 get an 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.
- Analysing complaints of end customers
- The offered rate for termination is below the range of most other offered prices (market price)
- CLI testing tool: Using a CLI testing tool one can make calls to predetermined numbers without asking the provider anything, and let the testing tool give you all the answers. Another method would be to get test numbers by the vendor solution provider. If a test call doesn't reach the expected destination, the call is possibly hijacked.

Approaches to avoid

- Change 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 wholesaler 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

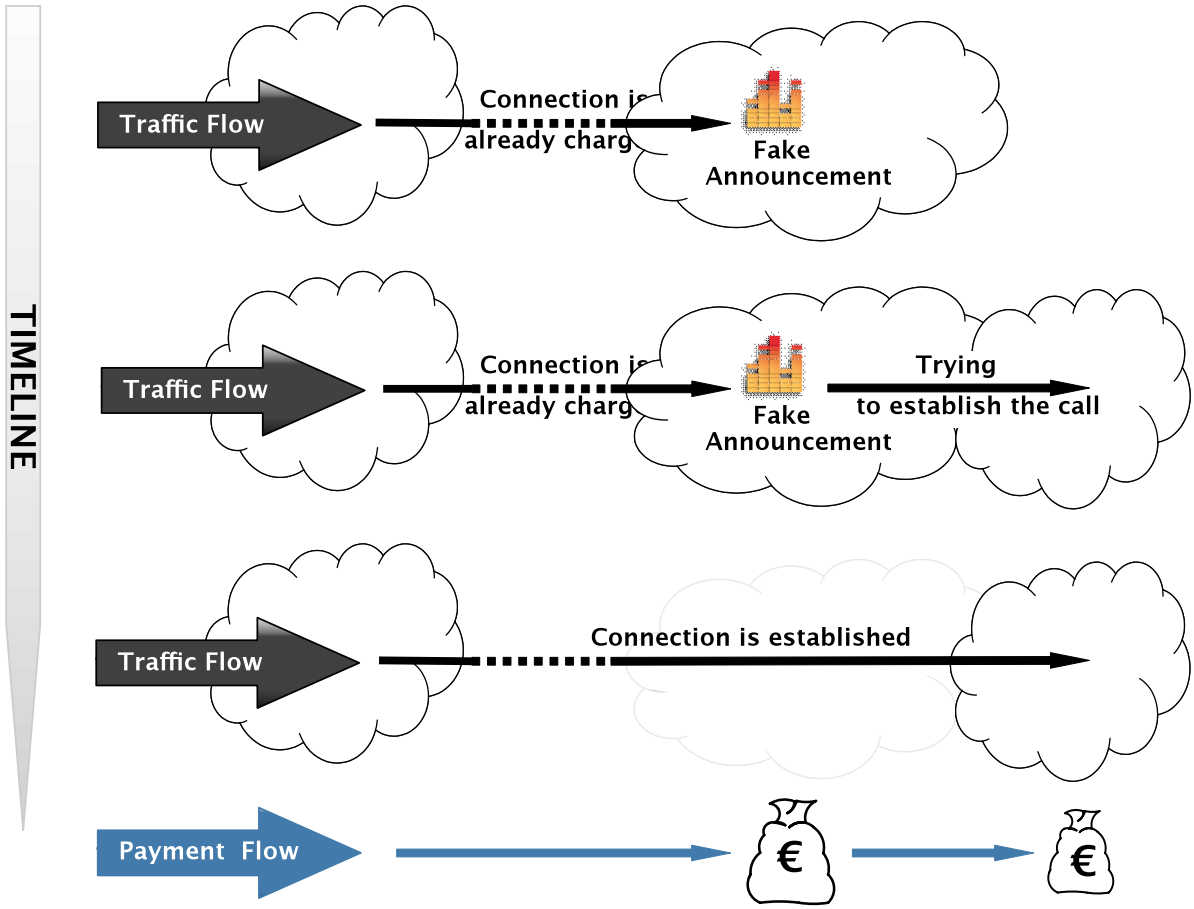

Figure 3: False Answer Supervision

Description:
For this, a party in the traffic flow chain sends a false signal indicating that a service has been established even though such is not the case. Calls are being charged for a longer call duration than the way commonly in the industry to measure call duration: calls not connected are billed as completed calls, the calling party is charged for the call set-up time (early answer, dead air, artificial answer, etc.).

Issue:
A call is charged before the service is actually established (between the calling-party and the called-party). Consumer has to pay more than they should. If the called party doesn't reply but the call is charged anyway, the consumer probably notices a wrong charge (especially in case of calling card operators).

- Winner:
  - Operator that starts charging for a call, although it isn't yet established.
- Loser:
  - Carrier and their wholesale partner (image, disputes)
  - Consumers get an invoice for services they didn't use

Approaches to detect:

- Comparing measured call duration with the expected call duration
- Analyse if there are calls with short duration (5-10 sec.)
- Analyse the duration of call status "ringing" and compare with the average and the median duration of all 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 call shops complain about FAS: Its customers don't pay for a call which isn't really established, but its operator charges the call)
- Implement a probe-based FAS detection system based on sample calls
- Implement a FAS detection system based on call patterns analysis

Approaches to avoid:

- Only reactive handling possible. Once detected the carrier should re-route the traffic towards another supplier and open a trouble ticket mentioning FAS.

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.
Further recommendations on FAS dispute handling (process, workflow, etc) are under investigation at the moment.

4.1.3 Hacking of a customer Telephone System / Software Manipulation

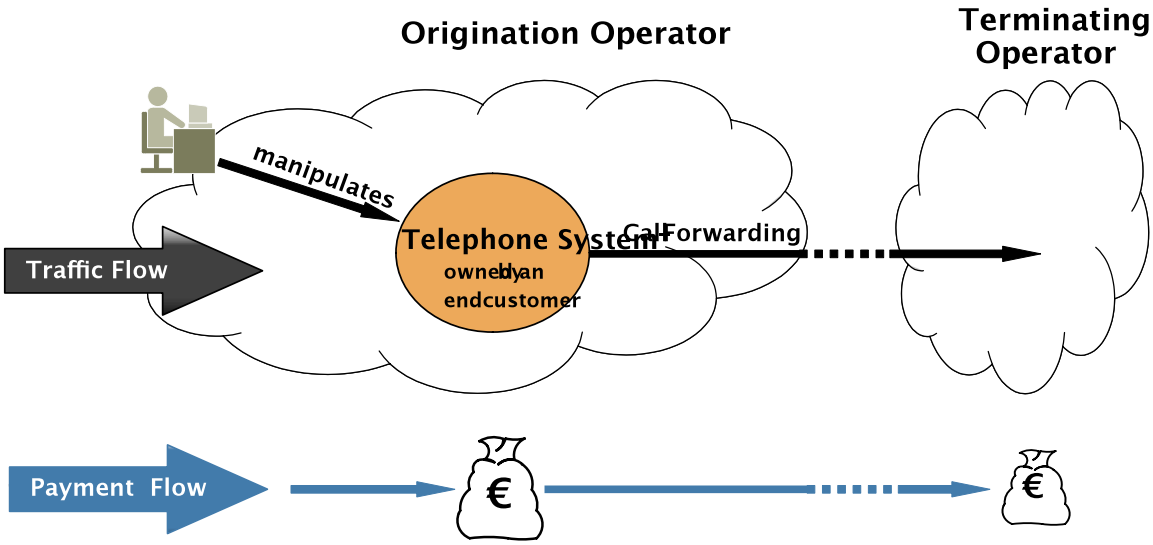

Figure 4: Hacking of Telephone System / Software Manipulation

Description:
An Attacker tries different default 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 makes a lot of calls to the telephone device which forwards the calls. In some other cases the attacker programs software which initiates calls automatically, instead creating call-forwarding or call dial-thru (is also 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.
  - This fraud scenario is observed in combination with fraud scenarios such as “call hijacking (short stopping of calls)” and “international revenue share fraud (IRSF).
  - All (retail) customer systems (pbx or ip-pbx or voip-routers) and or (retail) customer equipment (mobile smart phone or mobile stick with rogue dialler software) could potentially be misused too. This could be “fraudulently optimised” by using call forwarding and or roaming.

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 possibly to others (call-through services).
  - 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)
  - End Customer gets an invoice for services they didn’t want to use.
  - End Customer could get unreachable by customers and or could lose capacity due to a high load of manipulated calls (denial of service).

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 inform the Service Provider.
- Analyse the duration of calls to high price destinations from a particular calling party number.
- Monitor destinations of found traffic relative to existing and publicized number plans, traffic type, tariff models and possible extra white-and-blacklisting-functions (possibly derived from previous found 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 case:

- Inform customers and the related service engineers about potential fraudulent usage of retail customer telephone system (there is a bad messenger risk in case of already experienced misuse).
- Encourage customers, after raising awareness about the threats, to order 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 important 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 Premium Rate.

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 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 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.

- 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 disproportioned /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 a Premium number when a domestic premium option/equivalent exists?

Approaches to avoid the case

- 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)

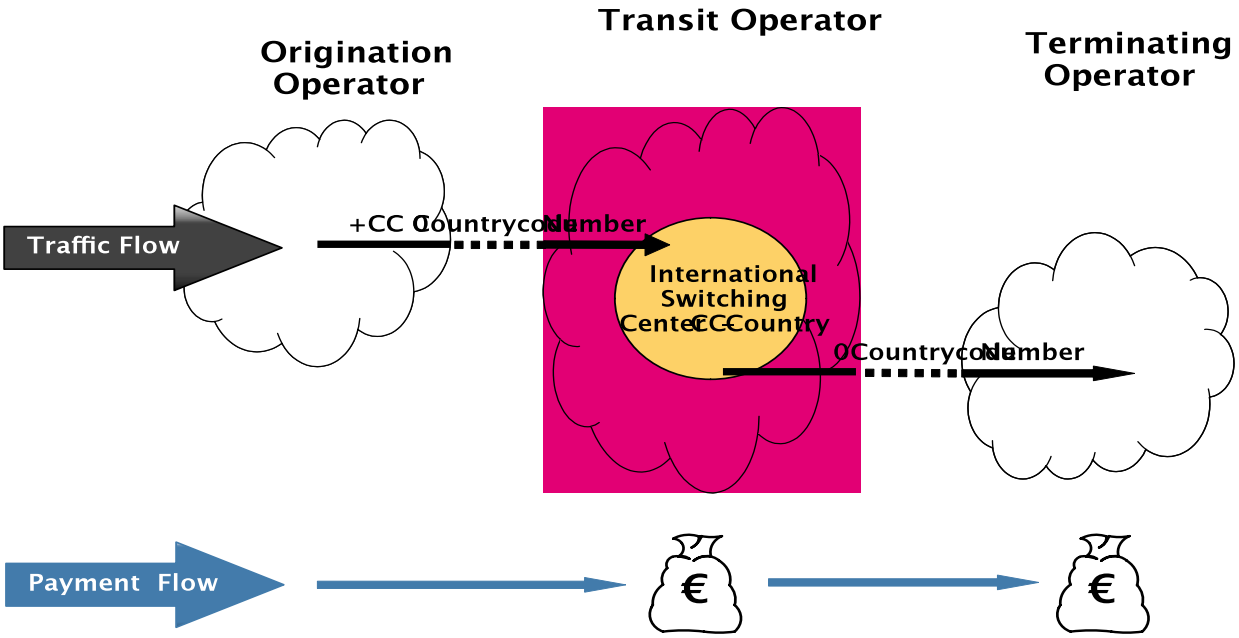

Figure 5: Calls to manipulated b-numbers (to +CC 0 xyz)

Description:
An originating operator sends a call with the prefix +CC 0 (CC = Country Code, e.g.: 49 for Germany) and after that a further (additional) country code and number. Due to the prefix +CC the call will be routed to the country's international switching centre. The switching centre cuts the +CC, detects a 0 and a further country code and routes the traffic to the destination accordingly. The operator of the calling-party will charge the connection with the country termination rate. The operator which provides the transit will charge the connection with the termination rate of the destination.

This scenario might happen due to technical restrictions or misconfiguration in the switch, or even local country limitations (eg. in Italy, local fixed numbers start by "0").

According to the recommendations of the i3F Technical WS, international codes should be prefixed with "+" instead of "00".

Issue:
Some carriers deliberately manipulate a called number to charge a lower rate for a particular destination. Other calls could be accidentally initiated by end customers. The billing systems of the involved operators record different services and prices and this probably results in a dispute.

- Winner:
  - End customer: Probably he has to pay a lower rate for his call.
- Loser:
  - Carrier Wholesale, Wholesale Partner: Dispute, because their billing systems detect different services and prices.

Approaches to detect

- Analyse CDRS on frequency and in duration for relative changes by time.
  Monitor usage of traffic from not registered a-numbers (white list check).
  Compare usage of own registered numbers with the found outgoing traffic (re-conciliation).
- Technical analysis of received call set up, call parameters and filtering unacceptable operational combinations out, if they look doubtful. A white list on the basis of the trusted and accepted own OPC (Originate Point Code) could offer such an analysis.

Approaches to avoid

- According to the contract between Carrier and other operators it is forbidden to send this kind of traffic.
  Although:
  - In the ISUP case: If the international switching centre strips the +CC will assign a NOA NAT and it will never route the call to an international carrier.
  - SIP case if we extend the logic of the NOA in the SS7 world on to SIP using the “+” sign on the SIP URI that will also not happen.

Information of dispute handling
In such scenarios, unless IRSF or number hijacking is involved, the carrier should not be impacted and disputes should be rejected.

4.2 Fraud-like Scenarios

4.2.1 Arbitrage (retail flat rates)

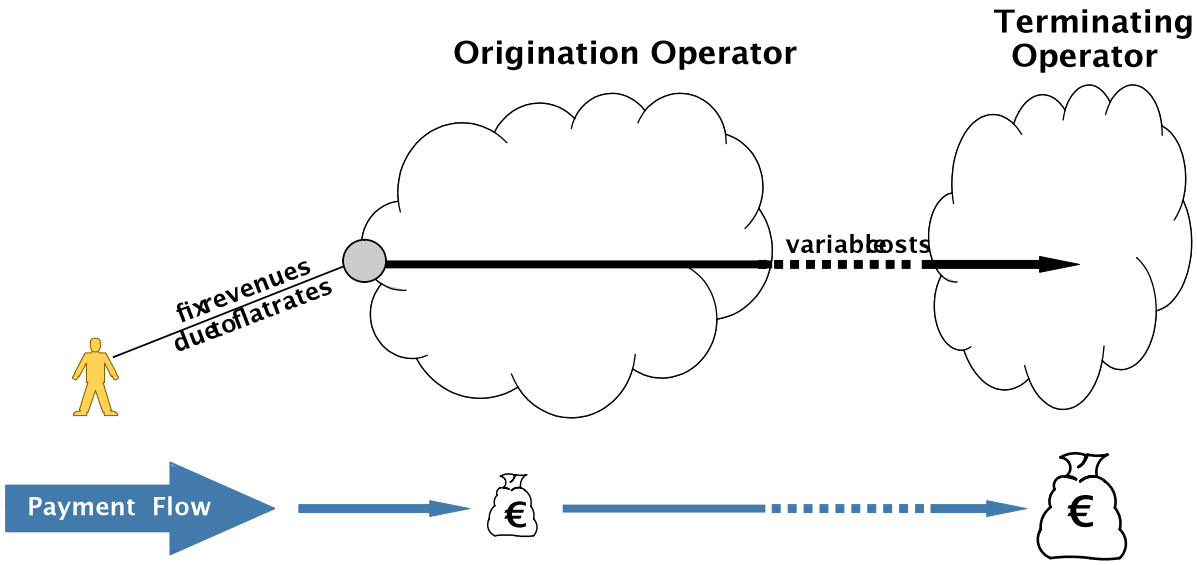

Figure 6: Arbitrage (flat rates)

Description:
A phone flat rate in a retail network to a particular destination or set of destinations contains an arbitrage misuse potential, because generally not the cost for all the destinations is covered by the flat rate and the calling network operator will have to pay the agreed termination rate per minute to the supplier operator.

In case of fraud, a lot of calls are made to generate revenue and the called party could be e. g. a just gathered traffic, 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 volume of minutes that a consumer is calling normally. 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) of a termination tariff. Also, a recently offered discount to retail customers can create the same situation, of a wrong business case.

- 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 fix 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 budgets or business cases become exceeded.

- Monitor destinations of found traffic relative to existing and publicized number plans, traffic type, tariff models and possible extra white- and blacklisting-functions (possibly derived from previous found cases).

Approaches to avoid

- Accurate retail pricing.
- 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 are covered by a fix price flat rate.
- 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 questioned 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

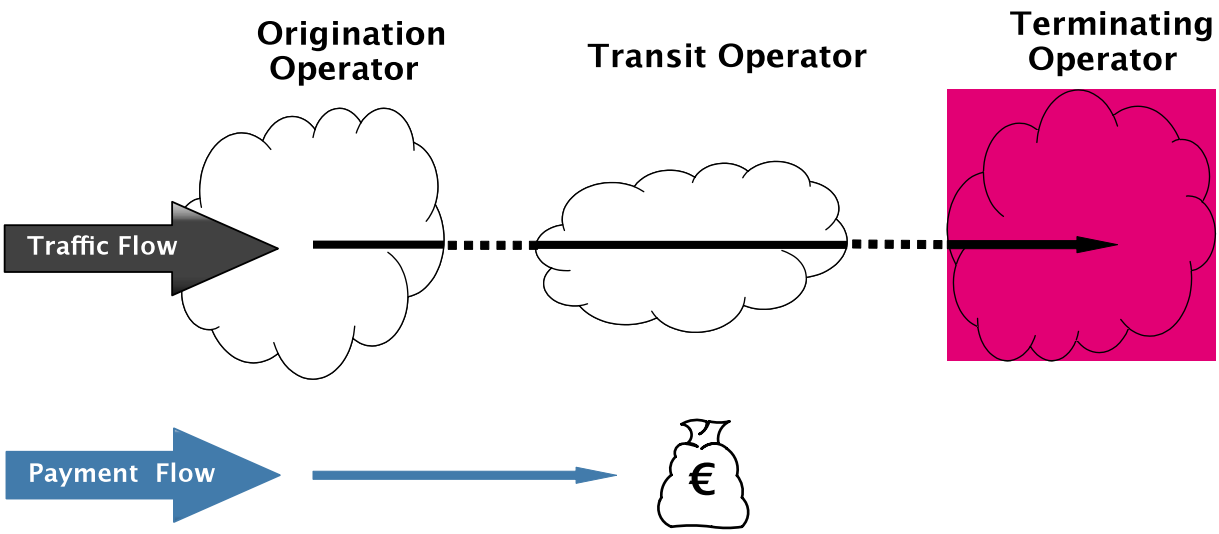

Figure 7: Insolvency

Description:
A carrier (transit operator) sends a lot of traffic, although it faces to become 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:
CARRIER 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
- Loser:
  - Carrier Wholesale doesn't earn the expected revenue, because a carrier is not able to pay the bill.

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 explodes suddenly
- Set up an alert of the news about an impending insolvency of a carrier in the current portfolio.

Approaches to avoid

- 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.

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. Disputed based upon such scenario should not be accepted by the wholesale community.

Issue:
The retailer 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 terminating the traffic should not be penalized for such fraud. Disputes based on this fraud scenario should not be accepted by the wholesale community.

5 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.