Fraud Management Systems in Telecommunications: a practical approach

Luis Cortesão
PT Inovação, R. Eng. José Ferreira Pinto Basto 3810 -106 Aveiro, Portugal
Phone: +351-234403510, Fax: +351-234420722, e-mail: lcorte@ptinovacao.pt

Filipe Martins
Telbit – Tecnologias de Informação, R. Banda da Amizade, 3810-059 Aveiro, Portugal
Phone: +351-234425095, Fax: +351-234425098, e-mail: fmartins@telbit.pt

António Rosa
TMN, Av. Álvaro Pais 2, 1649-041 Lisboa, Portugal
Phone: +351-7914918, Fax: +351-7914404, e-mail: antonio.rosa@tmn.pt

Pedro Carvalho
PT Inovação, R. Eng. José Ferreira Pinto Basto 3810 -106 Aveiro, Portugal
Phone: +351-234403481, Fax: +351-234420722, e-mail: pcarv@ptinovacao.pt

***Abstract* — Telecommunications fraud is a problem that affects all operators and is an important factor in their annual revenue losses. Aside from financial impact, it also constrains new service deployment and may contribute to adverse costumer perception and, consequently, churn increase. This paper generically presents the most relevant types of fraud in telecommunication services and how the usage of a process adapted and technology up-to-date Fraud Management System is crucial in reducing the impact of fraud into the telecommunication operators business.**

I. INTRODUCTION

In today's competitive market, shareholders have been placing great pressure on telecommunication operators to obtain larger profits, increase efficiency and simultaneously reduce costs. Unfortunately, for many operators that have reached the mature phase of their business cycle, the possibility of increasing profits by raising market share is increasingly difficult. Higher profits can more easily be obtained by maximizing efficiency and introducing new services in their already installed infrastructure, through an increase in traffic and other service revenue sources, reduction of costs and elimination of losses. With this in mind, one important factor that should always be identified as a source of revenue loss is fraud.

Several international organizations have estimated that fraud may affect between 3% and 6% of an operator's gross revenue. Having an efficient fraud management system may help reduce those values by contributing directly to the detection and resulting reduction of bad debt and fraudulent service usage.

This paper starts by generically describing common fraud types and Fraud Management Systems most common features. It then describes the "Centaur FMS" general architecture and specific detection tools and how they may be used in some specific fraud detection scenarios. It concludes by referring some future perspectives in fraud detection.

II. FRAUD

Fraud in telecommunications can be very complex and transversal to the operator structure. The authors propose a classification method used in the FMS case management that allows a better characterization of the fraud phenomenon and enables a detailed reporting. The approach used is based in the 3M's classification:

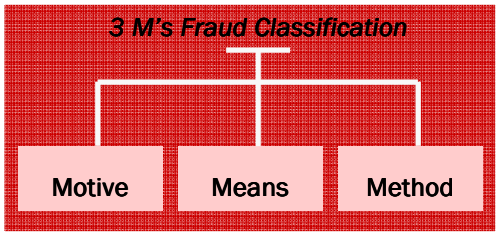

Fig. 1. 3 M's fraud classification

Motive: the fundamental objective of the fraud.

1. *Non-revenue fraud,* making use of a service with intent to avoid the cost but without the intention of making money. It includes providing no-cost services to friends or private usage.
2. *Revenue fraud,* which intends financial benefits as in Call Selling or Premium Rate Service (PRS) fraud (described below).

Means: the nature or form of the fraud used to satisfy the motive. Some examples:

1. *Call Selling*: sale of high tariff calls – usually international – bellow their market value with the intent to evade the operator payment.
2. *Premium Rate Services (PRS) Fraud*: inflation of the revenue payable to a Service Provider by generating calls to a PRS line.
3. *Surfing:* use of other person's service without consent which can be achieved, for example, through SIM card duplication (cloning), illegally obtaining calling card authorisation details or PBX hacking.

4. *Ghosting:* refers to obtaining free or cheap rate through technical means of deceiving the network. It can be performed, for example, by manipulating switch or database contents to 'alter' call records.
5. *Sensitive information disclosure* - involves obtaining valuable information (e.g. VIP client details or access codes) and selling it to external entities. This fraud is usually performed internally.
6. *Content stealing*: a more recent type of fraud, which deals with getting high value contents (videos, ring tones, games) for free, by exploiting the non real-time pre-paid billing pre-paid system (hot-billing) or by avoiding payment of the invoice (post-paid services).

Method: the generic fraud method.

1. *Subscription*: fraudulent subscription obtained with false credentials that allow debt accumulation by systematic payment avoidance.
2. *Technical:* more advanced fraud that is based in exploiting loopholes found in the operator network elements or platforms.
3. *Internal:* inside information systems abuse
4. *Point of Sale*: when the dealer manipulates sales figures to increase the compensations paid by the operator

III. Fraud Management Systems Overview

As previously stated, fraud analysts tasks clearly benefit from using a Fraud Management Systems (FMS), whose main architectural components are illustrated in Fig. 2.

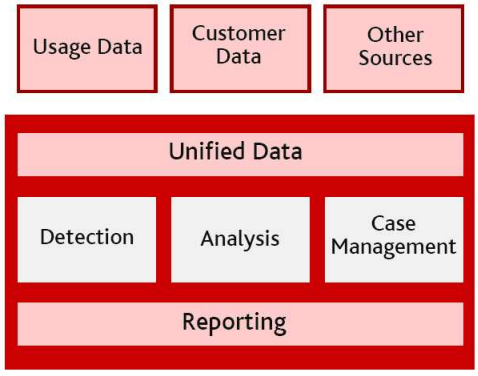

Fig. 2. FMS generic architecture.

A FMS should be able to collect data from multiple formats and sources, and through a process of data preparation and mediation, conveniently process and adapt it to the system internal data formats. Some of the relevant processes of this stage are data filtering, call assembly and call rating. With some FMS tools, it is possible to perform data enhancement through cross-relation of different data sources, which may boost performance in some more complex detection techniques.

Subsequently, detection processes are applied in order to generate alerts on situations that deserve closer investigation by fraud analysts. Some of the relevant techniques used in this stage are rule–based detection and profiling through Artificial Intelligence (AI) techniques like neural networks or decision trees.

Fraud analysts investigate alerts by accessing all relevant information (detailed client/account information, associated Call Detail Records, alert details, client alert history…) needed to conveniently assess the alert. Alert clarification may also benefit from graphic information describing client consumption profile.

Detected fraud cases are then forward to a case manager to initiate subjacent bureaucratic processes subsequent to fraud identification. All relevant information (e.g., CDR details, detailed client information, related alerts…) is attached to the case and the specific case fraud is classified (involved services and fraud motives, means and methods) along with financial indicators quantifying performed fraud detection gains against fraud losses.

Finally, the system must provide friendly and complete reporting tools, thus allowing access to all relevant information to analyst, fraud process manager and system management information.

Fraud tackling efficiency may also benefit from seamlessly integrating and cross-referencing multiple data sources (client and billing information), which may enable focusing on most suspicious alerts.

Versatility and adaptability of fraudsters imply usage of different tools and technologies for each scenario. These tools must handle huge data volumes (e.g., billions of call records) and allow the integration of any new relevant technology. Additionally, the regular advent and new services and client growth implies easily scalable tools.

IV. Centaur FMS Overview

Centaur is a newly developed FMS whose main focuses are flexibility, adaptability and integration. It has a plug & play architecture that allows its administrator to activate or deactivate any of its features. This plug & play architecture is crucial for the integration of newly developed detection and analysis techniques that may be required for emerging fraud scenarios.

Centaur has a context-based approach for the detection of fraud. Contexts are entities that can be used as detection targets, i.e.: MSISDN (Mobile Subscriber ISDN), accounts, network cell, handset, IMEI (International Mobile Equipment Identity), IP address, etc.

These contexts are also used in the definition of Lists used to store groups of elements with common features. Most usual lists are, e.g., Hot Destinations, Blacklisted Handsets, Safe Accounts, Suspicious Cards or Suspicious Cells.

A List can be associated with Multipliers. Multipliers are used to increase or decrease thresholds for the elements of the List in specific detection processes.

The most common detection processes tend to consider the behaviour of the chosen context over a specific time period. This time period is called time-window and each detection

process can be associated with several time-windows. For instance a Many Short Calls alert can be issued over an hourly, daily or weekly time window.

One common and flexible detection process is rule-based processes created by the analyst using a wizard. The analyst can choose the context, the record characteristics he wants to analyze, over which time window and when should an alert be issued.

More advanced detection processes, that take advantage of neural networks and decision trees are also available. These processes can be used to create client profiles. When a client profile deviation is detected an alert may be issued. Another useful detection process uses known fraudster profiles to encounter new "instances" under a different number.

V. FRAUD MANAGEMENT WITH CENTAUR FMS

A. Call Selling Operation

In simple terms, Call Sell Operation (CSO) is the sale of high tariff calls (usually international) below their market value. Usually, the fraudster uses counterfeit documents to apply for services in order to escape the payment and subsequent identification.

Centaur FMS considers several inputs - e.g. existing Call Data Records (CDR), customer details, high risk destinations list, etc - to detect this type of fraud.

For each defined time window, Centaur groups CDRs by client/account and, whenever the defined thresholds are breached, an alert is launched. The most common thresholds considered are cumulative amount, cumulative duration, number of calls, number of distinct country destinations, number of international calls, and client/account age.

The investigation stage of this kind of fraud is relatively expedite as the most common criteria are client antiquity, how much was spent and how much was already paid.
When in doubt, the analyst can automatically schedule and send a letter to the possible fraudster, asking him to pay in advance a specific amount. If the client fails to comply it is considered to be a fraud case that has been detected before full damage could be done.

B. Cloning

GSM mobile phones acquire their personality from a smart card known as the Subscriber Identity Module (SIM). All the access rights (including identification for billing) are based on the SIM, rather than the mobile phone itself.

GSM cloning refers to a process in which an attacker obtains sufficient information to clone the SIM of a GSM mobile phone. The aim of GSM cloning is to produce multiple copies of a SIM and defraud a network operator.

Independent tests have questioned the strength of GSM's security mechanisms aimed at preventing cloning, particularly if the attacker has physical access to the SIM.

As shown in Fig.3, it is quite easy to build a GSM Card Reader, and subsequently, clone it.

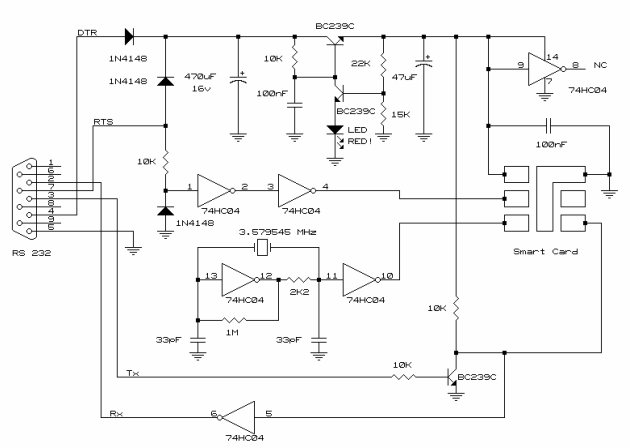

Fig. 3. GSM Card Reader

To detect cloning, Centaur FMS uses several different techniques, namely call collision, call velocity and customer profile deviation.

A call collision alert is issued whenever two or more calls overlap for more than a specified amount of time. A call velocity alert is issued whenever two or more calls are made from different locations but the average time to travel between those locations is higher than the time elapsed between those calls. A customer profile deviation alert is issued whenever a substantial call pattern deviation occurs.

When these alerts occur, Centaur correlates them and presents a consistent scenario indicating a possible cloning case to the fraud analyst.

If a positive case is detected, the analyst initiates several actions: notify the user that he needs a new SIM; block the cloned SIM in the Home Location Register (HLR); notify billing system for bill scrubbing (only if the user is completely innocent) and register the fraudulent profile for future detection.

C. GSM Gateway Fraud

GSM Gateway Fraud occurs when call resellers use GSM Gateway devices to transform interconnect (off-net) calls to "mobile-to-mobile" on-net calls (Fig.4). This way, traffic delivered to GSM operators by unlicensed carriers is billed as on-net rather than interconnect traffic. GSM operators only receive the value of on-network calls and do not receive the interconnect fee for call termination, which may produce substantial revenue loss. Besides the financial losses, there is an important QoS degradation due to the use of the GSM Gateways (e.g. radio spectrum congestion, jitter, CLI override, increased call drops, etc)

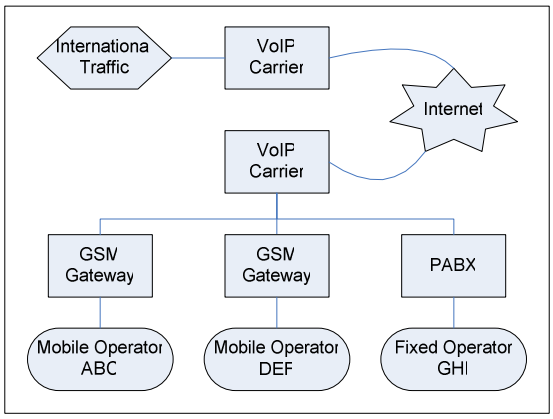

Fig. 4 .GSM Gateway fraud.

GSM Gateway Fraud requires a very small investment. Any private or corporate subscribers can do it with inexpensive and easy-to-use devices. The very low set-up costs permit it to be deployed almost anywhere, from small village communities to large corporate accounts.

Centaur FMS detects GSM Interconnect Fraud by correlating several different data: call ratios, constant activity indicator and very high usage of low profile accounts.

Whenever some or all of these alerts occur, the fraud analyst has the possibility to create a new case and, if appropriate, instruct the authorities to investigate the suspected client/account. If the case is classified as fraud, the call pattern from the fraudster is be used to train other Centaur FMS detection mechanism based on neural networks and decision trees, which may expedite future GSM interconnect fraud detection.

D. Voucher Fraud

In prepaid SIM cards where there is no contract between the operator and the client, the prepaid subscriber has to purchase airtime credit prior to use. One way of crediting prepaid SIMs is through airtime vouchers. These vouchers are pieces of paper with a code that is covered and must be scratched with a coin to be revealed. Once exposed, the code is punched into the keypad of the cell phone crediting up the prepaid SIM card with the vouchers amount.

Fig. 5. GSM Recharge voucher

In operators that use this kind of recharge method, the most common prepaid frauds are forgery or re-usage of recharge vouchers. In the first case, a fraudster tries to guess voucher codes by submitting random codes. On the second case, valid but already used codes are resubmitted.

Most of these unsuccessful attempts don't really affect the company, but continuous fraudulent recharge attempts increase the system load and overall operational costs.

If a fraudulent recharge really occurs, Centaur can detect it by analyzing the customer recharge attempt history and profile. When a successful recharge occurs after a long period of several different codes customer tries, the fraud analyst is notified and can take actions to prevent further losses.

VI. PERSPECTIVES

Fraud and legitimate behaviour are constantly changing and FMS systems should incorporate technologies capable of evolving or quickly apprehend those changes.

Although fraud cases differ greatly from each other, the accumulated experience in their detection and investigation is essential to prevent future occurrences.

With difficult to formalize models, as is the case of fraud, the usage of casuistic techniques like Case Based Reasoning (CBR) may prove a valuable approach in finding the correct output (fraud or non-fraud) and appropriate subsequent intervention methods. CBR is particularly adequate to create and manage a knowledge base that stores corporate experience in fraud management. Implementing this technique will clearly benefit the capacity of an FMS, as CBR ability to model exceptions is particularly adapted to the detection of new emerging types of fraud.

Usage of agent technology may also enable some breakthroughs in fraud detection as it permits the design of solutions made of multiple agents embodying different fraud detection tasks (e.g., pattern analysts, correlation searchers monitors of behaviour changes …) that cooperate with human analysts. This technology is quite powerful as specific agent functionalities may be adapted to better tackle fraud behaviour perceived changes. Additionally, newly developed detection technologies are seamlessly incorporated in the FMS by simply adding adequately developed agents.

VII. CONCLUSION

The impact of fraud in operator revenue justifies the introduction and consolidation of fraud detection processes performed by highly experienced fraud analysts.

These experts should be permanently aware of current fraud types and methods, and how to implement the appropriate detection techniques.

As presented, the usage of a flexible FMS enhances fraud detection processes and enables the articulation of multiple detection techniques. It also allows analysts easy information cross-referencing in the investigation stage and expedite subsequent procedures with a process adapted case manager.

Client dynamic behaviour obliges to constantly monitor changes in fraud and particularly assess new fraud opportunities when introducing new services.

It is crucial to permanently adapt current FMS detection techniques (e.g. adapt rules and thresholds or train neural networks and decision trees with new fraud behaviours) and

introduce new ones more capable of stopping emerging fraud types, enabling an increased efficiency in the detection processes.

REFERENCES

[1] Bill Seymour, "How Neural Network Technology Can Tackle the Growing Telecom Fraud Problem", *Information Security Bulletin*, CHI Publishing Ltd, April 2000

[2] E. G. Berbés, I. C. Múgica and F. J. G. Mazario, "Gestión del fraude en telecomunicaciones", *Comunicaciones de Telefónica I+D*, Numero 33, Marzo 2004.

[3] Michael Cahill, Fei Chen, Diane Lambert, José Pinheiro and Don X. Sun, "Detecting Fraud in the Real World", *Handbook of Massive Datasets*, Kluewer, 2002.

[4] Helder Biscaia, Spiros Alexiou, Fernando Pavón and Rolf Hulthén, "Do intelligent techniques aid fraud detection?", *Eurescom Project Reports*, March 2002.

[5] Tom Fawcett and Foster Provost, "Combining Data Mining and Machine Learning for Effective User Profiling", *Second International Conference on Knowledge Discovery and Data Mining*, August 1996.