Fraud Classification Guide

GB954

Version 2.2

March, 2013

Notice

Direct inquiries to the TM Forum office:

240 Headquarters Plaza,
East Tower – 10th Floor,
Morristown, NJ 07960 USA
Tel No. +1 973 944 5100
Fax No. +1 973 944 5110
TM Forum Web Page: www.tmforum.org

Table of Contents

List of Figures

List of Tables

Introduction

This classification guide is developed as a periodically growing resource to arm operators with fraud type information and offer them a best practice for a common fraud cases classification model. It is structured to support Fraud Operations activities associated with the TM Forum Business Frameworx model. This guide is intended to capture multi-technology fraud types, allowing carriers to access known fraud information for all technologies in Telecommunications from one resource. Questions, comments, and additional recommendations for fraud information to be added to this document should be forwarded to the Fraud Team Leader via the TM Forum website (Business Assurance Program >> Fraud Team),

Information contained within this guide is to be used for general and introductory purposes of understanding and identifying prevalent fraud types within the industry today. Certain types within this guide may also identify further, more detailed, reference information that the TM Forum recommends should be examined to better understand that specific fraud type.

Telecom Fraud Classification Model

Due to the constantly changing nature of Fraud, it is vital to accurately characterize and measure fraudulent events to help understand how Fraud is evolving and how effective the Fraud Management process is in tackling it. Therefore, it is clear there is a need to correctly classify and record each occurrence. However, the problem lies in the complexity of Fraud events. Usually an event includes more than one Fraud type. Also, to ensure an effective and efficient Fraud Management process, it is important to understand the context in which Fraud is committed to take the right corrective and preventive measures.

Another aspect of Fraud Management is the importance of information interchange and benchmarking, particularly in sharing Fraud Occurrences and mitigation practices with other operators and industry organizations. By providing this global response to Fraud, a fraudster's financial gains can be minimized when trying to replicate Fraud with other operators. This enables operators to take corrective and preventive measures at an industry level. However, to ensure efficient communication, it is important that there is a common and effective way of classifying the Fraud events. This way, it will be possible to avoid ambiguous situations, lack of information and, worst of all, double counting.

To better illustrate the current situation, it is common to see statistics of Telecom Fraud where both Subscription Fraud and IRSF are in the TOP 5 reported fraud types, either in quantity or value. The question that arises immediately is how much of this subscription fraud is made to commit IRSF? And consequently, are these statistics reliable? Are we not facing double counting of Fraud? Financial impact is rarely directly related with subscription fraud. It can be related with usage without intention to pay, equipment theft, misappropriation and many other Frauds. However, in order to take the right actions and preventive measures, it is essential to know that subscription fraud is one of the top ways of accessing services or goods.

The Model

From the previous example, it is obvious that is not possible to classify Fraud in a one-dimensional way. It is clear that we should at least keep track of the enabler technique (how the Fraudster gets access to the services or goods), and the main fraud types from which fraudsters benefit. Social engineering, Hacking, and Malware are other typical examples of enabler techniques used to perpetrate Fraud.

These two dimensions form the basis of the classification model proposed in this document, but we still need to ensure that the model can capture the context in which the Fraud was committed. Therefore, we need a set of attributes to describe this context, namely the ones needed to classify the operator who suffered Fraud, the impact of the Fraud, etc.

Looking at the two main dimensions in more detail, Enabler Technique and Fraud Type, and having in mind the need of capturing the information to properly give the context in which the Fraud was committed, it is easy to demonstrate that a set of attributes associated with these dimensions are also needed. Let's take as an example IRSF or Call Resell; it is obvious that a proper classification model should be able to collect auxiliary information like the country where the PRS numbers are located or to where calls are being resold.

Finally, for the purpose of ensuring the best practice of recording and sharing the proper mitigation strategies, together with the classification model, the proposed information system should include a section where the relevant mitigation strategy for the classified fraud is described.

Figure 1 summarizes the proposed Classification Model. This is a first version proposal that ideally will be used as a basis for a broader discussion and tested by a larger base of CSPs. Suggestions for improving this model should be sent via the forum. If appropriate, these suggestions will be included in the document's next release. Some cases may not be straightforward to classify and questions may arise, but the conclusions obtained by statistically analyzing separately enablers from Fraud Types in real cases covered during the short testing period are extremely interesting. It is also clear that further tests are needed to consolidate and enrich the model.

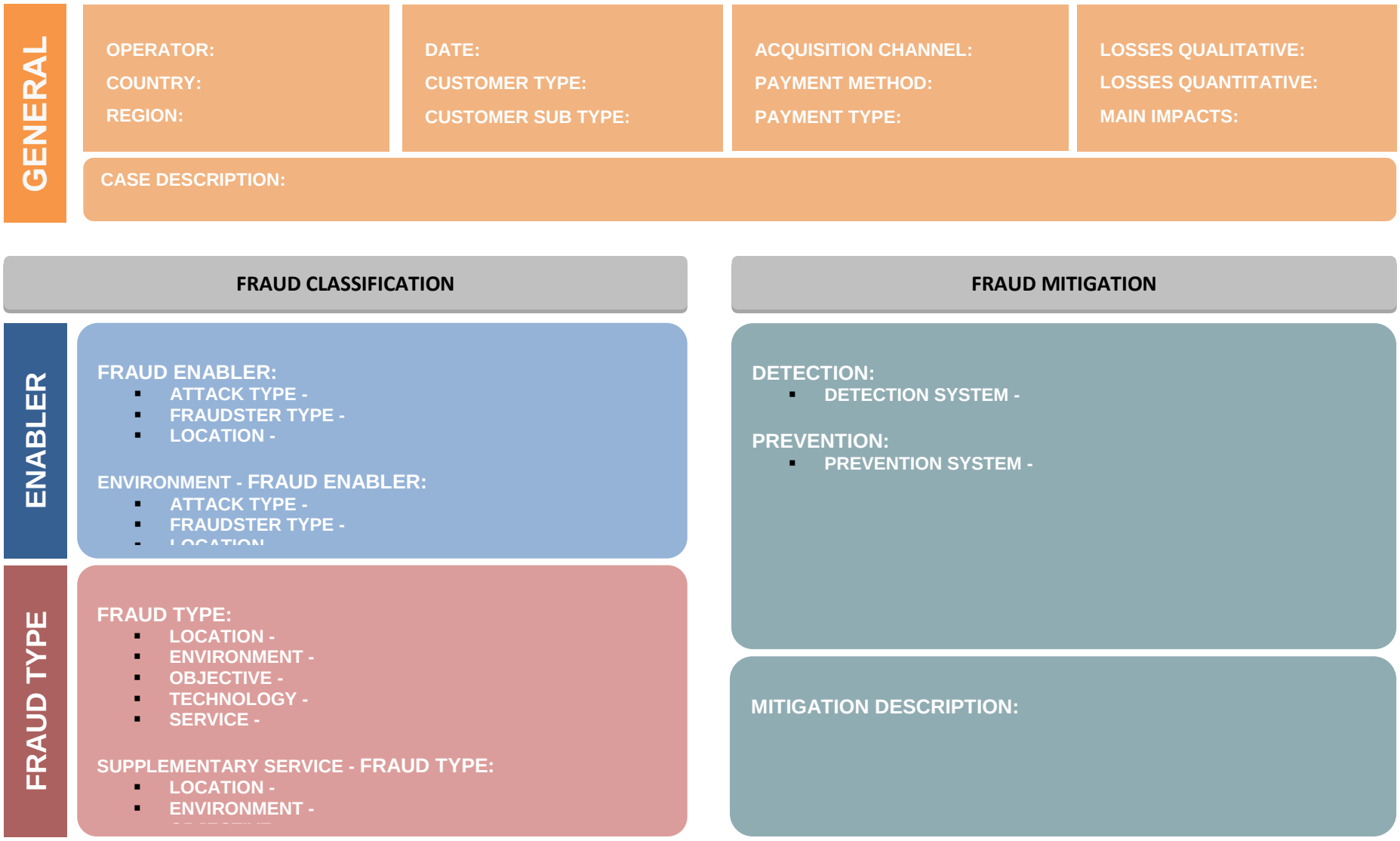

Figure 1: Fraud Classification Model

Classification dimensions and attributes

Classification Section: General Data

This section's goal is to collect the relevant information about the Fraud Event, namely the operator who suffered Fraud, and if possible to associate the fraud event to a specific customer account, information related with the customer, the acquisition channel, payment type and method. We should also register data here about the Fraud event's impact.

Figure 2: Fraud Classification Section: General

Classification Section: Fraud Enablers

This section's goal lists examples of Fraud enablers and Fraud enabler dimension attributes. Fraud enabler is the method or technique of getting access to the goods or service and perpetrating the Fraud. A Fraud Enabler can be an illegal action by itself. It is possible to have one or a combination of a set of Fraud enablers for a specific Fraud type. For example, for Fraud Type *IRSF*, the Fraud Enablers can be Fraud Subscription, PBX Hacking, etc. Also One Fraud Enabler can be applied for more than one Type of Fraud. For example Fraud Enabler Subscription Fraud can be a technique for IRSF, SIM Box, Reselling Calls, Equipment, etc.

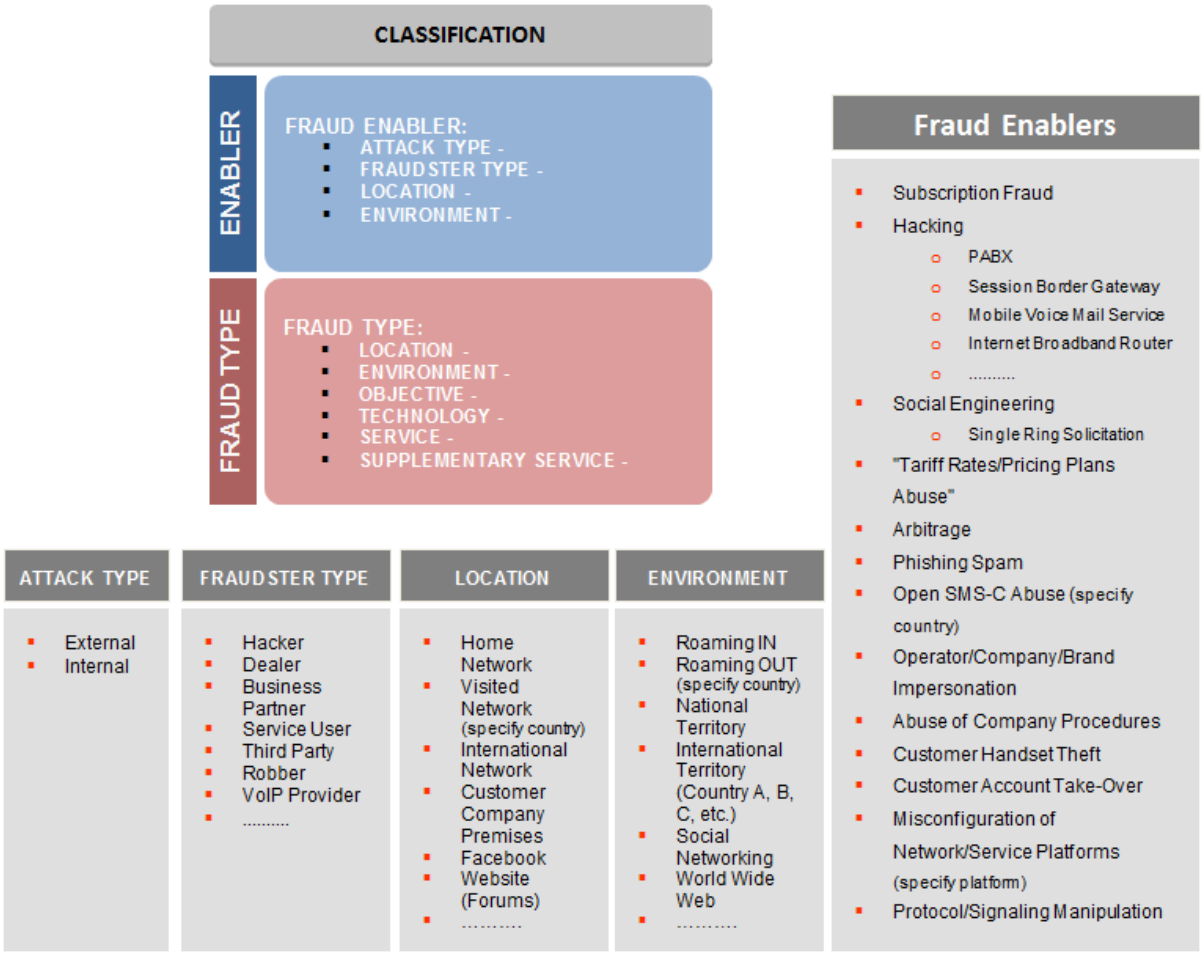

Figure 3: Fraud Classification Section: Fraud Enablers

Classification Section: Fraud Types

This section's goal is to list examples of Fraud Types and Fraud Type dimension attributes. The Fraud Type is the Fraud committed to get the illegal benefit.

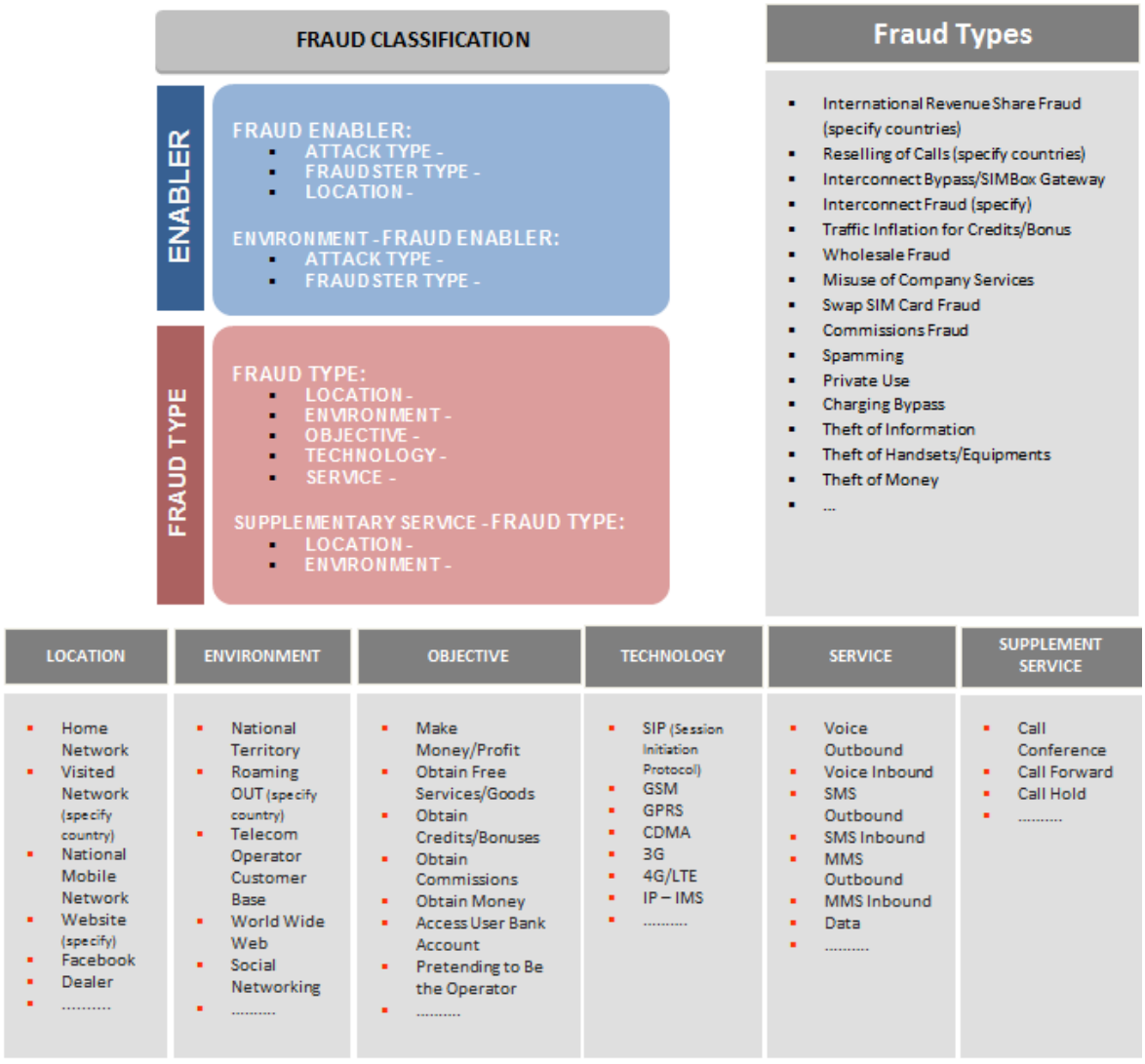

Figure 4: Fraud Classification Section: Fraud Types

Classification Section: Fraud Mitigation

This section's goal is to list the set of attributes and examples that describe the detection procedure used to detect the Fraud Event, the mitigation strategy and the preventative measures taken or advised.

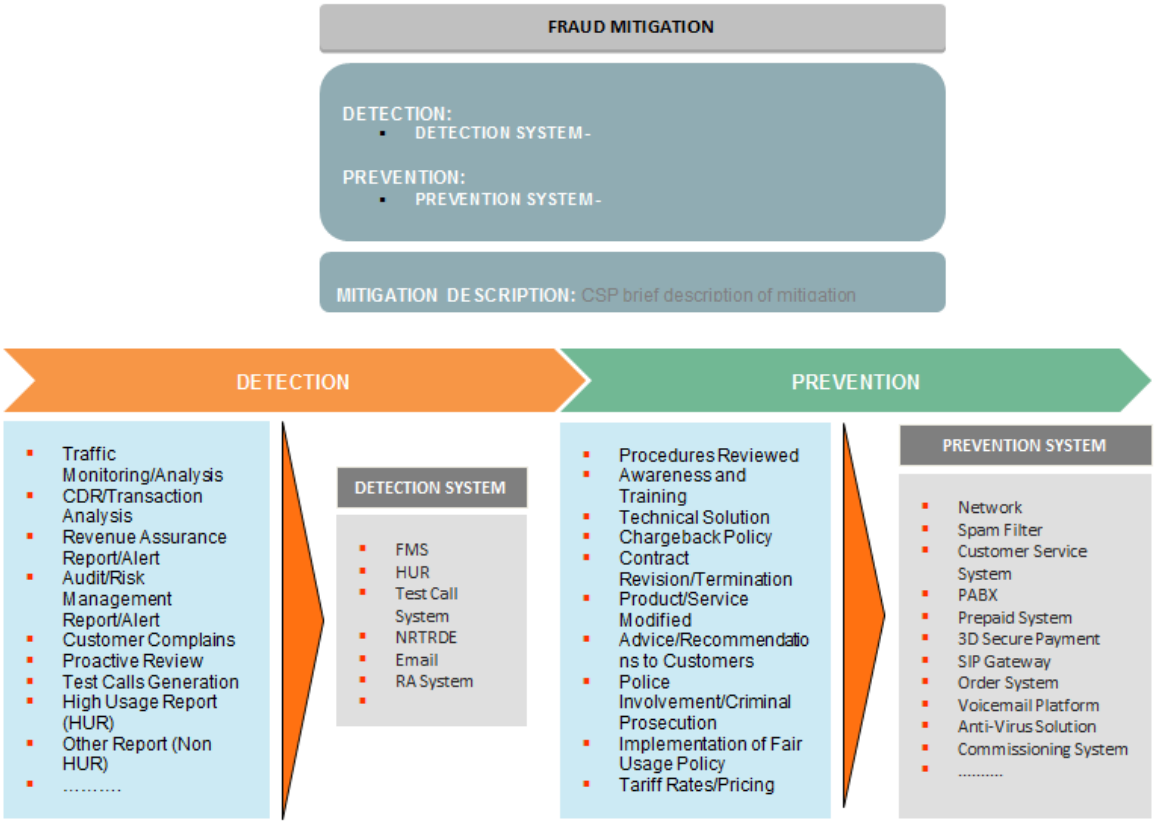

Figure 5: Fraud Classification Section: Fraud Mitigation

Classification Model: Future Work

As Fraud is a constantly changing threat, it is essential that the Classification Model is revised periodically to ensure that is fulfills its goals. It is important that a common Classification Model is widely adopted to ensure comparability of statistics and benchmarks, but also to ensure that all relevant information is collected in a common format for distribution, and to maximize the benefits of information sharing between CSPs.

Despite the fact that the model has been tested with hundreds of cases, this is the initial version and needs to be used and improved (as mentioned at the beginning of this chapter), either by using a better naming convention or enriching or correcting any of the existing information. Therefore, it is important for all users of this model to give suggestions through the TMF Fraud Team forum for them to be incorporated in future versions of the document.

Based on the suggestions kindly made by Herbert Galiano, Ericsson, in the next revisions the following points, transcribed from the feedback received, should be discussed and addressed after validation:

1. To revise naming conventions between Fraud Classification Model section and the Telecom Frauds description to ensure coherence throughout the document.
2. “In the Telecom Frauds description, there are some concepts that Telecom Fraud Community are not familiar, or are not part of day by day activities. For example. Page 20. Misappropriation of Assets - Lapping, False Invoice, Long Firm, Inventory Fraud, also pages 20 to 24 related to Financial Frauds. What we observed is today in the market neither consultants, vendors and CSP teams addressed solutions for those types of fraud. (Maybe this belongs to other areas in CSPs like Auditors, Corporate Security area or Chief Risk Officer). I Suggested that this forum contribute and focus only and exclusive in the traditional and new Fraud Types for the Telecom industry.”
3. On page 9 for the Fraud Classification Model: “Suggest to include the Action or Response as key process of the Fraud Management in Fraud Mitigation box. For example: Automatically. Manual, Semi-Automatic; Actions: Block call origination, block collect calls, disconnect, divert to Call center, etc. are some actions that fraud analyst should be taken immediately after detection to avoid more losses.
4. On Page 9 for the Fraud Classification Model: “Suggest include the 1st Fraud Alarm for detection. For example: FMS, RA System, e-mail HUR, external denounce, etc. This will be very useful for fraud managers to have statistics which systems /tools have a good performance.
5. On page 9 for the Fraud Classification Model: As we have *Quantitative* and *Qualitative* impact we need now the "*time*". Suggest to include the *TimeframeCycle* of the Fraud, since origination to the detection and action taken. For example, 5 days duration, 12 hours, etc.
6. On page 12 for the Fraud Classification box we have the Enabler and Fraud Type, What I suggest is to include a new variable in this model, the “Fraud Technical Method“ as the specific technique or method that fraudsters are using to perpetrate the fraud avoiding detection. For example. An international fraud criminal gang is using intelligent SIM boxes to perpetrate Fraud Bypass avoiding detection by simple FMS rules. Specifically they are using special features that simulate a human behavior for a set of SIMs inserted in the SIM BOX.
7. Example :
   Fraud Enabler: Tariff Rates/Pricing Plans Abuse
   Fraud Technical Method: Human behavior SIM BOX features

Fraud Type: Interconnect Bypass / SIM Box

8. The Fraud Classification Model on page 9 is a good framework to fill by Fraud Operations as describe specific type of fraud that they detected, however I´m not sure that it is very clear for people that will use this document as first time, so I suggest to include 3 examples with real cases (fiction companies)
9. I did not find some other types of fraud enablers/ types that are very common in fixed and TV operators like Clip on Fraud, Pay phone Fraud, Bandwidth selling, False Answer Supervision, Signal Piracy, etc. Also for Payments using fraudulent credit cards.

Telecom Fraud Category Matrix

	Focus: (I) Internal (W) Wholesale (E) Enterprise, (C) Consumer, Other	Fixed Line Telephony	Mobile Telephony	Data Services (Mobile)	Data Services (Broadband DSL and Cable)	Data Services (Enterprise PTP)	Data Services (Hi-Cap and Backhaul)	Video (Cable, Satellite, IP)
Fraud Types								
Subscriber Fraud	C, I	x	x	x	x	x		x
Misappropriation of Assets – Theft	C, I	x	x	x	x	x	x	x
Misappropriation of Assets – Embezzlement	I	x	x	x	x	x	x	x
Misappropriation of Assets – Lapping	I	x	x	x	x	x	x	x
Misappropriation of Assets – False Invoicing	I, Supplier	x	x	x	x	x	x	x
Misappropriation of Assets –Long Firm Fraud	Customer	x	x	x	x	x	x	x
Inventory Fraud	I	x	x	x	x	x	x	x
CNAM Fraud	W	x	x					
Wangiri Call Back Fraud	C		x					
Financial Misreporting – Revenue Falsification	I	x	x	x	x	x	x	x
Financial Misreporting – Expense Capitalization	I	x	x	x	x	x	x	x
Financial Misreporting – Understating Liabilities	I	x	x	x	x	x	x	x
Financial Misreporting –Misallocation of Cash	I	x	x	x	x	x	x	x
Bribery – Cash	I	x	x	x	x	x	x	x
Bribery - Labor	I	x	x	x	x	x	x	x
Bribery – Holiday	I	x	x	x	x	x	x	x
Bribery - Sponsorship	I	x	x	x	x	x	x	x
Bribery – Consultancy Fees	I	x	x	x	x	x	x	x
Bribery – Credit Cards	I	x	x	x	x	x	x	x
Extortion and Blackmail	I,Other	x	x	x	x	x	x	x
Kidnap – Stranger	Other*	x	x	x	x	x	x	x
Kidnap - Political	Other*	x	x	x	x	x	x	x
Kidnap – Tiger	Other*	x	x	x	x	x	x	X
Money Laundering	Other*	x	x	x	x	x	x	x
Insider Dealing	I,W	x	x	x	x	x	x	x

Procurement Fraud	I	x	x	x	x	x	x	x
Payroll Fraud – Ghost Employees	I	x	x	x	x	x	x	x
Payroll Fraud – Payroll Adjustments	I	x	x	x	x	x	x	x
Expense Fraud – False Claims	I	x	x	x	x	x	x	x
Expense Fraud - Undisclosed Credits	I	x	x	x	x	x	x	x
Expense Fraud – Inflated Claims	I	x	x	x	x	x	x	x
Treasury Fraud	I							
Bypass – Tromboning	W	x	x	x	x	x	x	x
Bypass – SIM-Boxes	W	x	x	x				
Bypass – Fixed Cell Terminals	W	x	x					
Bypass – Premicells	W		x					
Bypass - GSM/UMTS Gateways	W	x	x					
Bypass – Landing Fraud	W	x	x					
Bypass – VoIP Bypass	W	x	x					
Bypass – Interconnect Fraud	W	x	x					
Bypass – Toll Bypass	W	x	x	x				
Bypass – Third Country Fraud	W	x	x					
Bypass – Grey Routing	W	x	x					
Bypass – Int'l Simple Resale	W	x	x					
Missing Trader Fraud	Other*	x	x	x	x	x	x	x
Carousel Fraud	Other*	x	x	x	x	x	x	x
Roaming Fraud	C, I		x	x				
Cloning Fraud	C		x	x				
Spamming – Malware	C			x	x	x		x
Spamming – Spoofing	C			x	x	x		x
Spamming – IP/Phishing	C			x	x	x		x
Int'l Revenue Share (IRSF)	W	x	x	x				
PBX Hacking Fraud	W,E,Other	x	x					
IP – Subscription or Identity	C			x	x	x		x
IP – AIT/Click Fraud	W			x	x	x		x
IP – DoS (Denial of Service)	E			x	x	x		x
IP – Content Sharing	E,C			x	x	x		x
IP – Identity Trading	C	x	x	x	x	x		
IP – Spyware	E,C			x	x	x		x
IP – Pharming	E,C			x	x	x		x
IP – Online Brand Threats	E			x	x	x		x
IXC – Arbitrage	W	x	x				x	
IXC – Call Looping	W	x	x				x	
IXC – QoS Exploitation	W	x	x				x	
IXC – Technical Config Fraud	I,W	x	x				x	

SMS – Spoofing	C		x					
SMS – Faking	C, I		x					
SMS - Malware	C		x	x				
SMS – Global Title Scanning	C		x					
SMS – Flooding	C		x					
SMS - Spamming	C		x					
SMS – Open SMSC	C, I		x					
Pre Paid – PIN Theft	I		x	x	x			x
Pre Paid – PIN Guessing	C		x	x	x			x
Pre Paid – Stolen Voucher	I, C		x	x	x			x
Pre Paid – Altering Free Call Lists	I		x	x	x			x
Pre Paid – Manual Recharges	I		x	x	x			x
Pre Paid – Voucher Modification	I, W		x	x	x			x
Pre Paid – Duplicate Voucher Printing	I, W		x	x	x			x
Pre Paid – Fraudulent Voucher Reading	C		x	x	x			x
Pre Paid – Illegal Credit Card use for Recharges	C		x	x	x			x
Pre Paid – IVR Abuse/Hacking	C		x	x	x			x
Pre Paid – IN Flag Modifications	I		x	x	x			x
Pre Paid – Handset Manipulation	C		x	x	x			x
Pre Paid – Handset Installment	C		x	x	x			x
Pre Paid - Roaming	C, E		x	x	x			x

Other*: Related to external type of fraud, most commonly business fraud threats, can affect all kind of organizations

Table 1: Fraud Management by target communications segment

Telecom Fraud Definitions

1. Fraud Identifier: Subscription and/or Identity Theft

Definition

Subscriber fraud occurs when a fraudulent individual/s obtain customer information and uses it for securing service with an intent to avoid payment.

Description

Subscriber fraud involves the fraudulent individual obtaining the customer information required for signing up for telecommunication service with authorization. The usage of the service creates a payment obligation for the customer. It is common for fraudulent individuals to constantly move to avoid being detected. If the fraudulent individual was able to provide the identification credentials required for creating a false alias when opening the service account, it puts the onus on the customers to prove that the service was not used by them.

Subscriber fraud may be conducted in two ways:
- Fraudulent individual creating the account and using the service for their purpose
- An internal employee of the service provider is involved in the fraud

This fraud type is among the most common frauds due to the low technical knowledge required to perform the fraud.

2. Fraud Identifier: Misappropriation of Assets - Theft

Definition

This type of fraud when individual/s theft of service provider/ company assets for personal benefit. The company assets may include cash or non-cash assets (materials, trade secrets, intellectual property).

Description

Misappropriation of assets in the form of theft usually involves internal resources, but may also be committed by external supplier, customers or other entities involved in the industry. Theft may occur before the assets are recorded in the company's financial records (skimming), while the asset is held by the company (misuse of larceny) or during the purchase of the asset.

3. Fraud Identifier: Misappropriation of Assets - Embezzlement

Definition

This type of fraud occurs when fraudulent individuals who have been entrusted with the assets appropriates the asset through dishonest methods.

Description

Embezzlement involves the trusted individual/s converting the assets for their personal benefit. It usually starts with a small proportion of the assets to minimize the risk of detection and can continue for a long period of time (years or decades) without detection. Hence it usually involves systematic and methodical activities that is intended to conceal the fraud. Embezzlement is distinguished from theft from the fact that the fraudulent individual involved is responsible for the asset (while in the case of theft the person is not responsible for the asset). Embezzlement may also involve falsification of records done for the purpose of concealing the activity.

4. Fraud Identifier: Misappropriation of Assets - Lapping

Definition

This fraud occurs when the accounts receivable section of the balance sheet is altered in order to conceal the stolen cash that is intended for payment of a receivable.

Description

Lapping involves a chain of accounting manipulation triggered by act of stealing the cash intended for a payment of a receivable. The first receivable collected is used to cover the theft, while the second receivable is accounted to the first to continue the cover up. This is followed by the next cycle of using the third receivable for the second and so on in order to conceal the initial theft.

5. Fraud Identifier: Misappropriation of Assets – False Invoicing

Definition

This type of fraud occurs when an invoice is generated that does not relate to a real sale of service or product. See also: **Procurement Fraud**

Description

Usually this fraud type is conducted through trick. Additional substantiation may also be provided by the fraudulent entity to legitimize the false invoice produced. Appropriate approval process and procedures are key to detecting false invoicing. Usually this fraud does not involve internal staff.

6. Fraud Identifier: Misappropriation of Assets – Long Firm Fraud

Definition

This fraud type occurs when fraudulent individuals/companies systematically establishes trust and positive credit history with the wholesale or service provider before placing large orders that are fraudulent.

Description

Long firm fraud begins with the fraudulent individuals/ company places lot of small orders and pay them promptly. This environment creates trust between the service provider and the fraudulent entity. Having established a credit history, then the entity places large orders without an intention to pay for the service or the product. The delivery of the product or service is followed by prompt disappearance of the fraudulent entity, which then resells it for unlawful benefit.

7. Fraud Identifier: Inventory Fraud

Definition

This type of fraud occurs when the inventory of the service provider is misappropriated. This is usually sold off or stolen for personal benefit.

Description

Inventory fraud can be committed by manipulating different systems. One common way is to manipulate the inventory records directly. Another way of committing the fraud is to manipulate the sales or inventory depletion records which in turn results in an incorrect inventory record. In addition, the fraud can be performed by manipulating the purchasing records which in turn results in a wrong inventory record.

8. Fraud Identifier: CNAM Dip Fee Fraud

Definition

When terminating carriers are required to “dip” into a line information database, a fee is generated that must be paid by the terminating carrier to the originating carrier. Calls not answered also generate this dip fee revenue, opening a unique opportunity for fraudsters to flood a carrier with call traffic that is canceled before answered.

Description

Every call to a U.S. telephone number that has Caller ID (CID) enabled requires that the terminating phone company perform a lookup in one of several national databases (also known as line information database or LIDB) that contain all the U.S. subscriber names and numbers. This database lookup is called a CNAM (Calling Name) dip. When this

database is being accessed, or 'dipped', the originating phone company gets compensated by the terminating phone company – this is commonly referred to in North America as a CNAM dip fee (or simply, "dip fee"). This compensation happens for every call where the calling party name is displayed to the called party – *even if the call is not answered*. Fraud often results when multiple (potentially thousands or more) calls are sent to a carrier to terminate, yet the call is discontinued before completion – resulting in a "dip" action, and revenue generated to the fraudster.
Similar database repositories exist throughout other regions of the world, serving caller ID compatible technologies.

Other fraud cases are possible with CNAM 3rd party providers. These providers will supply international callers with virtual telephone numbers and then distribute that information to the CNAM databases within the North American market. These organizations then share in the revenue these numbers generate from dip fees while calls are terminated from those lines. This is a legal practice, and fraud occurs when these numbers are misused for call flooding (and non-completion) to generate dip revenues only.

9. Fraud Identifier: "Wangiri" Call Back Fraud

Definition

Wangiri ("One (ring) and cut") fraud is believed to have originated in Japan. Wangiri scams involve a computer using hundreds of connections to call random mobile phone numbers. The numbers show as missed calls on the recipient's handset. A percentage of customers will generally call back to see who called them. The numbers they call back are either premium rate lines with high charges, or they deliver advertising.

Description

In Wangiri Fraud a computer makes calls that automatically hang up after one ring, leaving a notification of a missed call on most mobile handsets. If the target victim returns the call they will most commonly receive a recorded message that will either be charged at a premium rate, and/or it will deliver advertising. In many cases the premium rate is charged as a flat connect fee, as opposed to MOU fee.

10. Fraud Identifier: Financial Misreporting – Revenue Falsification

Definition

This fraud occurs when the financial reporting is manipulated to falsely report revenue earned by the company in order to benefit some individuals in the company.

Description

Revenue falsification usually involves higher management of the company. Some of the most common ways of overstating revenue are sales booked before or without

completion of delivery, sales contingencies not disclosed to the management, false sales documents and agreements, revenue reported at gross than at net. This practice is relatively easier to commit in environments where strict financial reporting standards are not followed.

11. Fraud Identifier: Financial Misreporting – Expense Capitalization

Definition

This fraud involves incorrectly capitalizing expenses in violations of the financial reporting and accounting guidelines in order to incorrectly increase the profits.

Description

Account guidelines allow for companies to purchase large items as assets instead of expenses. By wrongly reporting expenses as assets, it is possible to improve the financial reporting. This technique enables the company to capitalize and amortize the expense over many periods rather than recognize it in its entirety in the current period, thereby falsely improving the performance in the current period.

Any expense capitalization typically requires authorized forms. This fraud may either include such authorized forms not present or incorrectly authorized in terms of the level of authority or the amount or the item not lasting the required period to qualify as an asset. This fraud involves financial and accounting department of the organization.

12. Fraud Identifier: Financial Misreporting – Understating Liabilities

Definition

This fraud occurs when the liabilities of the company is intentionally understated in the financial reports in order to improve the net profit of the company.

Description

This fraud involves misstatement of the financial reports to misguide the investor regarding the performance of the company, specifically the net profit. This fraud is usually found within publicly-traded companies. This fraud involves intentionally reporting reduced liabilities and expenses. This may also involve postponement of reporting of the expenses to subsequent reporting periods.

13. Fraud Identifier: Financial Misreporting – Misallocation of Cash

Definition

This fraud occurs when the cash is intentionally allocated wrongly to incorrect financial codes or ledger parts.

Description

This fraud could be used for wrongly reporting the performance of the company to mislead the shareholders or for subsequent skimming of the cash for personal benefit. In both cases this fraud typically involves the accounting department/ individuals and often the auditors as well.

14. Fraud Identifier: Bribery

Definition

Bribery is a fraud of collusion, involving the offering, giving or receiving of something of value in exchange for giving or gaining undue influence in a decision making process or obtaining another advantage. Both the giver and the receiver of the bribe are committing a fraud as bribery advantages both the briber - who gets an unfair advantage over others. The bribe is the gift bestowed to influence the recipient's conduct. It may be any money, good, right in action, property, preferment, privilege, emolument, object of value, advantage, or merely a promise or undertaking to induce or influence the action, vote, or influence of a person in an official or public capacity.

Description

Bribery involves offering or accepting something of value in a situation where the person who accepts the bribe is expected to perform a service which goes beyond his or her normal job description. It also used to gain an improper advantage over others through the intervention of a corrupt employee. Bribery is the giving of something of value by another party to a decision maker or decision influencer in exchange for influence in a decision making process. There is a grey area between bribery and innocent commercial marketing. Where does an attempt to market to or to build a professional relationship with someone become a bribe? The practical answer is the whether the employer has knowledge of and given approval for the person to receive the benefit offered. Without the knowledge and consent of the employer, the chances are that the receipt of a benefit by an employee can be viewed as a bribe, whether the benefit is being given to directly influence a specific decision or to maintain an overall relationship.

A. Types of Bribery

Most bribery frauds fall into one of two major groups - bid or tender rigging, and kickbacks or secret commissions. These are very similar, just different in ways of achieving the same result.

1. **Kickbacks (Secret Commissions)**
   Kickbacks are payments to the employee from the briber outside his terms of their employment that are usually made for obtaining a favorable decision or influence employer purchasing something from or selling something to the third party. It can be summarized as "You give me this contract and I will give you money or 5% of the profits". Kick-backs are commonly thought of as payments to gain that influence and may be based on a percentage of orders received, or some other basis.

2. **Bid/Tender-Rigging**
   Bid-Rigging is an employee improperly influencing the awarding of a contract through the normal tender process. This is done by giving the third party details of the other tenders received (giving them knowledge of the conditions to beat), and influencing the decision maker towards the briber's tender, even though it is not the most beneficial to the employer. Tender rigging is usually done during a tender process for a contract of supply or the sale of a large asset or for construction contracts, or for long term supply contracts.

   The major difference between kickbacks and tender rigging is the timing and calculation of the payment and the success factor. Neither of these factors may make a difference to the intended results of the bribes. Both are paid to get an unfair advantage. The challenge with detecting bribes is that no assets are stolen from and no entries are made in the records of the business. These transactions are outside the record keeping system of the victim.

15. Fraud Identifier: Extortion and Blackmail

Definition

Extortion
Extortion means demanding or obtaining property from another through the use of threats, coercion, or intimidation. This can include threats of physical harm or some form of blackmail such as threats to cause harm to one's reputation, livelihood, marriage etc. Extortion is a crime, which involves the illegal acquisition of money, property, or favors through the use of force, or the threat of force.

Blackmail
Blackmail is a crime of threatening to reveal embarrassing, disgraceful or damaging facts or rumors about a person to the public, family, spouse or associates unless paid off to not carry out the threat. It is one form of extortion which may include other threats such as physical harm or damage to property. In common usage, blackmail involving threats to reveal substantially true and/or false information about a person to the public, a family member, or associates unless a demand is met.

Description

Extortion
In some states extortion has only occurred when money or property has actually changed hands as a result of the threat. Extortion occurs when a person obtains money, valuables or other assets from another person or entity through some form of coercion. Coercion may include, but is not limited to, the threat of violence, damage to personal property, ruination of reputation and the threat of an action considered unfavorable to the extorted person. Historically, extortion was defined as an abuse of privilege on the part of a public official who used his or her position to get money or favors, but today, people at all levels of society could potentially commit extortion. Penalties for extortion vary, depending on the specifics of the crime. In some countries, extortion is treated especially seriously

because it is linked with organized crime, and sometimes special laws are designed to make it easier to prosecute and punish extortion.

Blackmail
It may be defined as coercion involving threats of physical harm, threat of criminal prosecution, or threats for the purposes of taking the person's money or property. Blackmail may also be considered a form of extortion. Although the two are generally synonymous, extortion is the taking of personal property by threat of harm. It is the use of threats to prevent another from engaging in a lawful occupation and writing libelous letters or letters that tend to provoke a breach of the peace, as well as use of intimidation for purposes of collecting an unpaid debt. The modus operandi of blackmail is by threatening to reveal damaging or embarrassing information in order to coerce money or other goods or forms of cooperation out of the victim. For blackmail to be effective, the blackmailer must, in most cases, have physical proof of the information he or she threatens to reveal, such as photographs or letters. The victim of blackmail is typically threatened with exposure of his or her private life, the consequences of which can range from embarrassing to socially devastating to legally damning. At its most serious, blackmail may rest on the exposure of a serious crime, which would do infinitely more damage to the victim than complying with the blackmailer. Even secret information that is not of a criminal nature, however, can make the victim of blackmail feel that he or she has no recourse against the crime.

Extortion vs. Blackmail
Extortion is often confused with blackmail. They are both similar crimes, but blackmail is considered less serious. Extortion is a theft crime with an element of force. Blackmail refers to a threat that is usually socially damaging, but the threat is usually not otherwise illegal. The threat in blackmail is often the public revelation of specific information. Neither extortion nor blackmail requires a threat of a criminal act, such as violence, but merely a threat used to elicit actions, money, or property from the object of the extortion.

16. Fraud Identifier: Kidnap

Definition

Kidnap can be defined as ‘taking away or transportation of a person against the person's will, usually to hold the person in false imprisonment, a confinement without legal authority. This may be done for ransom or in furtherance of another crime
Description

Kidnapping is a normal business fraud Threats, telecommunications can be affected when the kidnapper hold a hostage with the intention of forcing another person to assist the immediate theft of valuables or concede some other form of ransom from a telecom organization such as HLR manipulations, subscriber activations or other kind of internal fraud. In some cases is related to crime organizations.

Types of Kidnap

A. **Stranger Kidnap:** Stranger kidnapping victimizes more females than males, occurs primarily at outdoor locations, victimizes both teenagers and school-age children, is

associated with sexual assaults in the case of girl victims and robberies in the case of boy victims (although not exclusively so), and is the type of kidnapping most likely to involve the use of a firearm.

B. Political Kidnap: Kidnapper targets are usually public figures, ransom demands are not conventional, (Money), Political Kidnap looks to promote a cause or a change in an organization policy.

C. Tiger Kidnaps: A tiger kidnapping or tiger robbery is a crime in which abduction forms part of a robbery, murder, or any other crime. A person of importance to the victim is held hostage as collateral until the victim has met the criminal's demands.

17. Fraud Identifier: Money Laundering

Definition

Money laundering is the practice of disguising the origins of illegally-obtained money. If successful, the money can lose its criminal identity and appear legitimate

Description

Money Laundering is a normal business fraud Threats. Illegal arms sales, smuggling, and the activities of organized crime, including for example, drug trafficking and prostitution, can generate huge sums. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimize" the ill-gotten gains through money laundering. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. In summary, the money launderer wants to:

A. Place his illegally-obtained money in the financial system, without arousing suspicion;

B. Move the money around, often in a series of complex transactions crossing multiple jurisdictions, so it becomes difficult to identify its original source; and

C. Then move the money back into the financial and business system, so that it appears as legitimate funds or assets.

18. Fraud Identifier: Insider Dealing Fraud

Definition

Insider Dealing fraud occurs when an employee or company official uses confidential, internal information to gain personal profit or other advantage. This may be in the form of

pricing policies, business or market strategy, or other key areas of the business which external entities would be interested in having advance knowledge.

Description

Insider Dealing focuses around a person or persons who, as a consequence of their position in the company, have access to information that, if provided to others outside the organization, could materially impact the outlook or strategy of the company, including specific areas around:

1. Profitability
2. Financial position
3. Balance sheet
4. Market strategy
5. Etc.

Ultimately these impacts affect share price and/or overall value of the organization, and as a result may carry heavy legal and civil penalties for external disclosure.

As part of an overall company strategy, all external facing communications should be directed through a single, authorized channel within the business. Additionally, detailed and explicit policies for information disclosure about the company to any outside entity (person, group, business, etc.) should be created and provided to all employees.

19. Fraud Identifier: Procurement Fraud

Definition

Procurement Fraud is defined as the inflated or otherwise altered pricing that is presented to a receiving company for payment. In fact, the inflated pricing is designed to pay a dividend, benefit, or "kickback" to a party within the receiving organization, as discrete compensation for the purchase. See also **Misappropriation of Assets – False Invoicing**

Description

While this practice is seen throughout employee ranks of an organization, Procurement (or contract) fraud is most relevant to senior company officers, and is probably the least visible and most costly to the organization. This fraud is frequently a hidden byproduct of seemingly legitimate transactions, often involving millions of dollars, between the telecom carrier and a supposedly legitimate vendor. Very specific examples of this exist throughout telecom operators, especially in developing markets, and most prominently in countries where government-owned operators have far less audit control and mandate.

Audit entities worldwide have reported cases of discovered procurement fraud, however many carriers elect to not publish the findings due to risk of prosecution, poor customer relations, or other adverse results.

Most common procurement fraud involves an employee working with an outside vendor to award a contract or other purchase. The employee, as a discrete condition of the

award, instructs the vendor to inflate the invoice(s), and to deposit the additional payment into an offshore account in that employee's name (or holding entity). Generally, the most common procurement frauds include:

- Bogus or inflated invoices
- Services and/or products that are not delivered
- Work that is never done
- Contract manipulation
- Employee kickbacks

A report in 2008 by the Association of Certified Fraud Examiners (The *2008 Report to the Nation on Occupational Fraud and Abuse*) estimated that a typical organization loses a staggering 7% of its annual revenue to occupational fraud (including Procurement fraud). While this report encompassed more that telecoms, the impact is an almost *trillion* dollar fraud loss to a developed market (e.g., the United States).

20. Fraud Identifier: Payroll Fraud

Definition

Payroll fraud is fraud committed by an employee on their employer in the course of their employment. As a group they are more common and cause more financial loss in total to businesses than other third party frauds. As employees will continue to work at the business, they will generally try to hide these frauds permanently, meaning that occupational fraud can be committed over an extended period of time. This is an occupational fraud where an employee attacks the payroll system of a business. They include schemes against the salaries and wages payment systems and the expense reimbursement systems.

Description

Payroll fraud is one type of occupational fraud. This type of fraud can also be classified as asset misappropriation-cash that is disbursed in a fraudulent manner. There are several schemes associated with payroll fraud and the most prevalent is ghost employee schemes.

GHOST EMPLOYEES

A ghost employee is non-existent employees on the payroll, or someone recorded on the payroll system, but that does not work for the business. The ghost can be a real person that is placed into the payroll system, or a fictitious person invented by the fraudster. The aim of the fraud is to have a wage paid to the ghost and collected by the fraudster. The system does not require an accomplice to act as the ghost, but depending on the method of payment (cash, check or direct deposit of wages), an accomplice may make the fraud easier to commit, as it will eliminate the need to convert the payment from the ghost to the fraudster. The main factor that hides this scheme is size. There will have to be sufficient employees on the records for another not to be noticed. Size is also the greatest deterrent against this fraud. After a certain number of employees, the business will have to have a larger Human Resource division. After that critical size, separation of Human

Resource activities will come into play. To make a ghost employee scheme work, four activities must occur:

1. A ghost must be added to the payroll
2. Time information must be added
3. They must be paid by the victim
4. The payment must be received by the perpetrator

Adding ghost employees to the register may be as simple as using the 'Add Employee' function in the payroll system. In this way ghosts may be added without the normal authorization paperwork. Otherwise the employee will have to circumvent the controls in place in some other manner to get the ghost on the payroll.

If the ghost is paid a wage, time sheets or other wage information will have to be created as required. It is easier to make the ghost a salaried employee or similar so that this information will not be needed and constant maintenance of the fraud is not required. Once the ghost has been added to the system, the salary payment should be automatically generated. Adding the ghost can be accomplished by different means, depending on the internal controls in place, the ghost could be added by an employee within or outside the payroll department. Any payroll department employee with access to the payroll records and/or payroll software could potentially create ghost employees. Internal controls that would help mitigate ghost employees range from simple precautions to detailed procedures. For the payroll fraud mentioned earlier involving children of the perpetrators, simply requiring the employees to show identification when picking up their paychecks could expose ghost employees. Frequently changing passwords for payroll access can help prevent fraudulent entries as well as requiring payroll employees to take an annual vacation. Additionally, print a list of all new employees each week, and have a person not responsible for initiating new employees confirm those names with the employee's supervisor.

21. Fraud Identifier: Expense Fraud (False Claims)

Definition

Expense frauds are committed by dishonest employees that are aimed at attacking the payroll and expense reimbursement system of a business. They fall into two main areas, false claims for expenses, and false claims for wages. False expense claims arise when employees who are entitled to be reimbursed for expenses incurred while performing their work duties, claim expenses to which they are not entitled.

Description

False wages claims arise when employees who are paid on an hourly rate or remunerated on some basis other than a salary, manipulate the system to falsely increase their remuneration. Expense claim frauds are usually smaller than other occupational frauds as the amount of the expenses that may be reimbursed to employees are generally small - but they may be common and occur over long periods. Claims for reimbursements may be approved by someone who has no knowledge of what amount the expenses should be, or whether the expense was incurred at all.

Usually there is no need to hide the false claims once they have been paid. Like billing schemes, the conduct of the fraud itself makes the transaction look like a legitimate business expense. In effect, the fraud is hidden in plain sight in the records of the business. The fact that the employee does not need to hide the theft of the money makes it more appealing to do than simply stealing money, where the employee usually must hide it.

Generally the more senior the employee making the reimbursement claim, the less likely that the claim will be questioned. If that senior employee has access to the reimbursement process and can manipulate the records, a fraud will be difficult to locate, even if anyone decided to check the claims. The common ways to commit this fraud are:

1. Generating false documentation; and
2. Filling out blank receipts.

One popular method is to do **over-purchasing (inflated claims)**. Over-purchasing is purchasing too much of what is required or a more expensive item in the first instance and obtaining a receipt for that larger amount. The employee then returns some of the more expensive item, and obtains a refund. If needed, a less expensive version is purchased to replace the more expensive one. A claim is made for the greater amount, and the difference between the smaller actual amount purchased and the larger amount of the reimbursement is the gain to the fraudster.

Some businesses have no claim approval process at all. Expenses under a certain amount may be paid without any verification. This is usually done for expedience and cost saving on the basis that the claims are small and not worth examining. But the amount of an ongoing loss may grow to be significant over time. Most businesses that do not have regular expense claims made by employees have very few procedures to control reimbursements. Some will perceive it as a waste of resources. Added to that attitude, controls that are in place may be ignored when the expense is charged to a client. This is justified on the basis that the cost is not borne by the business and any improper increase will not cause a loss. This attitude will lead to the business to be less caring whether fraud is committed as they are not the ultimate victim. Most controls that are put in place are nothing more than providing a receipt to the appropriate clerk and possibly completing a short reimbursement request form. Further checks may not be made, unless the expense is particularly significant in size or very out of the ordinary.

These frauds are usually committed when a number of employees are making expense claims on a regular basis, or when the dishonest employee is making regular legitimate claims. The business will be expecting claims and the volume would help to hide any false claims. Inflating other employee's expense claims is usually done by the person processing reimbursement claims and without the knowledge of the other employee. That person increases the legitimate expense claim of another employee, draws the payment at the higher amount, pays the employee the proper lower amount and then keeps the difference. Generating false but professional looking documentation can be done with any personal computer or photocopier. False documents are submitted as genuine claims. One form of this fraud is for the perpetrator to write personal checks for what looked like business expenses, attach photocopies of these checks to the false documentation to make it look like they have paid the expense, and request reimbursement. The checks were never used, the purchase was never made, but the reimbursement is paid. Blank receipts can be obtained or stolen from vendors and

service providers. The easiest blank receipts to obtain are from taxi as they are hand written on the back of their business cards. There is no difficulty in obtaining a number of these blank receipts without suspicion. Some businesses still use off-the-shelf invoice books. These can be purchased by anyone at any news agency. False claims can be made in the perpetrator's name or, if the perpetrator has the required access, in the name of another employee.

22. Fraud Identifier: Treasury Fraud

Definition

Treasury, by definition, is where the money is, where the corporation's cash is guarded and managed. It is also where the money can be lost. Therefore, protecting the company's financial assets from fraud starts with a secure treasury. To ensure that only legitimate, authorized transactions occur, treasury managers must design and enforce procedures and controls that will prevent the fraudulent diversion of funds. And because treasury professionals have the greatest opportunities to misappropriate funds, treasury security must be especially tight.

Description

A trusted treasury employee who takes advantage of a gap in or breakdown of security measures can do irreparable harm. When employees have access to large amounts of money, the financial loss can be staggering. The recent downsizing of many treasury departments may have concentrated responsibility and increased workloads to the point where embezzlement is more likely to occur. Productivity improvements may even have inadvertently eliminated "redundancies" that were important checks against internal fraud. As a result, newly "lean" treasury departments have special reasons to review their exposures to internal fraud to make sure they are still secure. How can treasury professionals enforce tight security in their departments? They should concentrate on three areas:

- The receipt and processing of incoming payments,
- Electronic disbursements
- Check disbursements.

Although security analysis often focuses on disbursements, the flow of payments into the company also represents an important and vulnerable stream that must be protected by a carefully planned program. The theft of incoming payments not only deprives the company of working capital, it also may lead to huge public and investor relations problems. Employees can steal incoming payments from the mail before it is delivered to the company or after it is delivered but before payments are deposited into the company's accounts. Companies can reduce their exposure to these losses by implementing dual control procedures for mail collection and in-house processing or by using a lockbox for remittance processing.

23. Fraud Identifier: Bypass - Tromboning

Definition

Tromboning (i.e. delivering unauthorized traffic across restricted trunks) is widely used in Arbitrage and for the sake of By-pass; carried out by fraudulent carriers.

Basically, tromboning is where RTP media traffic originates at a certain point, and follows a path out into the network and back to a destination close to where the RTP traffic originated.

Description

In the richness and complexity of today's networks, especially in VOIP networks, the way to transfer any kind of data between 2 peers is enormous and has many paths.

In order to transfer this data, the network will direct the data between the shortest paths available within the network.

In a tromboning action, the servers may be configured to force the RTP media to go through the server itself instead of flowing over the shortest path between endpoint- and that is called tromboning.

Tromboning is another way of bypassing "regular" paths in the network in order to lower costs.

24. Fraud Identifier: Bypass – SIM Boxes

Definition

An apparatus (incl. s/w) housing several SIM cards (pre or postpaid) used to generate many concurrent mobile calls. Legally used by mobile operator to test networks, un-officially used for incoming (terminating) by-pass activities. Can swap IMEIs and IMSIs. Can be controlled from remote

Description

SIM box operators exploit the difference between termination rates (which are often regulated) and cheapest on-net rates.

SIM box has the ability to intercept a call and set a new on-net call, this in order to lower the cost of the call.

By intercepting and re-doing the call, the SIM box transfers the call from the originating network, to a mobile number of the domestic operators and creates a cheaper call.

For each of these calls there is a net loss, due to the bypassing of original routes, But the termination network usually does not mind as it receives the interconnect fee anyhow.

Important to note that such transition often affects the Quality of call and QOS as a whole.

Impact on quality of service will take place as:
- There is no CLI
- Recall and voicemail functionality often are jeopardized
- Inbound roamers are not reachable
- Call quality is highly affected

As far as the network is considered:
- High concentration of traffic
- Impact on quality to all users
- Incorrect statistics on international calls

25. Fraud Identifier: Bypass – Fixed Cell Terminals

Definition

Fix cell terminals offer access from otherwise landline services to cellular networks. The intent is often to re-route landline traffic to less expensive wireless transport.

Description

Several manufacturers offer fixed cell terminals as a legal, viable alternative to expensive landline calling, however in some regions this practice is considered fraudulent. A fixed cell terminal is often connected to a PBX (or similar) system, and in organizations with high volumes of outgoing traffic, especially traffic crossing LATA and Interconnect boundaries, cost savings by sending the traffic via CDMA/GSM instead of fixed lines/trunks, can be substantial.

26. Fraud Identifier: Bypass - Premicells

Definition

A Premicell is a device that is capable of routing an outbound (typically landline) call over the cheapest route within a cellular network.

Description

Premicell devices route a call over whichever network is the cheapest, based on whether it is local or long distance, time of day and whether the destination is a landline or a mobile number.

Premicells often pit landline operators against mobile operators (and premicell manufacturers), as mobile operators claim they have the right to help corporate customers slash their phone bills by using least-cost routing practices offered via premicell equipment. Fixed line carriers in many regions are in legal battles to have this practice declared illegal.

The practice lets a company install a premicell device to its switchboard to divert calls off traditional landlines and on to the cellular networks. It is so popular that in some regions it is reported that up to 90% of the largest enterprise customers are engaged in this practice to some extent. Mobile operators have claimed that the average company can slash 15% to 20% off its monthly bills by employing this technology.

27. Fraud Identifier: Bypass – GSM/UMTS Gateways

Definition

GSM/UMTS gateways are Devices that allow a call on a fixed line network to be connected directly to a mobile network .By "bridging" the 2 networks these devices offer a way to exploit price differentials of a mobile network provider.

Description

The GSM gateways are stuffed with SIM cards, placed in a steady place that receives service from a specific cell site, in order to connect to the network, instead of using a normal fixed interconnection between the networks.

Instead of paying the full price to determinate an interconnect call legitimately, the fraudster instead pays the retails costs of a local call.

The affected operator here is the mobile operator, that is losing some of its revenues.

Also, concentrating such high volume of traffic under a specific cell site might jeopardize its performance.

28. Fraud Identifier: Bypass – Landing Fraud

Definition

Landing Fraud occurs when a call is “landed” on a carrier’s network in a way that avoids toll charges. This is accomplished by making the traffic appear to have originated locally, or otherwise within the carrier’s network.

Description

Landing off-net calls onto a mobile operator's network, normally through the use of a SIM box, avoids the GSM gateway and thereby evades the GSM interconnect charge. GSM Gateway Fraud is a thread and problem evolving new business models. The low cost of set-up permits to deploy it anywhere where internet available and thus increase the exploit and chance of damaging interconnect fees between carrier.

Rerouting calls via landing will not only bypass regular routes (and thus avoid toll billing), but it can also jeopardize the network by providing low quality of calls, low quality of

service and even affect the network performance when a specific GSM gateway will overpower a cell site.

Landing fraud via fixed line services is accomplished via VoIP and PBX equipment, where voice traffic is extracted off the internet and exited out into a PSTN network via a PBX system.

29. Fraud Identifier: Bypass – VoIP Bypass

Definition

VoIP (Voice over Internet Protocol) bypass is most commonly a situation where traffic that would normally terminate on a local network via interconnect trunk routes has instead entered the network via an IP path, now appearing as local originated traffic.

Description

While VoIP traffic is becoming more prevalent today (computer-to-computer, computer-to-landline, landline-to-computer, etc.), VoIP traffic that is entering and terminating on a home carrier's network through fraudulent means is a significant threat to carrier revenues overall. Traffic transiting between carriers typically enters and exits carriers via gateways, and carriers have detailed agreements with their surrounding partners on rates for minutes of use for either terminating or otherwise transporting the originating carrier's traffic. In the case of bypass, two forms have existed:

1. Legacy Bypass: Carrier A and Carrier B have agreements in place to carry and/or terminate each other's traffic, and have contracts that outline settlement reimbursement schedules with each other. However, Carrier C has negotiated a cheaper termination rate with Carrier A. Carrier C then may approach carrier B and offer them a cheaper rate to get the same traffic to Carrier A's network. As a result, Carrier B will lower its expense, and Carrier A's revenues will similarly decrease. Legality questions around this practice vary based on region, regulations, etc.
2. VoIP Bypass: In the similar case of the same two carriers, A and B, Carrier B has moved a portion of its traffic destined for Carrier A to an IP network. Carrier B will most likely have access to an exit point (SIM box or PBX) where the traffic leaves IP and returns to SS7-based facilities within Carrier A's home network transport area. For all traffic now routed via IP into Carrier A's network, this traffic appears as local to Carrier A, and thus no settlement is billed to Carrier B. At the same time, Carrier B is still able to bill their event originators at full interconnect rates.

Prevalent Methods for IP to SS7 traffic transfer:

1. SIM Box – in this case, multiple SIMs are loaded into a "SIM Box" which acts similar to a PBX, yet moves IP voice traffic out to mobile networks for termination on either mobile or fixed line equipment.
2. PBX – this is a common approach to move IP voice traffic out to local fixed line networks. Due to the general acceptance and availability of PBX platforms, this is often a far easier method to move IP traffic to SS7 networks undetected.

Risks to Carrier A:

1. Loss of interconnect revenues – the carrier has terminated interconnect traffic unknowingly.
2. Increase in traffic overall – in these cases, to avoid detection, Carrier B may not decrease common settle traffic volumes via SS7-based networks, however Carrier B may engage in aggressive campaigns (to enterprises, other carrier partners, etc.) to increase traffic is may send via IP.

Detection Method(s)

Bypass in general tends to pattern itself with call traffic that is unbalanced, with much more emphasis on termination traffic.

30. Fraud Identifier: Bypass – Interconnect Fraud

Definition

Interconnect fraud involves the manipulation, falsification or removal of records by operators to deliberately miscalculate the money owed by one Telco to another. There are many forms of Interconnect fraud including:

- Interconnect peer inflates traffic figures to be paid more
- Arbitrage
- Tromboning

Description

Interconnect fraud appears in all sorts of forms, as described in this document, but the basis of all of them and the focus of attention will be an effort of one company to manipulate data of existing traffic, and disguise it by removal of files, sending in correct data etc.' – in order to create a misleading picture of a lesser volume of traffic- in order to pay less to the specific interconnect partner on which the manipulation has been done.

31. Fraud Identifier: Bypass – Toll Bypass

Definition

Toll bypass allows customers to bypass the PSTN network, and the associated toll charge. Toll Bypass is very similar to **Landing Fraud**, except the traffic may not enter the PSTN network at all in a Toll Bypass situation.

Description

The PSTN network consists of the tandem time-division multiplexing (TDM) based switches used for long-distance (or toll) voice calls. Enterprise customers who typically

depend on the PSTN for their interoffice (intra calls) voice traffic avoid toll charges by using an IP network with routers that serve as the edge voice gateways.

Toll bypass allows some Internet service providers (ISPs) to offer residential customers free, or very low-cost, long-distance voice calls by routing the calls over an IP network.

32. Fraud Identifier: Bypass – Third Country

Definition

Third Country Bypass fraud can be found mostly in messaging (SMS, MMS), although it does also exist in voice traffic scenarios, where the originator of messages (or traffic) spoof the origination IDs to a 3rd country/operator, which is later charged for the traffic.

Description

Third Country Bypass fraud occurs when the fraudster has the ability to alter the traffic origination information, thus causing a different entity to be billed for the traffic. In mobile SMS and MMS environments, spoofing of the origination ID of the message is the primary method, while in voice services, CDR traffic may be altered to show either a different origination point (home operator), of the origination point may be obscured all together. In those cases where origination points are obscured, intermediate parties carrying the traffic may be inadvertently billed for the call, with no carrier recourse.

33. Fraud Identifier: Bypass – Grey Routing

Definition

Grey Route is the arrangements that fall outside the regular course of business between the licensed telecoms companies in each country. The grey part of the route is usually realized at the far end where the call is terminated. Up to that point, the call is delivered normally and the call transfers from the subscriber to the sending carrier and then to the sending carrier and the satellite or cable operator for the trunk part of the call. The 'grey'-ness arises because the terminating end the call is made to appear as if it originates locally, as a domestic call, or arrives as an internet delivered call, rather than a more expensive standard international call.

Description

Gateway operators deliberately route international voice calls in an effort to avoid higher operator charges at the respective interconnection points. The most common method uses a **GSM gateway** (e.g., 'SIM box' or 'GSM Router') to terminate VOIP on an operator's network as a local call. Similarly in **fixed networks**, switch bypass operators may use a TDM Gateway, PBX, and/or other methods to terminate VOIP on an operator's networks as a local call.

In most situations, the "grey route" operator brings international traffic over the internet and terminates them as local calls on the GSM or Fixed operator's network, denying the operator the international termination rates.

Grey routing is also known as switch bypass fraud. This practice has maintained a very low barrier to entry due to global internet connectivity, plug-and-play equipment and the emergence of 24/7 minute trading – while countries are working to make this practice illegal, in many regions the legality of this method of bypass is still not fully defined.

34. Fraud Identifier: Bypass – International Simple Resale

Definition

Involves landing off-net calls onto an operator's network but avoiding the international gateway to avoid the International interconnect charges.

Description

International Simple Resale or ISR, is also a form of Interconnect Fraud. ISR involves landing off-net calls onto an operators network but avoiding the international gateway to evade the international interconnect charge.

A variant of ISR, known as GSM Bypass, involves landing off-net calls onto a mobile operators network, normally through the use of a SIM box, avoiding the GSM gateway and thereby evading the GSM interconnect charge. This is further explained in “Landing Fraud” in chapter 29.

35. Fraud Identifier: Missing Trade Fraud

Definition

Missing trader fraud is stealing large amounts of Value Added Tax (VAT) from a government by organized crime gangs who exploit the way VAT is treated within multi-jurisdictional trading where the movement of goods between jurisdictions is VAT-free The fraudsters steal money that could be used for essential public services.

Description

Missing Trade Fraud is a normal business fraud Threats. The simplest missing trader fraud is where a fraudster imports some goods, and then sells them. When he sells them, he charges the price of the goods, plus VAT. He then absconds with the VAT instead of paying it to the Government. This situation, where the goods are made available for consumers in the importer's home market is often known as 'acquisition fraud'. In telecommunications typically involves goods such as mobile phones and computer parts.

36. Fraud Identifier: Carrousel Fraud

Definition

Carrousel Fraud is an evolution of "Missing Trader Fraud", in this situation, the goods are sold to a series of companies, before being exported again. The goods therefore go round in a 'carousel'. These companies are called "buffer". In a real case there can be many buffers, all helping to blur the link between the final reclaim and the original importer, which will vanish.

This entire series of transactions can occur without the goods ever leaving the dock before being re-exported. Furthermore the same goods (telephones or computer parts for example) can be used again and again going through the various buffers, each pass around the 'carousel' bringing reclaimed VAT to the fraudsters.

Description

The typical carousel fraud usually operates in the following way:
Company A, in one EU member state, sells goods to company B in another member state, Company B either a defaulting trader or a trader employing a hijacked VAT number sells the goods on at a discount to a company C in the other member state. C is a buffer company that can therefore make further sales at a profit. Company B incurs a liability to VAT on the purchase of the goods (acquisition tax), but as it has used those goods for taxable transactions, it is also entitled to deduct that VAT as input tax. Although it has incurred VAT liability on the output tax it has charged to company C, company B goes missing before discharging that liability to the tax authorities. Buffer Company C then sells the goods on to another buffer company D, also in the other member state, paying the authorities the output tax it charged, after deduction of the input tax it has paid. This continues until a company in the second member state exports the goods to another EU member state. While exports are exempt from VAT, the exporting company is entitled to claim a refund of the input tax it paid on the purchase of the goods. Should the purchaser in the last member state turn out to be company A.

37. Fraud Identifier: Roaming Fraud

Definition

Roaming Fraud is the use of telecom products or services, such as voice or data services, outside the home network with no intention to pay for it. In these cases fraudsters exploit the longer time-frames required for the home network to gain visibility of usage by its customers.

Description

Roaming fraud can starts as an internal or subscription fraud in the home network, when obtained sim cards are sent to a foreign network the fraud or abuse starts. Roaming Fraud is related to other fraud types such as International Revenue Share Fraud, Call Selling, Call to Premium Rate Numbers,

38. Fraud Identifier: Cloning Fraud

Definition

A cloned cell phone is one that has been reprogrammed to access to a cellular network as a legitimate cell phone. The legitimate phone user then gets billed for the cloned phone's calls.

Description

Cloning has been shown to be successful in TDMA/ CDMA Networks, but rare on GSM. However, cloning GSM phones is achieved by cloning the SIM card contained within, not necessarily any of the phone's internal data (GSM phones do not have ESN or MIN, only an IMEI number.) There are various methods used to obtain the ESN and MIN; the most common are to crack the cellular company, or eavesdrop on the cellular network.

39. Fraud Identifier: Spam – Malware Fraud

Definition

Spam-Malware fraud is perpetrated when a spam event (email, text, advertisement, etc.) is received by the victim, and contains link(s) disguised as a trusted sites, yet contain damaging malware.

Description

Spam appears in most environments with telecommunication products today. In mobile text events, internet sites, internet advertisements, and email, spam has been inserted by persons and organizations to encourage viewers to access the link(s) contained within the spam. These links most often lead to malware.

Spam-Malware example: In blog spam, comments to the blog sometimes try to entice people to go to another site. The site being advertised may simply be trying to boost its search engine rankings to generate more ad revenue, however more often the site has malicious results by activating malware (e.g., a virus).

40. Fraud Identifier: Spam – Spoofing Fraud

Definition

Spam – Spoofing Fraud is the case of an unwanted or unsolicited message being delivered to the recipient, with the sender appearing to be someone else.

Description

Spam is commonly defined as unsolicited bulk messages (email, SMS, etc.). Year on year, users are reporting increasing amounts of received spam, and most consider spam a significant problem.

There are generally two types of spam: **Intentional** and **Unintentional**. Intentional spam comes from spammers who are soliciting products or attempting to commit fraud. Unintentional spam originates from computers and mobile devices that are infected with a virus or worm that activates e-mail or text distribution processes in the background. The virus or worm attempts to send bulk messages from the infected device without the awareness of the computer owner.

Spoofing occurs when the sender of an e-mail message pretends to be someone else. Spoofing is often used by spammers by simply changing the "FROM" e-mail address.

Spoofing may occur in different forms, but all have a similar result: A user receives a message that appears to have originated from one source when it actually was sent from another source. Spoofing is often an attempt to trick the user into releasing personal (or sensitive) information, making a damaging statement, or allowing access to additional recipient contact information.

41. Fraud Identifier: Spam – IP/Phishing Fraud

Definition

Spam – IP/Phishing Fraud is defined as an attempt to trick the user into entering personal information (accounts, passwords, etc.) for the purpose of identity theft. Phishing often appears as a legitimate message from a known entity (e.g., victim's bank).

Description

Spam is commonly defined as unsolicited bulk messages (email, SMS, etc.). Year on year, users are reporting increasing amounts of received spam, and most consider spam a significant problem.

There are generally two types of spam: **Intentional** and **Unintentional**. Intentional spam comes from spammers who are soliciting products or attempting to commit fraud. Unintentional spam originates from computers and mobile devices that are infected with a virus or worm that activates e-mail or text distribution processes in the background. The virus or worm attempts to send bulk messages from the infected device without the awareness of the computer owner.

Phishing is a special type of spam that is intended to trick the victim into entering personal information (account numbers, passwords, etc.) for the purpose of breaching the victim's account and committing identity theft or fraud.

In a typical Phishing scenario, a false message is delivered to you via email or text. The message *appears* to come from a legitimate source (see spoofing in the previous fraud

section), but in fact the message is a scam. The message may contain a legitimate corporation's logo, and appear to be sent from the corporation's e-mail address. The message may appear *exactly* as previous legitimate corporation messages. The message may ask you to click a link in the message to update your account, or run a software program to upgrade your computer.

Although the message looks legitimate, it is really trying to compel users to submit personal and confidential information, which will be used to steal credentials. Normally users are asked to enter information such as name, date of birth, place of birth, social security number, mother's maiden name, bank account number, and bank account PIN.

Virtually all internet service providers have been the targets of phishing scams. Today most internet-accessible (and provider) organizations state that they will *never* ask for disclosure of personal information via a message correspondence.

42. Fraud Identifier: (International) Revenue Share Fraud (IRSF)

Definition

IRSF is generally initiated by fraudulent traffic activity generated on a network that causes payments to another network or PRS provider, however the subsequent revenues will not be collect for those events.

Description

RSF is more commonly captured as ISRF (International Revenue Share Fraud), as most instances have been related to SIM card cloning activity. In general, RSF follows a particular path:

1. Cloning or otherwise unlawful acquisition of service (SIM cloning, PBX hacking, etc.)
2. Consumption of service (voice calls, PRS events, etc.) involving a partner network or PRS provider.
    a. Consumption of service in SIM cloning usually involves moving SIMs to a roaming network, and purchasing PRS services, causing payment to an often fraudulent 3rd party from that roaming carrier.
    b. Consumption of service in PBX hacking often involves calls being made to premium toll services operated by fraudulent 3rd parties. This results in toll charges being paid by the carrier and/or the enterprise which owns the PBX.
3. Activity is generally short term on any given SIM identification or PBX line, depending on detection technology available.

Detection Method(s)

1. Velocity Monitoring – Witnessing events belonging to the same SIM identifier which are geographically distant yet within a close timeframe (e.g., 2 events happening from the same GSM handset, 1000 km apart, with 10 minutes of event start time.

2. Event overlap – Similar in concept to Velocity, subscriber is detected executing 2 events simultaneously or overlapping in time, from different locations.
3. IMEI Change – A subscriber is changing their device (IMEI) several times within a certain time period (detected by xDR traffic IMEI identifiers from same subscriber)
4. Location Updates – Suspicious subscribers and past cloning suspects are monitored for location velocity issues daily.
5. NRTRDE Monitoring – Near Real Time Roaming Data Exchange (NRTRDE) traffic is monitored for overlap and velocity events. Latency of data (within 1-3 hours) may result in moderate losses before data is captured and analyzed.
6. CAMEL Monitoring – Typically a faster path than NRTRDE (Near Real Time Roaming Data Exchange); CAMEL Monitoring facilitates monitoring of current MOC/MTC traffic of roaming subscribers, to quickly detect overlap and velocity situations.
7. Proactive Clone Detection (PDC) – The practice of comparing authentication of services across multiple geographies, to look for cloning incident. This practice may heavily reduce event losses if processes are in place to quickly detect and suspend cloned equipment.

43. Fraud Identifier: PBX Hacking Fraud

Definition

PBX (Private Branch Exchange) hacking incidents typically occur when the PBX is directly accessible (business facility is unattended), the PBX usage is not monitored, or the PBX is accessible outside the business (e.g., via IP connectivity). When hacked (accessed through unauthorized means), call events are placed and routed via the PBX and the business owners are unaware of the events.

Description

Several Methods of PBX hacking are most common today:

1. **Brute Force Attacks**: In this case the PBX security is breached via the toll-free Direct Inward System Access (DISA) number. Many PBX systems allow dial-through, wherein a person calling into the PBX can access an external line by using appropriate passwords and control sequences. This feature is common in large business environments.
    a. Fraudsters hack into the PBX, obtain passwords, and then use the PBX to generate outbound calls (often for call selling or PRS revenue share).
    b. "War dialing" is often used for obtaining passwords. This method involves the fraudster using an auto dialer, which keeps on dialing the same number, then enters a continuing, exhaustive sequence of codes until it breaks through the password layer.
2. **Default Passwords**: One of the largest contributing factors in PBX hacking is poor or incomplete PBX installation and configuration, leaving default user and maintenance port passwords in place (fraudsters know the default passwords for the various switch vendors). PBX fraud commonly occurs when the customer fails to change the default password(s) or do not change passwords frequently. Default passwords can be found online in the relevant PBX user manuals etc.

3. **Internal Enemy**: Many cases of PBX hacking result from insiders or vendors who disclose the phone numbers, IDs and passwords necessary for breaching PBX security. Users may obtain passwords by unauthorized means, allowing the use of corporate lines for making personal calls or colluding with external fraudsters to help in PBX hacking. Strict security Policies should be in force for PBX password control. Additionally, the physical security of PBXs and phone extensions is also an important factor to consider in avoiding misuse of PBXs.
4. **Social Engineering**: The traditional (wired) phone scam involving the 90# buttons on corporate telephone lines does still exist, mainly on older, legacy PBX systems. In this case, employees within the business receive a call from someone claiming to be a telephone company employee investigating technical problems with line, or checking up on calls supposedly placed to premium rate services or other countries from your line. The caller asks the employee to aid the investigation by either dialing 90# (or similar combination) or transferring him/her to an outside line before then hanging up the telephone receiver. By following these instructions the employee will enable the fraudster to immediately place calls that are billed to the corporate telephone account. This attack is becoming more rare, yet it is still a relatively common technique used for obtaining passwords.
5. **Service Port**: PBX hackers may also target modems or IP ports attached to the service port of a PBX. This access is provided by PBX manufacturers to allow remote support of the PBX. Typically, the connection should be opened only when an authorized request goes from the PBX customer to the PBX vendor, but many PBX customers keep the connection always open and therefore prone to attack.

In addition to theft of service, the following misuse can occur through PBX hacking:

1. Disclosure of Information (eavesdropping on conversations, or gaining unauthorized access to routing and address data).
2. Modifying Data (billing information changes, or system modifications to gain access to additional services).
3. Denial of Service attacks (password changing to deny access, or forcing the PBX to fail or degrade call quality through excessive call volume).
4. Trac Analysis such as observing information about calls, allowing inferences to be made (industrial espionage), e.g. from the source and destination numbers, or frequency and length of calls.

44. Fraud Identifier: IP Subscription/Identity Theft Fraud

Definition

IP Subscription/Identity Theft Fraud occurs when information related to IP address or other IP account information is stolen from the user. The fraudster can then use the information to hack the user's account and/or computer, with the intent to insert malicious software and/or steal sensitive (personal) information.

Description

IP Subscription and Identity theft is very common in today's connected world, and has made it virtually unthinkable to not have at least one form of firewall, virus, or other protection software installed on every computer and handset today.

IP addresses reveal the location of computers, and in most residential applications today, these are dynamically issued (each time the computer or home broadband router appears online to the ISP). In businesses, however, static (fixed) IP addressed are typically secured, allowing consistent VPN activity, website access, etc., to external users. Either of these environments does facilitate attacks on the IP addresses by fraudsters, making firewalls, secure encryption protocols, and other protection mechanisms absolutely critical to protect the integrity of the information within the computer or network.

The problem is not just one of access from the outside to within your network or computer; access may also be facilitated by inadvertent launching of phishing sites, or other malware programs. This is also something virus software programs have been designed to combat, by examining web sites (in real time with user activity), emails, and most other forms of external communications, to immediately identify threats.

45. Fraud Identifier: IP – AIT (Artificial Inflation of Traffic) Fraud

Definition

AIT (Artificial Inflation of Traffic) is the practice of increasing traffic that incurs charges to originating customers and operators, with payments going to the fraudsters (at least in part).

Description

AIT takes place over premium rate and revenue share (where terminating operator receives a share of the billed revenue) numbers which typically have a cost to the customer. In the case of AIT, the owner of these destination number ranges aims to inflate the traffic for financial gain – all at little or no cost to himself.

This increase in traffic can be in the form of spam or missed calls encouraging people to ring a certain number, exploiting a gap in billing systems or through auto-dialers.

Some premium rate and revenue share numbers are charged to the caller on a so called "single drop" basis *regardless* of the call duration. This leads to frauds involving very short calls, either to generate very large amounts of traffic as part of subscription fraud or to defeat the billing system at the originating point.

AIT is also seen in PRS environments where tiered pricing strategies are employed. In this case, as volume of use of the PRS service increases, higher discount "tier" levels are reached – which translates into more revenue for the PRS provider. This has resulted in many cases of AIT as the PRS provider approaches another tier level within a billing period.

46. Fraud Identifier: IP – DoS (Denial of Service) Fraud

Definition

Denial of Service (also known as Distributed Denial of Service, or DDoS) is the intentional "flooding" of traffic to a target web site, network, etc., to render the target disabled or otherwise unable to function properly.

Description

A denial-of-service attack (DoS attack) or distributed denial of service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the methods used, the motives, and targets of a DoS attack may vary, it is typically the coordinated efforts of a person, or multiple people to prevent an internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, large enterprises, and other highly accessed web and network environments. The term is generally used with regards to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests. The volume of the inbound requests makes the target machine unable to respond to legitimate traffic, or it responds so slowly it is rendered ineffective or unavailable. More simply stated, DoS attacks are designed such that the targeted computer(s) must reset, or are forced to consume internal resources so that it can no longer provide its intended service.

47. Fraud Identifier: IP – Content Sharing Fraud

Definition

IP – Content Sharing fraud is defined as sharing or distribution of content by an unauthorized entity. This may or may not be for financial gain, but the sharing (or redistribution) of the content is in direct breach of licensing agreements.

Description

Content sharing may involve any number of services, but most commonly content is considered to be premium products, including ringtones, music, games, movies, screen savers, and other products for sale by the content provider or their authorized agent(s). When procured, buyers are asked to agree to license terms as a condition of the sale; redistribution is virtually always not permitted within these agreements, and a buyer must agree to them in order for the sale to complete and the content to be delivered.

Commercial content sharing is a far more elaborate enterprise involving more discrete activities, on a much higher volume. This is frequently executed over international boundaries, as prosecution and damage recoveries are far more difficult and expensive for content providers. Note that this is also a governmental concern, as taxes are also

usually circumvented during this fraud, costing governments substantial losses in potential revenues.

Consumer content sharing is a prevalent practice, and not easily detected. Certain companies have allowed limited forms of content sharing (e.g., Apple itunes) within their end user agreements, which has benefited both users and Apple in the longer term, however other forms of content sharing still cost the content industry enormous amounts in terms of unrecognized revenues.

48. Fraud Identifier: IP – Identity Trading Fraud

Definition

Identity Trading fraud is the practice of stealing identities of users (personal financial information) and then offering those identities and access information for sale to other fraudsters.

Description

Identity Trading (selling) is a highly active business globally today, with most identity thieves offering to sell stolen identities in low-profile, often secret chat rooms and other communication environments. These selling forums have constant streams of thieves providing detailed information about stolen user identities, to prove they have what they are offering for sale. Payments to the thieves may be as simple as a PayPal transaction, and delivery as simple as email, however more volume-based and elaborate schemes may involve monies being deposited to offshore accounts under bogus companies, and secure transmission of considerable volumes of stolen users and their sensitive information.

49. Fraud Identifier: IP - Spyware Fraud

Definition

IP Spyware Fraud occurs when a Spyware software is installed on the user's computer or handset (smartphone) without their knowledge. The spyware then collects and transmits sensitive information to a destination for (typically) malicious purposes.

Description

Spyware is secretly introduced to the user's computer or handset. Not all spyware is malicious, as some types may be installed deliberately by the user (or their IT administrator) in order to track or monitor the activity of other users. This may be used in some corporate, shared or public computer situations.

Malicious spyware (installed without the user's knowledge by an unauthorized source) can extract data about the user or other data from their computer or handset and send it elsewhere. It can interfere with computer operations, change settings, bring up different

home pages, cause loss of Internet service and interfere with the functioning of other installed programs. Spyware is most often intended to monitor the activity of the user while on the Internet.

Spyware programs can easily collect and transmit personal information. This business intelligence is of value to advertisers and others who interested in knowing what websites people visit and what are their Internet surfing habits. More malicious spyware can even redirect browser input to land the user on a different website than the user intended. Because of its intent to transmit information without user knowledge, spyware is classified as privacy-invasive software.

Spyware is often coupled with adware (advertising-supported software). By clicking the adware, this allows the spyware to infect the computer without the user's knowledge. The result of an infection is that the user's computer will run slower and there will often be many pop-up ads that appear. While spyware and adware may then simply introduce general (pre-defined) advertising, pop-ups, etc., more “intelligent” spyware and adware use the information collected about the user's Internet browsing to put up ads that are directly related to that browsing behavior.

Spyware also reports user activity to third parties. This can be reports about which websites a user visits, the number of visits and activity while on a website. This all occurs in the background while the user is actively browsing. The security problems involving spyware have generated an entire new industry devoted to foiling spyware and adware programs. Spyware has been used to steal identity information and credit card numbers.

50. Fraud Identifier: IP – Pharming Fraud

Definition

Pharming is an attack on a computer or handset with the intent of redirecting a website's traffic to another, bogus website. Pharming may be the result of a malicious change to the **hosts** file on a victim’s computer, or by the attack of a vulnerable **DNS server**.

Description

The most common places for pharming attacks are within a computer’s hosts file. The hosts file avoids website name lookup with its own local name to IP address mapping. Once changed via the attack, a legitimate request for a sensitive website can direct the user to a fraudulent copy. Personal computers are often better targets for pharming because they receive poorer administration than most internet servers.

Local network routers may also be attacked by pharming malware. Since the router typically serves many devices, this is cause for more serious concern. Many routers specify a trusted DNS to users as they join the network, therefore a redirection of IP destination here will affect all users within the LAN. Router compromise is more difficult to detect. Routers can pass bad DNS information in two ways: Malconfiguration of existing settings or complete rewrite of firmware. Nearly every router allows its administrator to specify a particular trusted DNS in place of the one suggested by an upstream location (e.g., the service provider). A pharming attack could specify access of

a DNS server under the attacker's control instead of a legitimate one. All subsequent name resolutions will go through the bad server.

Additionally, many routers allow the replacement of their firmware. This is common in upgrade scenarios. Firmware replacement can be very difficult to detect – good implementations of pharming malware will appear to behave the same as the manufacturer's firmware: Settings, administration menus, page look and feel, etc., will appear the same.

51. Fraud Identifier: IP – Online Brand Threats Fraud

Definition

Online Brand Threat fraud occurs when a specific brand is counterfeited and offered for sale as the genuine product. Several forms of online brand threats exist; not all are fraudulent, and are described in more detail below.

Description

Online Brand Theft fraud is most commonly a deliberate attempt to either sell a counterfeit product under the guise as genuine, or to otherwise falsely damage the reputation of the product for some financial gain (e.g., a competitor). In some cases, competitors have virtually "cut and paste" product claims into their own materials and web sites, even though there is no basis in fact in their claims. The illegality of this "cut and paste" practice is still in question in many jurisdictions, however.

Specific examples of online brand threats (not necessarily fraudulent) include:

1. Counterfeit Product: To take advantage of a market-leading brand, counterfeit products are introduced and sold as the genuine product. These counterfeits will look virtually identical, and not only will harm the sales of the original product, but also may cause brand dissatisfaction and poor brand perception should they not offer the same quality and reliability of the genuine product.
2. Consumer Complaint sites: These sites are often formed by disgruntled or otherwise unhappy customers of the target product and company. This typically invites other readers to share similar experiences, and often these sites lead to warnings about purchasing the product. This frequently results in loss of revenues, and even loss of customers.
3. Competition: Unethical competition often appears as the introduction of negative publicity and comment (often inaccurate), and usually via the unregulated channels of online blogs and customer complaint sites.
4. Social Networking: These sites are also mostly unregulated, and offer competition and others a chance to promote negative publicity around a product, brand, or company.

52. Fraud Identifier: Interconnect (IXC) – Arbitrage Fraud

Definition

Arbitrage Fraud is defined as the routing of traffic via other carriers and/or countries to take advantage of differences in settlement rates.

Description

Arbitrage is the practice of routing traffic via an intermediate carrier or country to take advantage of the differences in settlement rates. If carrier B has much lower settlement rates with carrier C than with carrier A, it might be cheaper for originating carrier A to send its traffic destined for carrier B *via* carrier C. While this may be considered good business practice, in reality it is often in direct contractual violation with the terminating carrier and/or the international traffic regulations as established by the terminating country.

One of the first larger arbitrage routes was for traffic between Australia and the US, which was cheaper if sent via New Zealand and Canada. Other arbitrage strategies have included telecommunications companies allowing their customers to make international calls without paying long-distance charges by dialing certain access numbers. The companies engaged in this arbitrage are paid an interconnect fee by the network operator, and then typically use part or most of this fee to buy additional international calling routes at low prices.

53. Fraud Identifier: Interconnect (IXC) – Call Looping Fraud

Definition

Call Looping Fraud is defined as the practice of disguising originating call numbers from the terminating carrier, such that billable call activity is unrecognized, and thus unbilled.

Description

Looping is a method in which fraudsters circumvent controls in telecom networks to avoid detection of their origination number. Looping may be accomplished by using any of several types of devices, such as a Private Branch Exchanges (PBXs), cellular phones or telephones that are call forwarded to an access number. These devices are all capable of originating a second call while keeping a first call on the line. The call looping perpetrators may loop calls through one carrier, or they may loop calls through multiple carriers. The final result is to bypass the control(s) that would normally identify the origination point of the call.

In a typical looping activity, the originating caller places a first call to an intermediate party in order to avoid controls established by the carrier to protect against fraudulent calls from the originating caller to the terminating party. The intermediate party includes a call-origination device, such as a private branch exchange (PBX), a cell phone service or a call forwarding telephone. If the originating caller can access the call-origination device of the intermediate party the originating caller can place a second call on the call-origination device to the terminating party while staying on the first call.

In international or other interconnect (long distance) scenarios, call looping fraud (when successful) makes the originating call appear as a local (in region) call, thus not billable as a toll call to the originating caller.

54. Fraud Identifier: Interconnect (IXC) – QoS (Quality of Service) Exploitation Fraud

Definition

Quality of Service (QoS) refers to the probability of the telecommunication network meeting a given traffic contract. Fraud in this case exists when the contracted QoS is deliberately not delivered by the interconnect operator.

Description

While several abstract definitions exist in the market today for Interconnect Quality of Service (QoS) Exploitation fraud, the primary focus of this fraud is the deliberate degradation of promised service levels (by the contracted operator network), typical in favor of other, higher revenue traffic.

Within unhealthy or poor performing networks, quality of service (QoS) management is ineffective in managing degradation issues. On a strong performing network, QoS is employed to help forecast growth, but otherwise not needed to alert for poor performance. Strong networks are able to adequately supply sufficient resources to all applications, allowing them to perform properly.

When network resources are scarce and demand is increasing beyond network capacity, QoS exploitation occurs most commonly when the operator begins to prioritize certain services, which will inevitably be at the cost of other services. Those "higher priority" typically are generating the highest amount of revenue. The fraud occurs as a result of the deliberate (and unannounced) decrease on QoS on those lower revenue carriers.

55. Fraud Identifier: Interconnect (IXC) – Technical Configuration Fraud

Definition

Technical Configuration fraud is a form of internal fraud that involves the configuration of (interconnect) routes, rate sheets, or other factors that will move traffic over more expensive and/or non-contracted paths.

Description

Interconnect routing is a complex set of processes designed to route traffic through the best interconnect partner. The "best" partner may be determined by price, time of day, quality of service, quantity of traffic, contracted volume agreements, or a blending of any of those factors. Depending on volume, more than one carrier may be selected for a

specific route or set of routes, with traffic priorities assigned as “most favored” routing, and on downward, resulting in the most effective routing costs and call quality for the operator’s customer.

In cases of Technical Configuration fraud, the internal fraudster has altered the routing configuration to favor a specific interconnect carrier’s routes, outside of agreed and expected parameters. While this will typically benefit the fraudster financially (rewarded by the carrier receiving the fraudulent traffic configurations), it may also have a negative impact in terms of penalties and losses incurred by the home operator, should an audit reveal traffic routing outside of contracted agreement.

56. Fraud Identifier: SMS Fraud

Definition
SMS Fraud generally consists of SMS message traffic being initiated that is either unbillable (the originator of the SMS is unidentifiable - technical, spoofing, or signaling fraud), and/or causes adverse effects to networks and recipients (e.g., malware delivery, spamming, etc.).

Description

SMS fraudulent activity can manifest as any combination of the defined tactics. In frauds where the originator is unbillable, weaknesses in the networks (SS7, IP, SMSC, etc.) to either block or properly identify the originator is exploited. All originating SMS traffic is handled by the home network of the originator, even if roaming (except in the case of open SMSC platforms on network where the message is being originated). SMS traffic is sent directly to the home SMSC via SS7 (or IP, in Valued Added Service Provider cases), and message signaling is either manipulated to appear as a roaming subscriber, or to “trick” the SMSC into believing the subscriber is someone else (a legitimate customer), and actually registered within the home network. In either of these cases, billable events are either unable to be attached to a customer, or an unsuspecting (uninvolved) customer is incorrectly billed.

Malware attacks via SMS occur when embedded software within an SMS event is inadvertently downloaded and/or activated by the receiving subscriber(s). These malware programs may generate enormous amounts of outbound traffic from those subscribers, collect and transfer personal information, generate automated PRS activity, and other unwanted effects. Malware attacks also have the capability of creating DoS (denial of service) situations due to significantly increased network activity they generate.

SMS **Spamming (flooding)** is also becoming a prevalent method in which fraudsters (often using spoofed or masked identities) will generate messaging to a significant number of subscribers. Quite frequently the message will contain a web link, a promise of a gift or reward for calling a number, or other advertising tactics to generate a response from the recipient. As with malware transmittals, network DoS is a significant risk with SMS flooding.

In most (if not all) cases of spamming, flooding, and malware transmittals, **Global Titling** (GT) attacks may have been used by fraudsters to query the home network for subscriber

location and identification information; this information will then be used to target recipients with these messages.

Detection Method(s)

Large message volumes from single subscribers (or groups of subscribers) should be closely scrutinized. Probing may also be employed to scan messages for unwanted content (web site information, etc.).

Corrective Action(s)
A key component to all actions to correct and protect against SMS fraud is to properly install and configure SMSC platforms with strong messaging subscriber identification protocols, and to protect against unauthorized signaling query attacks. Messaging from unrecognized subscribers should be rejected in all cases.

57. Fraud Identifier: SMS Faking.

Definition

A fake SMS is originated from the international C7 Network and is terminated to a mobile network. This is a specific case when SCCP or MAP addresses are manipulated. The SCCP or MAP originator (for example: SMSC Global Title, or A_MSISDN) is wrong or is taken from a valid originator.

Description

The delivery of a Mobile Terminated SM is in two parts:

A. The SMS-C uses the destination MSISDN to address a MAP message <Send Routing Information for Short Message>, to the Home Location Register (HLR) for that customer to find out whether the MSISDN is valid, can receive SMS, and if so, to determine the current switch (MSC) that the destination user is registered on. The HLR responds to the SMS-C with the information.

B. The SMS-C sends the actual text of the SM to the currently registered MSC and a MAP message <Forward Short Message>. The MSC responds to confirm the message was delivered, and generates a CDR containing all relevant information including the SMS-C address.

In the faking case, the first part is done exactly as described above. However, the second part is changed so that the source address in the MAP message <Forward Short Message> is changed, often to someone else's SMS-C address. The manipulation of the SMS-C address causes any inter-PLMN SM accounting to be in error, and means that any policing against the apparent Spam generator harms innocent parties and is ineffective against the real Spam generator.

The faking of the source address in the SCCP called party Global Title and the Service Centre Address in the MAP message <Forward Short Message> whilst having the

correct equivalent address in the MAP message <Send Routing Information for Short Message> is impossible without considerable efforts by the technical staff running the SMS-C. In other words, it does not happen either by accident, faulty configuration data or as the result of raw text messages received from the Internet. It happens because in most cases it requires a software patch on the SMS-C. Therefore; any instances of this happening are as the result of direct action by SMS-C staff, and probably in conjunction with assistance from the staff of the Associated PLMN.

58. Fraud Identifier: SMS Global Title Scanning

Definition

A Global Title is an address used in the SCCP protocol for routing signaling messages on telecommunications networks. In theory, a global title is a unique address which refers to only one destination, though in practice destinations can change over time. The Global Title Scanning is the fact to send SMS MO to all Global Title address from one mobile operator in order to find unsecured SMS-C (SMS-C that are not controlling the A number).

Description

The Technical Aspect of Global Title Scanning is:

- Multiple SMS Forward SM Submits are received, generally, from the same mobile MSISDN with the Called SCCP Address and Service Centre Address incremented on each attempt. It would appear that individuals using a mobile with a computer connection are instigating these scans.
- The easiest of these scans to spot are sequential in nature scanning 10,000 GT at a time. It has also been seen randomized scans, though on sorting the data it is clear that blocks are being scanned.
- This type of messaging is picked up in normal statistics in monitoring expected and unexpected combinations of direction, GT and message type.
- There can be no valid reason for such scanning of networks other than locating unsecured SMSC. With simpler computer integration with mobiles and SMS emulation software readily available this type of activity is likely only to increase. It would be desirable for such activities to be reported to the Home PLMN of the originating MSISDN in order to have the service removed.

59. Fraud Identifier: SMS Open SMSC

Definition

Open SMSCs are SMSCs that do not validate the sending subscriber that attempts to use them to deliver messages. Generally each operator configures their SMSC to reject messages from subscribers other than their own.

Description

Fraudsters may first attempt to locate open SMSCs by performing GT Scanning (also called SMSC sniffing), where multiple MO messages are sent trying to find an unsecured SMSCs. When the fraudster locates an open SMSC and then sends an MO message by changing the SMSC address on their device, it will travel to this open SMSC and be delivered via it.

60. Fraud Identifier: Pre-paid – PIN Theft

Definition

Any activity which allows use of an active PIN without paying the legitimate amount is PIN theft. This can be recharging of the services by the end user or retailing and distribution by the sales houses without paying the legitimate amount.

Description

PIN generation process is a much secured process and the systems involved are absolutely non-intrusive. The process involves generation of PINs, distribution of newly generated active PINs for voucher printing and finally selling the printed vouchers with active PINs through the chain of distributors and retailers to end users. The entire process is very vulnerable to theft. Active PINs can be stolen and used even before printing of the vouchers or can also be stolen during the voucher printing causing end user to suffer who has paid the legitimate amount only to get used PIN. PIN theft can be as simple as smart thieves look over the shoulder of original buyer while he is trying to recharge and use the PIN even before he is able to recharge.

PIN theft can be an isolated incident of stealing PIN number from an original buyer or can be an organized crime of stealing active PINs involving someone from PIN generation team or from vendors involved in voucher printing.

61. Fraud Identifier: Pre-paid – PIN Guessing

Definition

PIN guessing is essentially an act of guessing the PIN by trial and error, intelligence or by use technology either with partial information about PIN or its generation process.

Description

Knowledge about the PIN generation process or PIN as such lead to incidents of PIN guessing. In this case a fraudster with partial information about an active PIN may guess the remaining numbers and use the PIN before legitimate buyer can use it. These incidents can be isolated done by a novice, can be an act of organized crime where someone has leaked the information about PIN generation algorithm or an act of software hackers who may not be interested in making money but would break the system out of curiosity causing damage to the operators.

62. Fraud Identifier: Pre-paid – Stolen Voucher

Definition

This is specific case of PIN theft where printed vouchers with active PIN are stolen from anywhere in chain after voucher printing. It can be from printing press, distributors, and retailers or from the consumers.

Description

This is an act of direct stealing, where printed vouchers with active PIN get stolen either from the consumer or in the distribution chain. Thief in this case may use the voucher for subscribing to the services himself or resell it at same or lower cost to make money out of it. This can be an isolated incident where a thief steals voucher from retailer or consumer or it can be an organized crime where entire lot/series of voucher gets stolen from warehouse or from distributors.

63. Fraud Identifier: Pre-paid – Altering Free Call Lists

Definition

In this case user is allowed to make calls without being charged for it. This can be done by intruding the system with false information.

Description

There is a list which contains all MSISDNs/Phone numbers which are allowed to make free calls. These are usually numbers of staff, government personals and VVIPs to which operator has given this facility. Now someone who has/gets access to this list can alter it by adding self/family/friends phone number to the list thereby allowing them to make free

calls. As evident in the description this cannot be done without help of someone part of the operator who can get access to this list.

64. Fraud Identifier: Pre-paid – Manual Recharges

Definition

Act of manually giving credit to a subscriber without any legitimate case for the subscriber to get manual credit.

Description

There is a process by which customers are given manual credits with legitimate cases coming from customer care, customer grievance redressal cell, loyalty management systems etc. This is manually done by editing the account balance information of the customer. This leaves a possibility of fraud where a person involved or someone getting access to the system can manually grant credit to self/friends/family without a legitimate case enabling them to abuse the services. This is a kind of internal fraud.

65. Fraud Identifier: Pre-paid – Voucher Modification

Definition

Act of tampering the voucher by changing voucher denomination is voucher modification.

Description

Fraudsters modify the amount or duration or both denominated on vouchers to sell it at a higher amount than stipulated amount. It is the end user who suffers by paying more or not getting the requisite service, however this type of fraud impacts the reputation of the service provider as well. Fraudsters usually attach service providers in a planned manner by picking up the weak points in the vouchers. By the time it comes to the notice of the service provider this incurs huge loss in terms of customer grievances and dissatisfaction.

66. Fraud Identifier: Pre-paid – Duplicate Voucher Printing

Definition

Act of duplicating the vouchers with same PIN while printing with an intention of making more money is duplicate voucher printing fraud.

Description

Enterprise partners or someone internal is responsible for allowing/getting duplicate vouchers printed with same PIN on it. These vouchers are then sold in the market

through different channels. The user who consumes the PIN first gets the service and rest all suffer loss. This is an organized crime with involvement of staff or people from wholesale partners. Customers complain are often isolated and by the time fraud gets identified fraudster have already made huge money and escaped.

67. Fraud Identifier: Pre-paid – Fraudulent Voucher Reading

Definition

Act of using technology to smartly read the PIN information from a voucher without the knowledge of the user who has bought the voucher.

Description

Fraudster indulge in this activity use smart devices from magnifying glass to card readers to cameras to read PIN information while voucher is still in the pocket or wallet or while someone is trying to recharge. This is mostly an act of an individual who mostly tries to benefit himself or sell the stolen PIN to make money. They keep on inventing/learning new techniques to read the voucher information. This type of fraud mostly prevalent with credit cards and from there also has started impacting the prepaid vouchers.

68. Fraud Identifier: Pre-paid – Illegal Credit Card Use for Recharges

Definition

Act of using a credit card to pay for recharges without the authorization of the legitimate card owner. The user fraudulently impersonates the genuine account holder.

Description

Stolen credit card data, account numbers and expiry dates are readily obtained by corruption of hotel staff, restaurants, banks and almost anywhere cards are used. Stolen cards are easily used at point of sales having no on-line card verification. Even with on-line card verification the card may be freely used until the theft is reported to the card center and the card is blacklisted. Fraudsters make use of these gaps to recharge the services and abuse it till the time it really reported, investigated and identified. Usually before being identified or any action can be taken they use the amount and escape.

69. Fraud Identifier: Pre-paid – IVR Abuse/Hacking

Definition

Acts of abusing the IVR in order to recharge more than one account using the same voucher number, modifying the voucher status in order that it may be reused, and altering the PIN value.

Description

IVR abuse/hacking can be both internal and external. Internally a staff can modify the voucher status, its PIN value in the IVR system making it allowing for repeated recharge from same voucher or higher amount recharge than legitimate amount. Externally IVR system can be hacked to make changes in the voucher statuses or PIN recharge amounts. IVR systems can also be attached with simultaneous calls making it break or perform abruptly.. Hackers and technology enthusiast are often involved in these activities and take proud in breaking the established systems. Intention may or may not be to make money.

70. Fraud Identifier: Pre-Paid – IN Flag Modifications

Definition

Tampering the IN flags with an intention to abuse or benefit self/family/friends is IN flag modification fraud.

Description

All HLRs has a IN flag for services and rates to which any pre-paid subscriber the legitimately subscribed to. Charging from customer account happens based on these flags. Someone internal with an intension to abuse or benefit someone may temper with these flags. The impacted subscriber will continue to suffer the loss unless it comes to notice and then notified with the service operator and in case of someone getting benefited it remains unnoticed unless it is caught by some intelligent tool or during profile reconciliation or analysis.

Manual removal of the IN flag manually on the HLR or using a billing system specific command. Staff in collusion possibly in collusion with third parties, decide to remove prepaid flags to provide family, friends or criminals (supporting call selling operations) free prepaid calls.

71. Fraud Identifier: Pre-paid – Handset Manipulation

Definition

The manipulation of a handset to obtain information in engineering mode or to create an additional identity duplicating the original and the subsequent use of services provisioned to the original.

Description

Modifying the handset information like IMEI numbers or clone it so that it gets undetected and then using it for illegal purposes. Fraudsters set up and advertise a call selling service and route these calls through fraudulently obtained, cloned, or stolen handsets increasing the revenue share before network detection.

Fraudster configures false base station to look like the network they intend to attack. Network parameter/settings can be obtained from simple analysis of the surrounding base stations using test equipment or a handset in engineering mode.

72. Fraud Identifier: Pre-paid Handset Installment

Definition

Act of not paying the installment for handset either by escaping or reporting loss of the handset and later selling the handset or manipulating it for other purposes.

Description

Buying a handset on installment and not paying the installment either reporting loss of handset or escaping. Main intention behind this fraud is to sell the handset and make money or indulge in a bigger crime by manipulating the handset. This is a rare case of fraud in pre-paid services as handsets on installment are now not usually offered with prepaid services.

73. Fraud Identifier: Pre-paid Roaming

Definition

Act of making use of gaps of delays in accounting while roaming to use services with intension of not paying

Description

With the advancement of technology this no more exists, however roaming fraud still prevalent in case of post paid subscription. The basis lies in the fact that there is delay in getting the call/usage information from roaming partners. Fraudsters indulge in this kind

of frauds take benefit of this gap and then escape. By the time service provider gets to know about the usage it is already late. Nowadays, technology has completely prevented this fraud in case of pre-paid subscription and also to a large extent it has been prevented in postpaid as well with use of NRTRDE.

74. Fraud Identifier: TARGET FRAMEWORK

Definition
TBD

Description
TBD

Detection Method(s)
TBD

Investigation Process(es)
TBD

Determination Criteria
TBD

Corrective Action(s)
TBD

Additional Reference(s)

Administrative Appendix

This Appendix provides additional background material about the TM Forum and this document.

1.1 About this document

This is a TM Forum Guidebook. The guidebook format is used when:

- The document lays out a 'core' part of TM Forum's approach to automating business processes. Such guidebooks would include the Telecom Operations Map and the Technology Integration Map, but not the detailed specifications that are developed in support of the approach.
- Information about TM Forum policy, or goals or programs is provided, such as the Strategic Plan or Operating Plan.
- Information about the marketplace is provided, as in the report on the size of the OSS market.

1.2. Document History

1.2.1. Version History

Version Number	Date Modified	Modified by:	Description of changes
Version 1.0	17-OCT-2011	JohnBrooks	Team Vote
Version 1.1	19-OCT-2011	Alicja Kawecki	Minor cosmetic and formatting corrections prior to web posting and ME
Version 1.2	7-MAY-2012	Alicja Kawecki	Updated to reflect TM Forum Approved status
Version 2.0 (draft)	23-SEP-2012	José Sobreira Raul Azevedo	New chapter for the Fraud Classification Model (for member review)
Version 2.0	14-OCT-2012	José Sobreira Raul Azevedo	New chapter for the Fraud Classification Model
Version 2.1	7-NOV-2012	Alicja Kawecki	Minor style, formatting edits prior to posting

			and Member Evaluation
Version 2.2	18-MAR-2013	Raul Azevedo	Comments incorporated from Member Evaluation

1.2.2. Release History

Release Number	Date Modified	Modified by:	Description of changes
1.0	17-OCT02911	JohnBrooks	Release to Member Evaluation
2.0 (draft)	23-SEP-2012	José Sobreira Raul Azevedo	Release to team evaluation
2.0	14-OCT-2012	José Sobreira Raul Azevedo	Release after team evaluation

1.3. Acknowledgments

The following people and organizations have contributed considerable time and energy to the creation of this document. Their knowledge and insight have been instrumental in ensuring this document contains relevant, high quality information, and I would like to thank them for their commitment.

Version 1.0
John Brooks, Fraud Team Leader, Classification Guide Contributing Editor

Contributor	Organization
Mohamad Mohamad Zain	Telecom Malaysia
Amiruddin Hussin	Telecom Malaysia
Fernando Soto	CanTV
Vinoo Jacob	Vector Communications
Abhishek Sinha	Connectiva Systems
Tal Eisner	cVidya Networks

Version 2.0
José Sobreira, Fraud Classification Guide Contributing Editor, Optimus
Raul Azevedo, Fraud Classification Guide Contributing Editor, Fraud Team Leader, WeDo Technologies

Contributor / Reviewers	Organization
Krista Saarinen	Rogers Canada
Santhosh Gopalan	Du

Gabriela Sobral Gil	Telefonica Internacional
Cristian Vesperinas	Telefonica
Durbinth Pacheco	Telefonica
Tal Eisner (Fraud Team Leader)	cVidya Networks