subex
powering the ROC

White Paper

Bypass Fraud- Are you getting it right?

www.subex.com

White Paper Bypass Fraud- Are you getting it right?

Contents

White Paper Bypass Fraud- Are you getting it right?

Abstract

Bypass fraud is proving to be one of the most fertile and costly frauds in today's mobile industry making mobile operators and telecom regulators face a staggering annual revenue losses due to these fixed/VoIP to GSM/CDMA/Fixed line gateway equipments, which are used to terminate international inbound calls to local subscribers by deviating traffic away from the legal interconnect gateways.

Bypass fraud is more prevalent in the countries where the cost of terminating international call exceeds the cost of a national call by a considerable margin or the countries where international gateways are monopolized by government carriers. Fraudsters (individuals or organisation), through the use of different Bypass mechanisms, sell capacity to terminate calls cheaply in these countries, on the open market or through direct connections with interconnect operators.

Operators sending outbound international traffic are then attracted by these interconnect operators with lower interconnect rates. This leads to lost revenue for terminating network operators. Bypass is considered illegal since those who undertake it are not licensed to provide telecommunications services in the affected country. In some countries this act is also considered to be a national security threat due to the limitations posed in complete lawful intercept of these illegally bypassed international incoming calls. Africa & Middle East have been identified as one of the regions severely affected by Bypass Frauds.

The common approaches to combat against Bypass Frauds have been the use of monitoring calling patterns and profiles through Fraud Management Systems and the use of Test Call Generators. Both approaches, having their own set of merits in terms of accuracy, coverage and flexibility, also suffer from drawbacks which make the use of any individual technique against Bypass Fraud, insufficient.

This paper by Subex puts light over an integrated and hybrid approach combining best of both FMS and TCG to create a comprehensive and best in class solution to combat Bypass Fraud. As there are currently numerous ways of conducting Bypass fraud, this paper will concentrate more on the SIM Box mechanism, currently the most popular way of conducting Bypass Fraud, for demonstrating the problem and the proposed solution.

> Approximately **2.88 Billion USD of** revenue is lost due to Bypass Fraud every year. An increase of more than 44% over the 2009 survey
>
> *- CFCA 2011 Global Fraud Loss survey*

Bypass Fraud Is Big

What is a Bypass Fraud?

Bypass Fraud is used to describe the use of various least cost call termination techniques like SIM Boxes, Leakey (hacked) PBXs etc. to bypass the legal call interconnection and diverting international incoming calls to 'on' or 'off' network GSM/CDMA/Fixed calls through the use of VoIP or Satellite gateway, thus evading revenue for international call termination which operators and government regulators are entitled to.

White Paper Bypass Fraud- Are you getting it right?

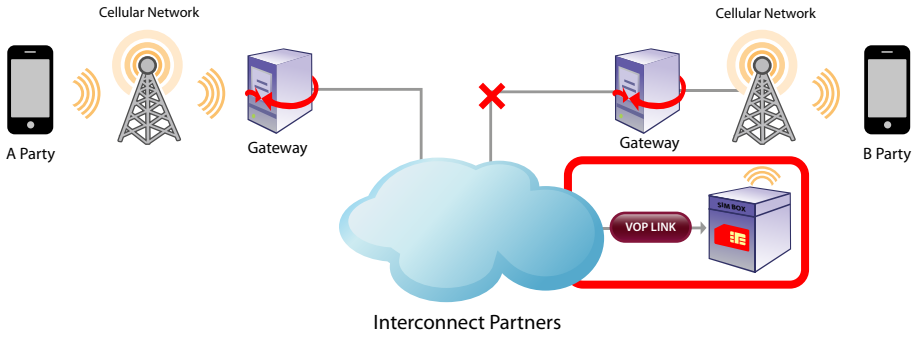
The Motivation

Fig. 1 below details the use of a SIM Box in conducting International call bypass through a VoIP link and the increase in revenue obtained by the interconnect operator bypassing the call through a VoIP link which in turn is terminated to the end user using a SIM Box.

Bypass Fraud is generally prevalent in the countries where there is a big difference between the national retail calling rates/national interconnect rates and international terminating rates, either set by the regulator in the country or set by individual (or group of) operators (unregulated). It is also popular in the countries where international gateways are monopolized by government operators. The difference in rates ensures there is enough profit margins for the fraudsters, which serves as the key motivation factor for them to invest on obtaining the technology, equipments and GSM connections required for conducting Bypass fraud on a large scale.

Countries where the international to national terminating charge margins are low, nil or negative, the Bypass fraud either does not exists or is conducted at a very low scale.

The connections used for conducting Bypass Fraud can either be hacked PBX/Voicemail systems or normal Fixed/CDMA/GSM postpaid or prepaid lines, generally picked up in bulk under the name of a Small-Medium enterprise or by conducting a subscription fraud, with or without the help of a dealer. Generally 99% of the connections used are found to be prepaid as prepaid connections are easily available without much documentation or proofs.



Normal Call	*Retail cost = 1$, A's revenue = 40c*	*IC Cost = 60c, IC revenue = 20c*	B's revenue = 40c
Bypassed Call	*Retail cost = 1$, A's revenue = 40c*	*IC Cost = 60c, IC revenue = **50c VoIP carrier = 10c***	**B's revenue = 5c, Loss = 35c** *(Only Retail or Offnet Termination revenue)*

***IC = Interconnect Operator*

As fraudsters conduct Bypass fraud to earn through the international to national terminating charge margins, they strive towards keeping the connections, which are used to generate national terminating calls, always up and running through constant recharges (prepaid) or making regular payments (postpaid) or through constant hunting and hacking of less/un-secured PBX/Voicemail systems.

Due to the involvement of payments for the services used, the legacy Telecom Fraud definition *'the intention of non payment'* might not apply in case of SIM Box or Fixed line flavour of Bypass Fraud. This fact when combined to the outgoing load balancing, actual subscriber usage pattern mimicking (like SMS generation, inter calling, data usage etc.) and other counter detection capabilities provided by the modern equipments providing Bypass capabilities, makes the detection of Bypass cases complex and prone to a prolonged fraud run time.

Onnet & Offnet Bypass Fraud

The connections used to conduct Bypass fraud are generally the ones which have the least national calling rates to the terminating party (B Party). This ensures maximum international to national terminating charge profit margins for the fraudulent parties involved in the racket.

As the ONNET calls are expected to provide the least national calling rates, some modern Bypass equipments (SIM Boxes, computer programs etc.) scan the terminating party numbers and originate calls only from those connections which belong to the same operator's network as the terminating party.

But in the regions where even OFFNET calls rates are on par with ONNET, there can be national calls originated even from the OFFNET connections to conduct Bypass fraud.

For an operator, if a fraudster uses its own network's connections to terminate the bypassed calls, it is identified as **ONNET Bypass Fraud**

But if the fraudster uses competitor's connections or any other means for termination, it is identified **as OFFNET Bypass Fraud**

Huge Losses From Bypass Fraud

Presence of Bypass Fraud, ON-NET or OFF-NET has equal negative effects on operators, regulators and customers alike. Few major impacts are

Revenue loss due to call redirection

International calls are intercepted, redirected and terminated whilst being re-conducted via the fraudulent route, creating a cost / revenue shifting along the way.

In the most extreme cases it is claimed that bypass fraud can account for a 50% reduction in international termination revenues. Reductions of $250K/month in revenues are certainly commonplace, and reported losses up to $200M per annum have been known at a single operator and regulator.

Revenue loss due to service inaccessibility & missing call backs

Bypass Fraud has the negative effect that multiple popular services, e.g. voice mailbox, may not be available. Revenue loss and unhappy customers is the consequence. Also, due to the redirection of calls, none or wrong CLIs will be displayed at the recipient's side; immediate impact is the inability to "call back" resulting in a significant opportunity loss of retail revenue.

Call Hijacking and lack of Lawful Interception

Bypassing involves hijacking call traffic and routing them over unauthorized channels. This act is identified as illegal in many countries not only in terms of route bypassing, but also in terms of possible national/personal security intrusion.

Also, due to the lack of the original CLI, Lawful Intercept (LI) of the bypassed call is not completely possible. This leads to a failure in terms of national regulatory compliance.

For **On-Network terminating calls** (connections used for Bypass Fraud belong to the home operator), the revenue loss per call is directly related to the difference between the international interconnect termination price and the retail price of on-network call.

For **Off-Network terminating calls** (connections used for Bypass Fraud belong to competitor), the revenue loss per call is directly related to the difference between the international interconnect termination price and the local interconnect termination price of off-network calls.

Additional Investment

Sometimes traffic hot-spots and congestion caused by bypassed traffic can lead to substantial unnecessary site acquisition and roll-out costs for new radio access equipment (BTSs, Node Bs, and even BSCs).

Image loss due to bad QoS

Bypass Fraud generally is based upon redirecting calls over inadequate, highly compressed IP connections, resulting in poor voice quality and increased call failure rates because of congestion caused through use of a bypass. Call setup time or routing delays are extended which also leads to the impression of an overall bad service quality by the home network operator.

Different techniques used to detect Bypass Fraud

There are currently two popular ways of uncovering Bypass fraud being used by operators and regulators:

- TCG Approach
- Statistical Profiling based detection through an FMS or scripts

TCG - Test Call Generation

This approach is based upon automatic generation of controlled traffic to known MSISDNs in operator's network through large portfolio of originators across the globe including fixed, CDMA, GSM, VoIP, calling cards etc. and monitoring the landing CLI on these MSISDNs or analysing the call information in operator's network through probes.

TCG approach shows the following advantages and disadvantages:

Advantages

- **Very high fraud hit ratio** – Sometimes even more than 90%
- **Proactive identification** – Connections can be detected even when no Bypass Fraud call pattern is shown in the past

Disadvantages

- **Incomplete coverage** – Not possible to cover all VoIP services across the world. Coverage is also tightly coupled with number of test calls generated.
- **Susceptible to counter attacks** – TCGs may become useless just after few days of operation as the Call bypass node may be programmed to reject (or leave) calls originating from the TCGs after some experience or pattern analysis.
- **Minimum learning out of Fraud Hit** – In absence of CDRs, information related only to fraudulent MSISDNs with route information is obtained. This leads to a situation where maximum of one fraudulent MSISDN can be identified per test call.

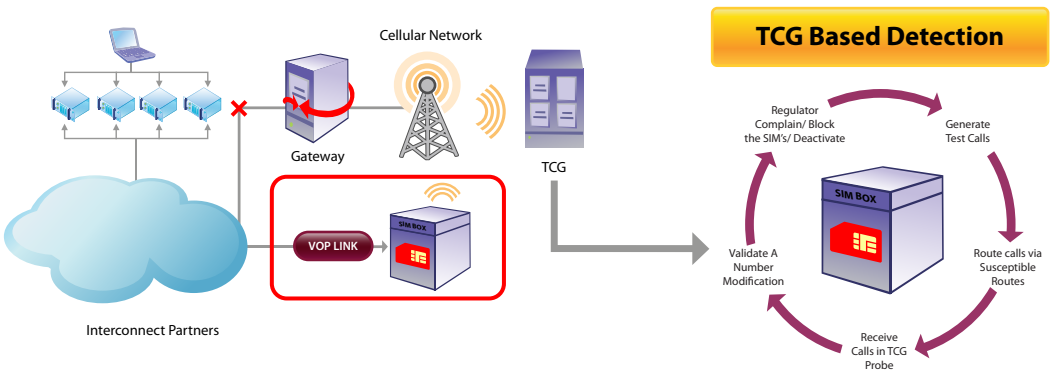
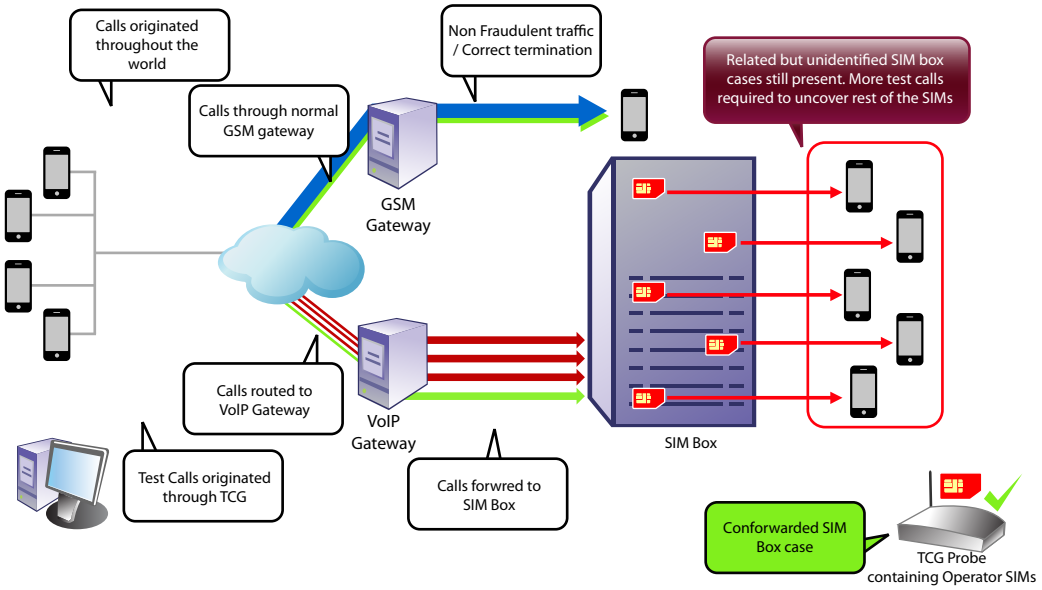


Figure 2 provides a high level insight over the TCG approach.

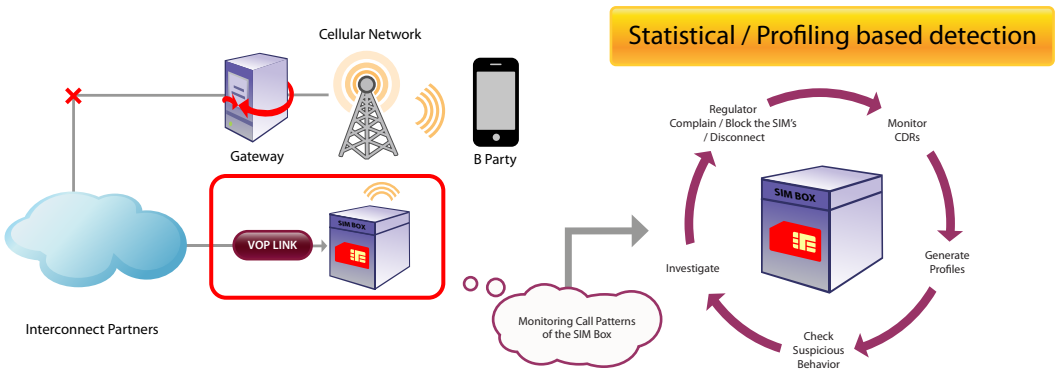
Figure 3 details the 'Minimum learning out of Fraud Hit' problem faced by TCG approach.



Fraud Management System

This approach is based upon identification of Bypass Fraud by monitoring complex call patterns (Outgoing call count, distinct destinations ratio, cell sites used, incoming to outgoing call ratio, SMSO, SMST counts etc.) originating from an Operator's MSISDN or terminating over it. Any cases identified can then be used to profile and uncover other associated MSISDNs which are being used in the same Bypass Fraud racket.

Figure 4 provides a high level insight over the TCG approach.



FMS approach shows the following advantages and disadvantages:

Advantages

- **Better coverage** – With the availability of CDRs, call profile and pattern based detection, accompanied by advanced analytics, It has the potential to cover all
- **No additional investment** – No additional cost apart from FMS
- Bypass Fraud specific call patterns can be converted to Rules for identification

Disadvantages

- **Susceptible to counter attacks** – With the evolution of Bypass fraud through hacking, programmable equipments, Inter connection voice and SMS, Data usage, actual subscriber usage pattern mimicking etc., fraud detection through FMS has become more difficult than ever
- **More reactive monitoring** – The detection techniques provided by FMS tend to be more reactive than TCGs. Unless there is a usage made with a specific pattern, the case will remain undetected
- **Latency in detection** – Providing a reactive method of detection followed by the investigation process involved to confirm the fraud, FMS leads to some amount of detection latency

Some sample call patterns shown by SIM Box, the most popular means of conducting Bypass Fraud:

Stationary or low mobility – Number of distinct BTSs not high

Voice only usage – No or extremely low number of incoming and out SMSs

Less incoming call but continuous outgoing calls (not always very high in number)

No common number calling – Distinct called parties

Sample conversion to a FMS statistical rule:

Outgoing call count > 80/day

Incoming/Outgoing call ratio < 1%

Number of distinct called numbers/Number of total outgoing calls > 95%

Number of Outgoing SMSs < 5

Number of Incoming SMSs < 10

Number of distinct Cell Sites used < 3

**Not all FMSs have a capability of statistical analysis and rule formation*

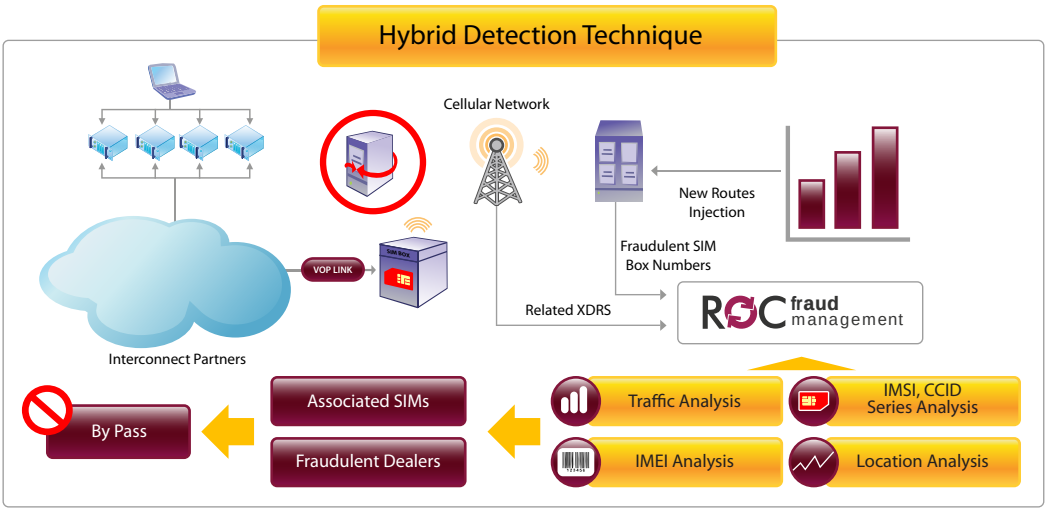
Best bet! Combine TCG and FMS to prevent Bypass Fraud

With the strengths and weaknesses of the FMS and TCG approach known, what can be the solution to the ever increasing Bypass Fraud problem faced by the operators and regulators equally?

How about bringing both the approaches under a single complementing solution which will eradicate the deficiencies faced by each of them individually?

Integrating the accuracy offered by a TCG solution with flexibility and higher coverage offered by a FMS may prove to be the perfect weapon in this current fight against Bypass fraud. Figure 5 details the high level architecture for the proposed integrated solution.

White Paper Bypass Fraud- Are you getting it right?

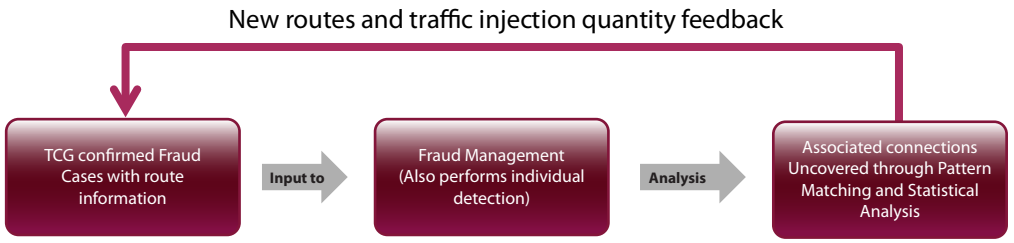


The idea behind integration is to generate a maximum impact on the whole Bypass Fraud racket using every confirmed fraud MSISDN identified either by TCG or FMS, with both the systems sharing actionable intelligence.

Solution Details

If the confirmed Bypass Fraud MSISDN cases detected by the TCG are provided as an input to FMS automatically, with details like fraudulent MSISDN, Route/Trunk Information, Call origination country, time of the test call made, FMS can then initiate a dedicated and combined Traffic, Account, IMEI, IMSI, CCID, Location and Profile analysis, over the Subscription and Usage database readily available to it, in order to uncover the associated numbers involved in the same Bypass Fraud racket, but remained undetected by TCG. This will ensure there is a much deeper level of penetration and impact done over the whole Bypass Fraud racket with every confirmed fraudulent MSISDN identified by TCG**.**

Figure 6 below details the working of the integrated solution:



Apart from performing a deep dive analysis over the cases produced by TCG, FMS will also continue to work independently to uncover the Bypass frauds, using its inbuilt statistical, behavioural and profile analysis engines. The cases identified by FMS alone can then be input back to TCG as **new/unexplored route identification mechanism and traffic injection control feedback.**

Analysis In FMS : Uncovering Associations

For every confirmed fraud MSISDN information provided as an input, FMS can perform the following analysis to uncover other associated MSISDNs being used the same Bypass Fraud:

Traffic Analysis

- Profile matching of the fraudulent MSISDN across existing active subscriber base to uncover similar calling pattern cases
- Account level Analysis to uncover the associated connections, if postpaid
- Common Dealer identification to uncover the involvement of a Dealer in arranging the connections in bulk for use in a Bypass Fraud
- As connections used in Bypass Fraud are generally acquired in bulk, phone number series analysis and identification would also provide fruitful results
- Modern Bypass equipments, as part of the counter detection techniques used, can also make calls or send SMSs to the different phone numbers used in the same equipment. Therefore, identification of the terminating numbers for the SMSs/calls sent by the confirmed fraud case identified by the TCG may also lead to other associated numbers in the same Bypass Fraud.
- B Number cloud analysis can also be performed to uncover the common A numbers which are part of the any Bypass Fraud
- Route Analysis can be performed to identify the source of traffic origination (country) for more focus or reporting with the interconnect operators involved

IMSI/CCID or other unique connection ID Series Analysis

- As connections used in Bypass Fraud are generally acquired in bulk, IMSI/CCID or other unique connection ID series analysis and identification may also lead to higher hits.

IMEI Analysis

- Exact IMEI/Equipment or prefix analysis can be performed to uncover the related connections from the same equipment used to conduct Bypass Fraud.
- Luhn check or any other verification mechanism can be applied to uncover Bypass equipments with invalid IMEI or other equipment identity, which have high chances of Fraud as these equipments are generally manufactured and sold in grey markets

Location Analysis

- Cellsite or Geo Position analysis can be performed over the confirmed cases reported by TCG to identify high risk locations for higher concentration

Location analysis can also become an input to other private/government/law agencies for accurate identification of the bypass equipments installation location in an area for its complete physical removal

Peace of Mind! Benefits of using optimal solution for Bypass Fraud prevention

Integrated Solution

This approach provides a much needed, intelligence feedback based, 360 degree control over the Bypass Fraud detection and a single consolidated solution with seamless integration, workflow and maintenance which leverages positives of both active (TCG) and passive (FMS) monitoring techniques. This leads to a chance to uncover the whole Bypass Fraud racket just through one confirmed lead provided by either TCG or FMS.

Integrated Resourcing

No need to build separate teams for both FMS and TCG operations. A single integrated pool of resources should be able to handle investigations for cases reported by both TCG and FMS. This approach makes sure that integration is not only at the product solution level but also at the resourcing level.

Integrated Operations

Integrated operations can be built by loading of confirmed bypass cases identified by TCG into FMS for bringing these cases into mainstream investigations executed through predefined workflows. TCG specific reporting and charts can also be built into FMS which will ensure there is a single integrated management and reporting platform too.

A single reporting platform also provides regulators a much needed way to keep an eye over the health of every operator in terms of Bypass MSISDNs/cases identified in their respective networks

Integrated RoI Identification

With history CDRs available with FMS, accurate RoI identification for the confirmed bypass cases identified by the integrated solution is possible from a single location with minimal efforts

Integrated Actioning

Automatic provisioning (suspensions/deactivations) actions can be initiated through FMS, if required, for confirmed fraud cases identified by both TCG and FMS, providing a single integrated platform for the whole workflow

Quantifying Benefits of FMS + TCG Integration approach

Table 1 below provides an example to quantify the coverage, latency and fraud loss avoidance benefits provided by the FMS+TCG integrated solution against Bypass Fraud over the FMS or TCG only approach:

GENERAL BYPASS FRAUD SITUATION ASSUMPTIONS				
Total Bypass rackets in the network: 10 **Associated connections per racket are assumed to be:** 100 **Call Volumes** With an average of 3 minutes per call and a gap of 10 seconds between each call, maximum of approx. 450 calls can be done per MSISDN/day involved in the Bypass Fraud racket. **Loss per minute** 0.1 $ **Total Bypass Fraud loss** 45000 $				
SOLUTION	**IMPACT**			**IMPACT CRITERIA**
	TOTAL MSISDNs IDENTIFIED	**MINIMUM DETECTION LATENCY**	**FRAUD LOSS AVOIDED**	
Only FMS Based	300/day	12 hrs	approx. 6750 $ (12 hrs lost)	**Hit Ratio:** 30% **Minimum threshold:** 100 outgoing calls **Investigation delay:** 2 hrs **Effectiveness:** Considering a hit ratio of 30%, minimum threshold of 100 outgoing calls and investigation delay of 2 hrs, a minimum of 12 hrs will be taken to 300 fraudulent MSISDNs. **Penetration:** 3 Bypass rackets are penetrated.
Only TCG Based	250/day	0.1 hrs	approx. 11000 $	**Hit Ratio:** 50% **Total test calls per day:** 500 **Disconnection:** Immediate **Effectiveness:** With a hit ratio of 50%, 250 distict MSISDNs are uncovered as fraudulent in 24 hrs without any connection between the MSISDNs. **Penetration:** 5 Bypass rackets penetrated, but the fact remains unknown as there is no connections between the fraudulent MSISDNs identified
TCG + FMS Integration based	**800/day**	**0.1 hrs**	250 TCG cases: approx. 11000 $ Remaining cases identified with a FMS analysis delay of 3 hrs: approx. 22000 $ **Total Loss Avoided: approx. 33000 $**	**Hit Ratio: 80%** **Disconnection of confirmed TCG cases:** Immediate **Analysis and Investigation delay over cases forwarded to FMS:** 2-3 hrs **Effectiveness:** With all the confirmed fraud cases identified by TCG and FMS being used in FMS to uncover the whole racket, the effective hit rate reaches 80% with around 800 fraudulent MSISDNs uncovered. **Penetration:** 8 Bypass rackets penetrated. Penetration of the integrated solution increases with the increase in hit ratio of either TCG and FMS

About Subex

Subex Limited is a leading global provider of Business Support Systems (BSS) that empowers communications service providers (CSPs) to achieve competitive advantage through Business Optimization - thereby enabling them to improve their operational efficiency to deliver enhanced service experiences to subscribers.

The company pioneered the concept of a Revenue Operations Center (ROC®) – a centralized approach that sustains profitable growth and financial health through coordinated operational control. Subex's product portfolio powers the ROC and its best-in-class solutions such as revenue assurance, fraud management, credit risk management, cost management, route optimization, data integrity management and interconnect / inter-party settlement.

Subex also offers a scalable Managed Services program and has been the market leader in Business optimization for four consecutive years according to Analysys Mason (2007, 2008, 2009 & 2010). Business optimisation includes fraud, revenue assurance, analytics, cost management and credit risk management. Subex has been awarded the Global Telecoms Business Innovation Award 2011 along with Swisscom for the industry's first successful Risk Reward Sharing model for Fraud Management.

Subex's customers include 16 of top 20 wireless operators worldwide* and 26 of the world's 50 biggest# telecommunications service providers. The company has more than 300 installations across 70 countries.

*RCR Wireless list, 2010
#Forbes' Global 2000 list, 2010

subex
powering the ROC

www.subex.com

Subex Limited

Adarsh Tech Park,
Devarabisanahalli,
Outer Ring Road,
Bangalore - 560037
India

Phone: +91 80 6659 8700
Fax: +91 80 6696 3333

Subex Inc.

12101 Airport Way,
Suite 300 Broomfi eld,
Colorado 80021
USA

Phone: +1 303 301 6200
Fax: +1 303 301 6201

Subex (UK) Limited

3rd Floor, Finsbury Tower,
103-105 Bunhill Row,
London, EC1Y 8LZ
UK

Phone: +44 20 7826 5420
Fax: +44 20 7826 5437

Subex (Asia Pacific) Pte. Limited

175A, Bencoolen Street,
#08-03 Burlington Square,
Singapore 189650

Phone: +65 6338 1218
Fax: +65 6338 1216

Regional offices: Dubai | Ipswich | Sydney