Telecom Fraud
Introduction, Types, and Solutions

This whitepaper addresses the most common types of telecom fraud impacting network service providers today and incorporates discussion on different fraud types, ways telecom pirates elude detection, and essential techniques to detect these fraudulent activities. It also focuses on the impact of fraudulent activities on consumers, operators, and regulators. Recognizing and thus effectively eliminating such events is key to safeguarding revenue generation to network operators.
I. Introduction

In recent years, there has been a substantial rise in the development of ubiquitous cellular network technologies, with many of these new developments helping to fuel a revolution in the telecommunication industry. Unfortunately, however, this phenomenal growth has brought with it, an increase in variety and complexity of fraudulent activities on mobile networks. Interconnect Bypass Fraud and International Revenue Sharing Fraud (IRSF) are considered the most relentless and threatening frauds today and both continue to challenge telecom operators and cause gigantic revenue losses per annum.

Depending on individual or organizational setup, the primary goal of the typical telecom pirate is to make sure that legal calls are directly or indirectly routed through Subscriber Identity Module (SIM) Box operators or fraudulent SIM boxes. SIM Box operators utilize the significant benefit of their premeditated positioning by injecting fraudulent traffic towards the cellular operator network by illegally terminating calls without the permission of the home operator.

This paper shines light on the dominant types of telecom frauds, the source of their existence, different methodologies and tools telecom pirates use to elude detection, as well as the methods necessary to detect and eliminate telecom frauds.

II. Telecom Fraud

Within the telecommunications industry, fraud is an ever-increasing and most prolific threat. Telecom fraud has become more pervasive and sophisticated as additional means of communication have been introduced, while the implementation of these modern forms of communication has promised greater revenue. Within the telecommunication industry, the exponentially growing issue of fraud has become an encumbrance for network operators. It has created severe international problems for GSM and PSTN service providers and its annual impact has been observed to be billions of US dollars.

Fraud can be defined as ‘theft by deception’ while telecom fraud most often refers to the illegal use of network operator resources without paying the service provider. Fraud is an unceasing risk to network operators’ revenue and it remains difficult to predict exactly how, when, or where new fraud settings will attempt to attack services.

III. Factors Leading to Telecom Fraud

Provided are the factors which lead to telecom fraud:

- Failure to understand the complexity of new technologies
- Dissatisfaction of employees due to a lack of experience with new technology
- Weaknesses in operation systems
- Irresponsible business models
- Criminal greed
✓ Money laundering
✓ Political and ideological factors
✓ Ineffective audit systems; a lack of follow up relating to compliance reports presents opportunities for telecom pirates
✓ Free financial Gain

IV. Types of Telecom Network Fraud

Telecommunication fraud encompasses a variety of illegal activities. There are types of frauds, which adversely affect the carrier providers, not only financially but also in terms of extensive voice bandwidth and network resources. These may include roaming, premium service (phishing), and subscription frauds.

Provided are the most prevalent types of network frauds. All of these have been discussed in this paper and all have equal negative influence on operators, regulators, and customers.

- Interconnect Bypass Fraud
- International Revenue Sharing Fraud (IRSF)
- False Answer Fraud
- “A” Number Pass-through / Interconnect Agreement Compliance Testing

A. Bypass Fraud

Bypass Fraud has plagued the performance of network providers to a substantial degree and is the most damaging and costly type of fraud. This fraud type is also known as ‘Grey Routing’ or SIM Box Operator Fraud. Bypass fraud is the exploitation of immobile to mobile gateway equipment, typically termed as SIM boxes, to hijack inbound international calls while transferring them over Voice over Internet Protocol (VoIP) to the mobile network. As a result, it re-injects the call back to the mobile network, thus terminating as a local call at the destination. In this manner, the carrier operators lose their call termination charges.

Existence of Bypass Fraud

In a particular region or country, SIM Box operator fraud occurs when international termination charges become larger than the local mobile call charges. The fraudulent service provider ensures earning by proposing low-cost rates for international voice calls to other operators. The telecom pirates take advantage of the local call rates in that the rates, which should be charged by the local carrier operator at high international rates, are instead charged at local call rates. As a result, calls are produced at the user end with either a Calling Line Identity (CLI) manipulation number or with no CLI. Mostly, SIM Box operators use pre-paid SIMs to perform these illegitimate acts because the ownership and address of a pre-paid SIM is difficult to know.

Types

On-Net Bypass Fraud

On-Net Bypass Fraud is a type of bypass fraud in which the fraud commiters use their own network connections to terminate the bypassed calls. The purpose of these on-net calls is therefore to provide the
lowest national calling rates. For this reason, contemporary bypass equipment such as GSM gateway SIM boxes are employed to examine the terminating party numbers and re-initiate calls only from those connections which fit in the home operator’s network as the terminating party. For on-net termination of calls, the revenue loss per call is directly related to the difference between the international interconnect termination fee and the retail price of the on-net call.

**Off-Net Bypass Fraud**

Off-Net Bypass Fraud is a type of bypass fraud in which the fraud commiters utilize the connections of competitors or any other means for termination. In some countries, the off-net call rates are equivalent to the on-net call rates. In these regions, national calls can be initiated from numbers belonging to other networks in order to commit the bypass fraud. For off-net terminating calls, the revenue loss per call is directly related to the difference between the international interconnect termination rate and the local interconnect termination rate of the off-net calls.

**Hardware Used to Facilitate Bypass Fraud**

Telecom pirates use various methodologies to commit bypass fraud. They utilize SIM boxes, VoIP Gateways, and Session Internet Protocol devices to conduct bypass fraud respectively.

**SIM Box**

A SIM box is a device that holds a large number of SIM cards, which are linked to a gateway but stored separately from it. Therefore, SIM boxes are used as part of a VoIP gateway installation. A SIM box comprises SIM cards of distinctive network operators, thereby allowing it to function with several GSM gateways situated at
TELECOM FRAUD - INTRODUCTION, TYPES & SOLUTIONS

distant locations. The function of the SIM box is to make and terminate calls.

**VolIP Gateways**

VolIP Gateways are telecommunication devices through which calls from fixed or mobile telephone networks are routed directly over VoIP to the targeted GSM network. A modern GSM VoIP gateway installation can support hundreds of mobile SIM cards, functional SIM rotation, pre-paid recharging and off-site SIM card storing.

**Session Internet Protocol Devices**

Session Internet Protocol devices are used to enable VoIP. They are employed to connect a cellular network directly to an Internet Telephony Service Provider (ITSP). This permits VoIP to function as well as other real-time media such as voice, video, and web conference without the requirement of any IP-PSTN Gateway or Digital gateway.

**Working of Hardware**

The SIM Box operator usually bypasses the call routing by buying large numbers of Subscriber Identity Module (SIM) cards; then installing these into ordinary hardware to link to the cellular network, hence making it function like a SIM box. At the next step, the fraudulent service provider routes a call by means of VoIP to the GSM SIM box in the recipient region so that the delivered call can be terminated as local. As a consequence, the original carrier operators are deprived of their right to receive call termination charges.

**Ways Telecom pirates Attempt to Avoid Detection**

Detection avoiding schemes may become troublesome for telecom pirates as they often demand large investments. There are a number of ways that telecom pirates use to intercept phone calls and texts. Some of these are explained below:

**Bit Stuffing of False CLI**

Telecom pirates use different methodologies to manipulate the caller ID. Within telecommunications, bit stuffing is the insertion of non-information bits. Therefore, if a number is dialed showing the country code, the telecom pirate can manipulate that number by adding or deleting digits from it. As a consequence, the called party cannot recognize the actual number.

**Deletion of CLI**

CLI Deletion is another type of telecom fraud in which telecom pirates remove the CLI of the incoming call. In this way, the telephone number of the originating party will not be shown on the Caller ID Box. Accordingly, the immediate affected parties are: the operators, end users, and regulators.

**Emulating Traffic Stats and Usage Patterns (Rotating of SIMs)**

Today, telecom pirates use human behavioral software tools and traffic patterns, which allow the SIM box operator to emulate the behavior of network subscribers. On the basis of this, they can determine which calls are coming from real subscribers and which are coming from test
call generation systems. Telecom pirates use new technological innovations like SIM servers to have control of SIM boxes sitting anywhere around the world. To avoid detection, they tend to virtualize SIM cards so that SIMs can be assigned to modems and rotated between calls. By doing this, the traffic volume, which is dependent on any one SIM card, is abridged to the extent where it falls off the usage pattern analysis radar.

**Emulating Traffic Usage Patterns**

Telecom pirates can change their SIM box operator destination in places where their SIM cards can influence multiple cell sites. Another method telecom pirates utilize is the delivery of artificial SMS messages or the acceptance of a few incoming calls. For this reason, moving vehicles can be used to make their broadband connections.

**Cloning of SIMs, IMSIs, and IMEAs**

In this scenario, the telecom pirate clones (copying the identity of one mobile to the other) an existing SIM card. Commercially available software is used to clone SIMs, IMSIs (International Mobile Subscriber Identity), and IMEIs (International Mobile Equipment Identity) associated with the mobile subscriber network type, number, and mobile handset. They may use physical means to clone SIM cards with the help of a
PC and a card reader. In this manner, the subscribers receive a frequent number of wrong calls, experience difficulty in placing outgoing calls and retrieving voice mail messages, while incoming calls constantly receive busy signals or increased billings.

### B. International Revenue Sharing Fraud (IRSF)

International Revenue Sharing Fraud (IRSF) is one of the most persistent types of fraud within the telecom industry. In the case of IRSF, telecom pirates often utilize illegal resources to gain access to an operator’s network in order to bring traffic to phone numbers obtained from an International Premium Rate Number provider. This devious activity boosts subscribers and draws them to use attractive services offered by calling a telephone line. This results in substantial charges to the caller.

**Existence of IRSF**

IRSF is challenging to eliminate due to the complexity of the mobile network system and the involvement of multiple operators. It encompasses organized groups using illegally obtained connections to bring a large volume of calls into high cost 'revenue
share’ service numbers while capitalizing on the roaming ability of SIM cards. It often requires 24 to 36 hours for those call records to return to the home network.

Thus, the telecom pirates are given the opportunity to dial as many IRSF numbers as they can before the home network becomes aware of the traffic and initiates termination of the SIM card. An International Revenue Sharing Fraud scenario is provided below.

**Types**

**Premium Rate Traffic Stuffing**

Premium Rate Number Service Fraud occurs when fraudulent telephone calls are placed to phone numbers with premium rates (higher than normal national call rates). This fraud takes place when the organized groups or companies coordinate with the content service provider in sending inflated volumes of traffic to the aforementioned premium numbers. Normal subscribers can also fall prey to premium rate fraud unknowingly. In this case, they require certain content, which is extracted from premium rate number content providers. However, in several cases, the content provider may belong to the same group to which telecom pirates are, thus generating a greater number of calls to those illegitimate content premium number services. These numbers are deliberately available and for this reason encourages the international premium number aggregators to hire persons to bring larger call traffic.

**SIM Chip Theft and Call Generation**

Telecom pirates can commit IRSF fraud by procuring SIMs from stolen phones and utilizing them to call international revenue share (IRS) numbers either in roaming or international areas. Again, the call records will reach the home network in 24 to 36 hours, leaving ample time for telecom pirates to make as many calls as possible, thus maximizing monetary gains.

**“Free” Conference Call Services**

Today, telecom pirates implement access stimulation (also known as traffic pumping) in order to intensify traffic by illegal means. This occurs when a local carrier with a high access charge comes into an agreement with another service providing company delivering high volume operations, such as “free” conference calls, etc. This stimulates massive call traffic into the local carrier’s service provider area. As in the agreement, the local carrier must share a portion of its increased access revenue with the “free” conference call service provider. Again, the terminating party or free service provider will be deprived of its access fee share due to this additional traffic generation.

**Actual Pay-per-Call Fraudulent Services**

In this fraudulent service, normal subscribers become victim unsuspectingly. Sometimes they may want to get information on different services offered by the service providers like entertainment, weather, business, etc. In this way, the fraudulent service providers pervert the services offered by them. The perpetrators ploy customers into dialing pay-per-call services by following directions to expose a ‘personal activation code (PAC)’, which essentially links them to a pay-per-call line.
Therefore, they are forced to pay for this unintentionally. The following diagram represents the working flow of IRSF.

Ways telecom pirates Use to Avoid Detection

With every introduction of new technology, the telecom pirates are equipping themselves to avoid the new obstacles that come in their way. For example, the introduction of the smart phone has allowed them to avoid detection from fraud management systems.
Because they can exploit the conference call capacity installed in the smart phone they can generate six calls simultaneously. Additionally, telecom pirates are now making use of access stimulation or traffic pumping schemes to avoid detection.

C. False Answer Fraud

False Answer Supervision (FAS) fraud is a type of telecom fraud in which subscribers are charged by a fraudulent service provider for non-conversational time.

Existence of FAS

FAS fraud occurs when telecom pirates falsely identify themselves as legitimate carriers and instead of terminating calls, they deliver a false answer message (e.g., “the number you are calling is not reachable at the moment, please call back later”) to the real carrier network. In this manner, the subscribers are deceptively charged for completed calls.

Types

False Answer Supervision is comprised of two types of frauds. Both occur when the carrier in question initiates the answer message before the called party has answered.

Early Answer

Early answer FAS is a fraud in which billing begins when ringing begins, thereby increasing the apparent call duration, and cost. In some cases, the customer is charged even if the call ends with no answer.

Recorded Message

In this type, the fraudulent carrier diverts the call to a previously recorded message, which begins with a ringtone, and is followed by a recording that imitates an answer and conversation. The intent is to keep the caller on the line and thus forcing them to pay for the call as long as possible. This is a significant problem as the caller is never able to communicate with the desired person and is charged for wasted call time.

Ways Telecom pirates Use to Avoid Detection

Telecom pirates have developed effective tactics such as the utilization of traffic patterns and the answering of a proportion of calls. This allows them to change their destination and activities with respect to time. Therefore, they avoid debunking from FAS fraud indicators (such as short phone calls of duration 5-10 sec etc.).

D. “A” Number Pass-through /Interconnect Agreement Compliance Testing

In this type of fraud, the fraudulent service providers illegally make use of routing and special discounted termination rates as per an agreement with local carrier operators. The telecom pirate, through SIM boxes or switches, terminates traffic onto mobile operators using their locally installed SIMs so that it appears to be a local call. They can change the “‘A” number’ (which identifies the originator of the event) for each call into a fake local number and then terminate onto the national trunks of mobile operators instead of international trunks.
V. Methods Used to Detect Fraud

Operators and regulators have devised several fraud detection schemes for generated revenue assurance.

A. TCG - Test Call Generation

What’s Involved

With the identification of SIM Box fraud recognition, test call generation has proven to be an effective method for pinpointing grey routes and fraudulent numbers. The primary goal in generating test calls is to identify grey calls in a specific network where found in excess. Calls are then initiated to those numbers from various countries; by means of different interconnect voice routes worldwide. With this procedure, the grey routes origination and the paths followed to reach the SIM Boxes in the home country are realized.

TCG is a probabilistic method in which the number of fraudulent SIM Boxes identified increases as more calls using more routes are generated. The routes identified with a higher volume of SIM Box terminations are then further communicated to operators for action. This technique has been successful; however, telecom pirates have discovered new ways to elude detection.

Hardware and Software Needed

Different hardware components are utilized to generate test calls for both fixed line telephone and GSM/CDMA networks.

Network Hardware Testing Units - Generally contains a number of SIMs or calling cards to identify the type of network. Either it is a 2G/3G network or a fixed line telephone network.

System Software Needed - Generally contains;

- Base Controller Unit to execute automated calls
- Customer Data Record (CDR) report importer, detailing the type of fraud for reported numbers to the corresponding operator CDRs
- Supporting algorithms for generation of different CDR formats according to operator CDRs
- Integrated system for the evaluation of CDR independently.

Global Presence

Test Call Systems exist globally, which keep check on the billing records of the subscriber’s service usage within the operational network. These services are entirely programmed and under the regulation of the groups who corroborate the billing process and measure the quality of service. Although these methods are relatively new to network operators, an understanding of these methods is the key to managing revenue assurance.

Telecom pirates are constantly working towards understanding and utilizing technological advancements, therefore, TCG’s weaknesses are not unknown to them. They are analyzing the test calls regularly to determine which calls are coming from real subscribers and
blacklisting those numbers that are coming from test call generation systems.

**B. CDR Analysis and Analytics**

**What’s Involved**

Call detail records take account of necessary information relating to the important characteristics of each call. CDRs are used to identify fraudulent activity through extensive analysis while performing analytics on fraud indicators by comparing different fields of the CDR such as time, duration, mobile originating and terminating numbers and country codes, call type, IMEI, IMSI, LAC-CID (Location Area Code-Calling Line Identity), account age and customer segment. In SIM box detection, the Fraud Management System (FMS) uses CDRs to create user-based profiling that distinguish between fraudulent SIMs installed in SIM boxes and legitimate subscriber SIMs.

The current systems of fraud identification include extensive CDR analysis by comparing the function field relating to the corresponding application. With differential analysis, user behavior patterns are examined by comparing the most recent activities to the historic activities of the user. As a result if there are anomalies in the user calling pattern, the activity is then estimated and timely reports are generated. This ensures that the billing and subscriber records are reconciled.

**Hardware and Software Needed**

Hardware components and software is essentially required for CDR analysis. All customer call data is recorded on to a local hard disk drive at the end of the call, which contains various fields stored in a text file format. This information is analyzed further using pattern analyzers and the essential data is loaded into the fraud detection framework of the operator for required action.

**C. Hardware Probes Installed in the Networks and Related Services Such as DPI**

With the rapid transition of the telecom industry towards more data consumption and IP services, telecom pirates have switched their vehicles of action and are now looking for opportunities towards IP data related fraud. Tethering is the illegal connection of multiple devices using a single internet access point. This negatively affects operator planning and causes overloads by forcing operators to expend more on the service. One of the dominant methods for detecting IP based fraud is to use unconventional data sources such as Deep Packet Inspection (DPI). Instead of analyzing headers or volumes of traffic, DPI analyzes the contents of data traffic and network protocols from layer 2 to layer 7 of the OSI model and identifies abnormal activity. In the case of illegal mobile access, abusers try to invade restrictions and deprive operators from charging premium rates for bundled data services. With the help of DPI we can eliminate the abuse of proxy servers that mask the user’s original IP address. This will encourage operators to make deals with over the top (OTT) services providers to boost data consumption.
VI. Who Benefits from Fraud Detection and Elimination?

Telecom fraud is a multifaceted and complex issue, which is affecting consumers, operators, and governments in a number of ways. Timely efforts to detect and eliminate frauds are thus, a boon to mobile operators.

A. Consumers
   
   **Quality**

   The congestion of traffic caused by bypassing the call would increase call failure rates and poor quality of service, which could seriously impact the public image of mobile operators. Effective detection and elimination of fraud ensures improved quality of service to consumers.

   **Safety**

   Consumers will feel secure moving around their desired networks. In this way, consumers will experience legal calls with no interference of eavesdroppers, denial of service (DoS) attackers, caller ID theft, or SIM cloning through authorized GSM gateways during short and long distance call services.

B. Operators

   **Revenue Generation**

   By underpinning the detection and elimination techniques, revenue can be recovered effectively. The different techniques involved would make sure that the mobile operator’s bandwidth resources are not being used fraudulently, thus enabling subscribers to fully utilize the delivered services via legally allocated routes.

   **Stop Losing Revenues**

   Every form of fraud causes undesirable effects such as the inaccessibility of popular services such as voice mailbox, CLI, etc. Because of the re-routing of calls, a manipulated CLI or no CLI is presented at the receiver’s end with the instant effect being an inability to “call back”, which results in a loss of revenue. Revenues are then collected by the fraud committers and the networks are left with unpaid invoices and settlements of roaming charges. Intelligent revenue assurance techniques must be implemented to stop the loss of revenues.

   **Branding and Image Maintenance**

   Consumer insights are the mainstream reflection of any service provider business. Customers rather associate such fraudulent activities with the service operator brand. Therefore, unnecessary billings and the absence of desired services can affect branding and image maintenance. Not just the present service but other services or products may be affected as well. However, the quicker the fraud is detected, the more likely the desired services can be provided to the consumer.

   **Quality of Calls**

   The number of incoming calls made by perpetrators is often greater than the number of outgoing calls. The network may become congested due to a large number of calls being sent using VoIP routes. As a consequence, the call failure rate increases
and thus overall quality of calls degrades. By effectively recognizing and eliminating these grey routes, poor quality calls can be mitigated and the quality of calls can be restored by re-routing these calls using original GSM gateways.

**Improved Relationship Management**

To gain a competitive advantage, detection of abusive activities is necessary. The operators, who have a comparatively better understanding of detection techniques, have the edge in improving customer relations. In fact, such carriers have effective solutions, which enable them to respond as quickly as possible. This will focus them towards future marketing and sales campaigns. The operators can improve relationship management, reduce customer churn, and more efficiently acquire and retain customers through improved service quality.

**C. Governments - (Regulators and Ministries)**

**Safety Support**

If a system is plagued with a specific and persistent type of fraud, regulators or stakeholders (ministers) will be hesitant to invest due to a fear of loss. Implementing fraud detection and elimination techniques better enable stakeholders to incur the required investments in network financial services.

**Revenue Management**

Without doubt, non-standardized policies devised by the regulators may expose the mobile network in becoming vulnerable to fraudulent activities. A well-structured detection and elimination system will allow regulators to manage revenue effectively without compromise in regards to customer protection. In this way, better detection will help mobile financial services recover revenues from committed frauds.

**Proper Fees and Taxation Compliance**

With the implementation of a fraud detection and management system, the non-taxpayers who are deceiving the policies enforced by the regulators can be identified. Therefore, revenues can be incurred by regularly peer reviewing compliance statements, thereby mitigating fraud.

**Conclusion**

It is evident that the volume and versatility of new network technologies have created many opportunities for telecom pirates and in order to combat the telecom pirates. Telecom operators must stay one step ahead. There is an immense need to boost research awareness, and devise prudent fraud management systems to detect such frauds, which impose irreplaceable harm to the telecom industry.