



**WHITEPAPER**

**TELECOMMUNICATION FRAUD MANAGEMENT**

**STEPHEN BROWN  
JANUARY 2005**

# Telecommunication Fraud Management

Stephen Brown, CSO

Waveroad

## 1. Executive Summary

Telecommunication Fraud is the intentional and successful employment of any deception, cunning, collusion, artifice, used to circumvent, cheat, or deceive another person, whereby that person acts upon it to the loss of his property and to his legal injury. However, there does seem to be a general consensus that telecom fraud, as the term is generally applied, involves the theft of services or deliberate abuse of voice and data networks. Furthermore, it is accepted that in these cases the perpetrator's intention is to completely avoid or at least reduce the charges that would legitimately have been charged for the services used.

On occasion, this avoidance of call charges will be achieved through the use of deception in order to fool billing and customer care systems into invoicing the wrong party.

Fraud is different from revenue leakage. Revenue leakage is characterized by the loss of revenues resulting from operational or technical loopholes where the resulting losses are sometimes recoverable and generally detected through audits or similar procedures. Fraud is characterized with theft by deception, typically characterised by evidence of intent where the resulting losses are often not recoverable and may be detected by analysis of calling patterns.

Telecommunications is an attractive target for fraudsters. In terms of volume, it is now measured in the billions world wide. Service providers are being hit with fraudulent requests for service of over 85%. Recent highly sophisticated schemes are employed by organized crime using hackers and self learning. Estimated that telecommunications fraud is more attractive than the drug trade.

The Communications Fraud Control Association conducted a survey and determined that \$35–\$40 billion in losses are due to telecom fraud worldwide.

It has been estimated the fraud problem is worth between \$12bn and \$55bn per year globally. In Africa alone, carriers write off 700m a year to fraud. That is expected to increase now that more than 30million Africans have access to cell phones, giving criminals a huge wireless market to infiltrate. While many large operators have developed sturdy FMSs to combat fraud, others have not. FIINA concluded that perhaps only about 10% of operators worldwide have set in place sensible and effective fraud strategies.

There is a pressure to deal effectively with crime. Indeed, it declines in the market coupled with huge debt burden. The shareholders pressures to protect the revenues they are generating. Also, companies are losing up to 15% of their total annual revenue. Losses attributed to other issues such as interconnect discrepancies and data corruption, some companies lose up to 30% of total revenue. Globally, telecommunication fraud is a bigger business than international drug trafficking, with operators losing \$55bn a year. It is the single biggest cause of revenue loss for operators, costing them between 3% and 5% of their annual revenue.

The motivation behind crime is attributed to migration & demographics, penetration of new technology, staff dissatisfaction, the 'challenge factor', operational weaknesses, poor business models, criminal greed, money laundering and political & ideological factors.

Revenue losses due to fraud is approximately equal to revenue leakage within the systems and procedures of a company. Properly designed Revenue Assurance procedures extract data at every step of the revenue-earning chain, subjecting it to a rigorous integrity check. The traditional time-based and cost-based approaches of processing CDRs alone are rapidly becoming obsolete. They must be enhanced by methods of detecting fraud from multiple intelligence sources: services, content, broadband devices, service quality reports, etc.

## 2. The Evolution of Fraud

With the evolution of technology, traditional types of fraud such as counterfeit/ stolen cards and altered

checks, pyramid schemes, chain letters and investment swindles have been replaced by more sophisticated systems. The telecom industry was hit from as early as the year 1900. The following lines described the evolution of fraud over the years:

- 1900: operator services
- 1950: teeing in
- 1970: payphone 'tapping'
- 1980: meter tampering, black box, red box
- 1990: 3rd party billing, calling card, tumbling ESN, cloning, ghosting and PBX DISA
- 2002: subscription, roaming, IMEI cloning, free phone, call forward, pre-paid, PRS, CDR suppression, magic phones, social engineering, voice mail hacking

The common fraud techniques are call selling with a motive on revenue for organized crime, subscription with a motive to avoid payment for individual, activations with a motive on subsidy theft for internal, PBX hacking with a motive on dial through for organized crime, pre-paid top up with a motive to avoid payment for individual and roaming with a motive on revenue for individual. The subscription fraud (40.8%), roaming fraud (16.3%), internal fraud (8.2%) and pre-paid (9.5%) are the most important in terms of losses by number of incidences. The internal fraud (40.3%), roaming fraud (11.4%), pre-paid (10.8%), subscription (11.6%) and premium (13.1%) are the most important in terms of losses by values.

In multiple, new and immature Services, content's value is increasing whereas the cost of the connection is decreasing. As an example, an SMS message to a vending machine to buy cigarettes. If no payment is collected, the loss is the value of the cigarettes, not the value of the message.

The main issues for the future are the increase in number of access methods (voice & data), the additional payments (the handset becomes a credit card), the improved identity techniques (possible biometrics), the internal fraud (increased access to key systems), the increased transaction repudiation (as per credit card sector), the money laundering (new regulatory requirements) and the need to use specialist Neural Network based FMS.

The size of telecom market makes it very attractive to fraudsters mainly because of the increased number of business transactions and the increased usage of distribution networks such as Internet, IP networks, LAN's, VPN over public networks, wireless networks and distributed computing and grid networking. Traditional telecom fraudsters will be joined by individuals from the Finance, IT & IP 'hacking' fraternities, sophisticated fraudsters will focus on content and conventional fraudsters continue to focus on voice.

Mergers and acquisitions play a major role in the fraud evolution arena. Indeed, acquisitions pushed up the price of its stock, providing the currency for further acquisitions which made investors happier and on and on. With a high stock price wrt earnings, WorldCom acquired companies with lower price-earnings multiples and because of simple math automatically increase its per-share earnings. After the deals, WorldCom subtracted millions and sometimes billions from its profits as a "write-down" of the value of certain assets acquired. Included in this charge were future company quarterly expenses. The result was bigger losses in the current quarter but smaller ones in future quarters.

The fraud management becomes more and more important as the new methods of access become available such as cable networks, wireless networks, DSL, Satellite, metropolitan optical networks running Ethernet, broadband wireless systems (radio, microwave, or infrared). The new network access services supports the convergence of voice and data networks into an all-packet-switched network that interconnects with the older PSTN for backward compatibility. This is the so-called NPN (new public network). The concept is to improve the quality of service on the Internet to support voice and other real-time traffic with the same.

Because the methods of access become more and more important, it is essential to build new billing systems and processes that bill various types of transport, access, transactions and content as well as time and distance. Processes that take into account pre-mediation, permitting users to perform secure

authenticated authorizations. Pricing that dynamically changes based upon quality of service changes, third party charges and competitor's pricing. And knowing the huge increase in data generated by users such as transaction volume, content carried transaction, text message, data, voice, payment, alerts and emails, the need for fraud management is there and needs to be improve as the telecommunications market grows.

The main benefits for fraudsters are the evasion of payment for service; the Service Level Agreement (SLA) violations meaning that the fraudster does not deliver contents of the agreed quality; the improper use of service content, resources or procedures including e.g. use of services in a unintended way and unauthorized use of resources, such as networks; the sabotage of service. And the way they do it is using a service without paying (such as "promises" to make payment, phoney personal identities, phoney equipment identities, stolen identities, unauthorized entry, faulty tracking, tapping, line surfing, ghosting) and call selling to others ( such as BYOB (Be Your Own Bell), selling phoney equipment, selling bogus prepaid cards, selling "tapped" access, selling "line" surfing (ie pbx access), selling stolen credit cards, stolen identities and equipment, selling "know how", selling accounting **fraud** (eliminating the records)).

### **3. Subscription Fraud**

The subscription fraud is the most prevalent since with a stolen or manufactured identity, there is no need for a fraudster to tackle a digital network's encryption or authentication systems. Its low tech with less chance of detection. Subscription fraud is one of the fraudster's preferred methods for digital roaming fraud.

The modus operandi of subscription fraudster is posing as a credit worthy person or company, the fraudster can gain access to any network, anywhere—1G, 2G or 3G. Typically the first step for fraudsters is to use subscription fraud to gain access to the home network. This way they appear on the network as a valid subscriber accepted by the digital network and authentication system. Often fraudsters work with corrupt dealers or internal groups within the service provider in order to create the subscriber accounts. They obtain roaming privileges, for example by posing as a small company or by behaving as a good paying customer for a period of time (known as a "sleeper"). The fraudster then roams to a foreign network and generates a high volume of lengthy calls in quick succession, usually on multiple handsets.

To recognize it, the carriers are learning the patterns of subscription fraud, including the common indicator of a billing address change within the first 15 to 30 days of opening an account. If a new user deviates substantially from the average new user and uses services for an excessive amount, a flag is raised. Certain services are more prone to subscription fraud such as third party sales like resale of long distance, roaming and international Call back.

The most common techniques to minimize impact and loss are threshold based analysis, inference rules analysis (ie callback scams), profile based analysis (habitual user profiles) and neural networks.

The main vendor tools for eliminating subscription fraud are:

- Credit Worthiness Checking Software.
- Cross Checks to External databases
- Biometric piece of information about the subscriber
  - i. The most compelling of all biometrics in the telephony world is, of course, the voice
- "ProFile" an intercarrier database of accounts-receivable, write-offs and service shut-offs that provides on-line prescreening of potentially fraudulent applicants. Helps identify applicants with a history of bad debt.
- "InSight", a customer database that carriers scan for previously qualified applicants to eliminate the re-qualification process.

### **4. Internal Fraud**

Internal fraud represents 8.2% of incidences but generates 40.3% of value lost which is equal in value of

the following four types of fraud combined: roaming (11.4%), pre-paid (10.8%), subscription (11.6%) and premium (13.2%). The motivation for such a fraud is caused by companies not prosecuting, shady management accounting practices, unrealistic performance targets, few checks and balances, and disgruntled employees.

The method to hi-lite internal losses are the following:

- Computer assisted audit techniques (CAAT)s enable investigators to obtain a quick overview of business operations, develop an understanding of the relationships among various data elements, and easily drill down into the details of specific areas of interest.
- The use of digital analysis techniques such as Benford's Law
  - i. Frank Benford, a physicist at GE discovered that in just about any given set of numerical data, numbers occur as the first or second digit at a predictable rate. For example, "1" will appear as the first digit 31% of the time, but "9" will appear first only 5%. Benford tested lists of numbers from many different sources accounting ledgers, geographic data, even magazine articles -- and found that the same probability persisted.
- Example application of Benford's Law
  - i. In 2002, Darrell Dorrell, a principal at accounting firm Financial Forensics in Lake Oswego, Ore., used a computer program to apply Benford's Law to more than 21,000 payroll records of a health-care company accused of defrauding investors. He found that the number "0" turned up as the second digit in the payroll records twice as often as it should have, and "5" showed up 60% more often than would be expected.
  - ii. With that information, plus lots more evidence from other tests, he reported to the company's receiver that the records "appear to be contrived."
- Review records for the existence of duplicate transactions, missing transactions, and other anomalies.
  - i. Comparing employee addresses with vendor addresses to identify employees who are also vendors.
  - ii. Searching for duplicate check numbers to find photocopies of company checks.
  - iii. Scanning vendor lists to find those with post office boxes for addresses. Further follow-up to ensure they represent legitimate vendors.
  - iv. Analyzing the sequence of all transactions to identify missing checks or invoices.
  - v. Identifying all vendor companies that have more than one vendor code or more than one mailing address. Such listings may represent "phantom" vendors,
  - vi. Finding several vendors with the same mailing address. These records also may signal phantom vendors.
  - vii. Assuming that each employee in the organization receives only one paycheck per pay period. Search for duplicate records in a single pay period.
  - viii. If the assumption is correct, the existence of employees receiving two or more paychecks may indicate fraud.
  - ix. If the assumption is invalid--some employees may receive a separate check for overtime in addition to their regular pay, for instance--the auditor can then form a revised hypothesis that each employee should receive only one paycheck for regular hours per pay period.
- Conflict Checkers ...
  - i. look for relationships between potential new hires and business units, with an eye to uncovering conflicts of interest or illegal activity
  - ii. The latest systems will scroll through payment information looking for suppliers that aren't listed in any online commercial database -- a possible sign that they aren't legit
  - iii. or that operate from addresses that have been associated with fraud in the past.

Effective method for mitigating risks need to be implemented. Actions such as utilizing well trained auditors, improvement of hiring practices and background checks, prosecuting when caught, no single point of failure and effective training for employees that handle cash will minimized the risks. Conducting internal investigations is also a solution to minimise risks. The purpose of internal investigation is to gather sufficient facts to lead to a conviction. It consists of deciding whether its covert or overt. Team members require complete independance from the operational teams and need not to be chosen from the development team. Finally, computer assisted tools are essential for such

investigation.

## 5. Partnership Fraud

Resellers (wholesalers) may represent a risk because of limited assets with which to support recovery actions. Partners can mis-represent their transactions. They often have significant access to OSS/BSS systems or how your business works. Outsourcing creates opportunities for fraud. Distributors may have access to authentication activation codes, they can create phoney customer accounts, mis-represent sales volumes, etc.

Therefore, the need to effectively manage relationships is absolutely necessary and requires appropriate actions with the following:

- Operators
  - Interconnect agreements should address fraud
  - Cooperate with your partners on identifying fraudsters
  - Use similar fraud prevention technologies such as authentication.
- Third Party Providers
  - Examples:
    - Outsourced Logistics providers such as tower and BSS installations,
    - content providers
  - Periodically Conduct proficiency tests.
  - Contractually determine who owns the risks?
  - Share what you know – offer assistance.
    - Resellers that are running high numbers of "never-pay" accounts. Maybe they are not a fraudster, but the quality of their subscribers may be poor and they may need help'
- Commercial Dealers
  - Interconnect agreements should address fraud
  - Cooperate with your partners on identifying fraudsters
  - Use similar fraud prevention technologies such as authentication.
  - Carriers that have an FMS in place are still susceptible to fraud on their resellers' networks. Fraudsters can move to a telco's customers.
  - The industry "never-pay" average for resellers is around 15-20%, with some as low as 5-6%, and others at 80% never pay,"

Interconnect fraud is also a threath and need to be addressed:

- Interconnect agreements should address fraud
- Organized Crime Operates Across Borders
  - International call back subscription fraud
  - International Roaming fraud
- The fraudster may actually be a telecom company
  - Setting up operations in shared telecom hotels
  - Paying their bills for the first few months then running up sizable unpaid accounts off shore
  - The forum for international irregular network access (FIINA), comprising fraud experts from incumbent operators and large vendors around the world to exchange information on fraud, estimates the average telecom operator loses around 6% of annual net revenues to fraud.
  - But, according to Nortel, weighing in the cost of interconnect payments--where the operator receives no revenues from the fraudster to cover them--the combined impact on earnings can be as great as 20-30%.

## 6. Fixed Network Fraud

Fixed networks are evolving and becomes more and more attractive for fraudsters. Improvements such as migration from circuit switched (TDM) to packet switched (IP), High Speed Digital Access (ADSL, Cable, Broadband satellite), Soft switches rather than hardware switches, the emphasis switching to content rather than carriage, extending access to the SS7 signalling and supervision networks to

Operators and partners, and changes in numbering plans provide fraudsters with new media and new opportunities to increase their presence. The most common types of fraud affecting fixed telco lines are line surfing, ghosting, subscription, slamming and cramming, PRF, call selling, PBX hacking and activation (internal fraud). The less common are prepaid and social engineering fraud.

Subscription fraud is where a fraudster gains access to a service, usually by using false identity details. It also relates to circumventing credit checks upon subscription. In some cases, a firm or individual will pay their first month of service before increasing their call volumes through call selling for one or two months and then leaving town without paying the bill.

Physical attacks on networks are Payphones, tapped lines, customer premises – PBXes, vandalism in manhole, outside plant terminals, ISP servers – denial of service attacks, ISDN lines (see SS7 attacks).

Premium Rate Service (PRS) fraud is perpetrated by setting up a "legitimate" high tariff PRS in another country and then creating calls at the expense of the originating telco. In some cases, office cleaners have been organized to dial these numbers, and leave phones off the hook all night. Also known as "cramming" in the United States, tricking someone into accepting 9xx charges on someone's bill. Premium rate SMS (ring tones, clip art, micro payments) and Premium rate WAP (information services) are also known as fraud risks.

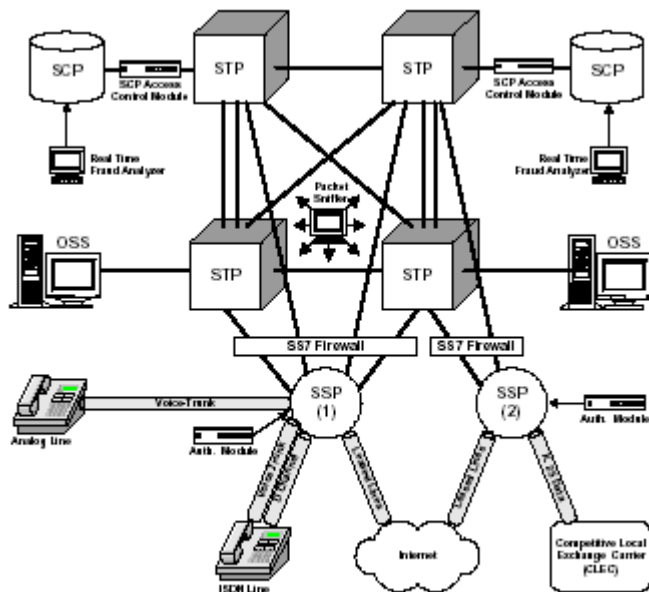


Figure 5. SS7 attack management system.

There is also a threat of SS7 attacks where the no. 1 concern is denial-of-service attacks. There is limited mitigation tools which consists in basic SS7 surveillance tools and expanded firewall functionality. It is not designed for encryption. The attacks aimed at SCPs, STPs, SSPs. It impacts local number portability, LIDB ( billing data, collect calls, PINs, etc).

The mitigating method for eliminating such frauds are installing FMS systems, fraud management organizations, internal auditors, revenue assurance checks, better hiring practices, correlation checks, traffic monitors and updated OXX/BSS systems.

## 7. Mobile Network Fraud

The security of mobile networks is more of a concern than wire networks. Physically accessing the network is easier than with wired. Authentication and privacy (via encryption) are issues. Both voice

and computer traffic suffer from security concerns. As the industry migrate from 2G to 3G networks, all traffic becomes packets of information carrying voice, data or video. The use of rogue base stations and rogue wireless access points are real threats.

Encryption plays a major role for operators & handset/SIM. In the case of the operators, UMTS security standards based upon 802.11i (secure encryption) at access point or base station and SSL (Internet traffic), IP Sec for VPN tunnelling is used. For handset manufacturers, SIM cards are responsible for authentication and secure storage of authentication keys. All transactions in GSM terminals have been secured. Thanks to the SIM using symmetric and public-key algorithms. Transactions will be secured under WAP version 1.2 using the public-key-based WAP-identity-module functions, likely to reside in a SIM in most WAP handsets. Security could also be achieved by shutting down phones. They are built with chipsets like the Xilinx chip. Once phone is reported stolen, the phone company sends new data to the handset, that turns the chip into a block between the keypad and the rest of the phone, preventing further use. This makes the handset unusable; even if the thief changes the SIM (subscriber identity module) card, the reconfigured chip continues to prevent use of the keypad. The same technology can be used to re-activate the phone if and when it is returned to its owner.

Network security needs to change since "SSL provides one level of encryption of the traffic but not strong authentication." In other words, the data will be encrypted but there is no guarantee who is sending the data. SSL will be replaced by another Internet security standard called transport layer security, which is backwards compatible with SSL but uses stronger encryption protocols. Migration to 802.11i from WEP based encryption will take place. Public Key System for multiple merchant transactions is also a key to security. Indeed, rather than using the same key for both the encryption and decryption of data, each customer is given two keys — a private key that he does not share with anyone and a public key.

We are currently observing a rise in mobile phone related theft. Indeed, in the UK, cell phone thefts have nearly tripled since 1995, with mobile phones targeted in about 28 percent of all robberies. UK officials are considering legislation that would force phone networks to institute antitheft measures. Also, there is rising theft amongst children and a variety of new featured phones makes them more attractive.

Cloning, tumbling & other ways of compromising mobile networks and handsets are affecting security in mobile networks. Cell phone cloning is copying the identity of one mobile telephone to another mobile telephone; Cloning required access to ESN and MIN pairs; In tumbling, you pretend to be from another cellular carrier. Next, you modify your mobile telephone to generate a random ESN (Electronic Serial Number) and a random MIN (Mobile Identification Number) from an Area Code of this carrier for each call; Subscription fraud; Stealing the handset and changing the SIM card.

The best ways to reduce mobile network fraud are: installing FMS systems to alert, block and analyse traffic; implementing authentication & RF finger print technology; installing phone theft disabling technology; installing encryption to prevent sniffing of ESN and MIN; implementing better anti subscription fraud practices; and introducing PKI (Public Keys) technology.

## **8. Prepaid Fraud**

There is many ways for fraudsters to exploit prepaid services: Using lost or stolen credit cards or bounced cheques; internal engineers can access and alter billing-activation systems; stealing cards, PIN numbers and recharge codes at production and support sites; scan for data from legitimate phones and duplicate the information onto stolen devices. These prepaid phones appear legitimate but steal minutes from an honest customer; call support lines and claim their calls were not connected or replenishment cards are faulty; Simultaneous refills with the same HRN; Guessing HRN's.

Operators can curtail these methods in many ways. Beefing up company security and carefully watch employees; point of sale activation (POSA) system for card activation at the time of purchase. Stolen cards without activation have no value, and access, PIN, and replenishment codes are generated upon sale; requiring wire transfers for large orders, avoiding credit card and bank check scams; send inactive cards that are activated only when funds clear to the carrier account; and installing Pre-paid FMS

systems with logs and alerts.

Also prepaid users need to be regulated in teaching them how to spot abuses and in requiring them to charge the card within a specific period of time. Activation at point of sale and limit where they can recharge (ie within country only) is also a way to prevent fraud.

However, there is risks associated with recharge methods. There is four types of prepaid systems widely in use. These are: a. 'Advice of Charge' based system; b. 'Hot Billing' based system; c. 'Service Node' based system; d. 'Wireless Intelligent Network' (WIN) based system. In SIM based (AoC) communication from MSC is not encrypted. Credit information is stored in the SIM, it is not very difficult to modify the same illegally. Hot Billing Systems have "last call" issues whereby the last call can overrun the limit on the voucher. C) and D) : IN based systems don't generate logs

In order to minimize the impact of prepaid fraud, the vendor community is developping techniques such as Real time billing and rating systems, combining pre-paid and post paid systems into one, generation of logs for changes made to IN based systems; activation at point of sale systems; migration to IN (Intelligent Network) based systems.

## **9. Roaming Fraud**

Roaming subscriber makes calls on another network as a visitor (roaming subscriber). Call charges are routed via TAP files to the subscriber's home network. This fraud is similar to subscription fraud in that the perpetrator has no intention to pay for services used. The time delay of high call rate identification and notification to home network when roaming on another network is exploited by fraudsters. Prevalent among customers who get new service and immediately thereafter use service as a roamer on another network.

Roaming fraud causes severe loss to telcos. (CFCA) Global Fraud Loss Survey 2003, fraud losses are typically 4% of revenues. For mobile service providers, approximately 25% of their total fraud is roaming fraud. Losses per handset range from \$100's per handset if real time record checking is in place to \$10,000 with HUR (High Usage Record) systems and \$50,000 per handset for carriers that rely on clearing house data.

Criminals use different fraud methods: Subscription fraud is one of the fraudster's preferred methods for digital roaming fraud. The delay in the home provider receiving roamer call data can be anywhere from one to several days; Stealing mobile phones belonging to roamers, usually in vacation destinations. Often the victim does not report the theft until several days later when they've returned home; Cloning: As service providers began to prevent them on their network, the problem migrated to roaming partner networks; Flaws in the authentication algorithms used by the SIM card in GSM mobile networks. Fraudsters are now cloning SIM cards like they use to do with the cloning of ESN/MIN numbers.

The GSM Association is making major efforts to minimize the impact of roaming fraud. It has developped a security accreditation scheme (SAS), designed to minimise the one-to-one security audits carried out by operators on suppliers. It has also created IREG's Permanent Reference Documents relate to roaming tests between operators. These documents are an essential reference re- source for the Association's membership -a library of case studies, principal, technical theory and informed prognosis. IREG also serves as a forum at which operators can share the experiences and expertise that contributes to efficient problem solving.

Vendor community is currently working on techniques to prevent or minize the impact of roaming fraud such as clearinghouse, High Usage Report (HUR) and Roamer CDR Exchange (RoamEx). Clearinghouse provides information such as individual call details, individual call charges and billing specific data. HUR provides information such as call summary for subscribers that exceed threshold and approximate charges. RoamEx provides information such as individual call details and fraud specific data.

## **10. Content and Value Added Services Fraud**

Many content risks and liabilities exist. It is far greater than the costs of the call. It takes on the financial liability by agreeing to bill subscribers for retail purchases or receive payments for value-added content. Also, there is a greater number of partners involved, often simultaneously during the same session. Therefore, some systems cannot bill for some services. Copyright laws differ regionally and from country to country. Finally, paying for the call even if the content provider isn't paid.

Content theft relates to file swapping networks for music and video; copying, sharing of software; ripping CDs and DVD; adult content freely available via the Internet; photocopying books, manuals and other copyrighted materials

There is many ways to manage the risk. Credit Card fraud is rampant on the Internet so treat content payments made with credit cards accordingly. Also withhold a percentage of each transaction in order to settle or cover bad debt. Another way is to limit the value of transactions that can occur using micro – payment services. E-identity is used throughout the banking, finance, retail and travel industry sectors, and is said to be consistently detecting 90 per cent of fraudulent online credit card transactions. And finally, uses services that improve "card not present" (CNP) transactions.

Therefore, to minimize the impact, the payment mechanisms should be operator bills for content, micro-payment services using the handset, third party payment houses ie PayPal and Credit Card companies.

Other solutions could be used to minimise the fraud. Watermarking permits the content owner to identify his content and and its origins. Encryption prevents intercepted content from being used or resold without the key. DRM (Digital Rights Management) permits only the purchaser of the Content to view it. Prevents copies being made.

In order to maintain revenue streams through, secure delivery channels and WIB-enabled services are used. Secure Delivery Channels uses USIM card solutions (Universal Subscriber Identity Module) which manages important security functions, ensures authorised access and manages different applications residing in the USIM . Also does encryption of data, handling of digital signatures. WIB-enabled services leverage SMS-based technology plus SIM toolkit that enables the SIM card to drive the handset interface, using the Wireless Internet Gateway (WIG). The gateway opens up a secure channel (utilising GSM 03.48 security) to the WIB on the SIM.

## **11. Data Mining Applied to Fraud Detection and Prevention**

Data Warehouse Data Modelling is a tool that provide the following information: Ensure all customers are entered into the billing system; Ensure the quality of the data; Ensure all billable calls are being billed; Examine major contributors to revenue, profits and losses; Reconciliation of revenue with other sources of data from accounting to the network as well as any inventory.

Data Mining is an information extraction activity whose goal is to discover hidden facts contained in databases. Using a combination of machine learning, statistical analysis, modeling techniques and database technology, data mining finds patterns and subtle relationships in data and infers rules that allow the prediction of future results. Typical applications include market segmentation, customer profiling, fraud detection, evaluation of retail promotions, and credit risk analysis.

Data Mining could be applied to fraud detection and prevention by looking for patterns and relationships between various data sources, by helping prioritizing your investigations and expenditures wrt revenue losses, by spotting organized crime rings operating in your territory and by identifying internal fraud.

## **12. Fraud Detection and Prevention**

Main Categories for the fraud processes are internal fraud, roaming fraud, pre-paid, subscription, premium rate, cloning, PBX related and phone theft.

Many fraud activities have been recognized. They are described in the following tables.

Fraud Type	GSM	FL	Description
Subscription	▲	▲	Most common form. Perpetrators of this fraud apply for a service and once activated, immediately use it for national and international calls with no intention to pay for the calls made. It is almost always associated with call selling.
Clip-on		▲	Includes teeing an instrument across a subscriber's line (parallel connection) and diverting the line (stolen line worker) so that the legitimate user does not have access to it.
Clip-on to Payphone		▲	A second instrument is connected in parallel to the coin or card phone line. Payment is avoided by seizing the switch with an instrument that does not have a coin recognition device or card reader device. Detection will have to be based on irregular usage as coin phones will in all probability not generate CDRs and access to the card phone systems CDRs may not be available.

Fraud Type	GSM	FL	Description
Payphone Meter Pulse Defeat		▲	Pulse suppressing circuitry is connected to the payphone line. Payment is avoided by preventing a card or coin instrument from receiving the switch metering pulses.
Collect Calls to Call Office			Where a customer requests an operator to dial the destination and ask the answering party at the destination to accept the charges for the call. If agreed, the operator will connect the customer to the destination. Payment is avoided by accruing the charges to the destination; in this case a Call Office. The Call Office Identification Tone may be disabled to prevent the operator from disallowing a call to a Coin Phone or requesting periodic payments from a card phone.

Fraud Type	GSM	FL	Description
Booked Calls from Call Office			A booked call is where a customer requests an operator to dial the destination. Once the destination has been successfully reached, the operator will dial the original customer back and connect the two parties. Payment is avoided by accruing the charges to the Call Office number. The Call Office Identification Tone may be disabled to prevent the operator from requesting periodic payments from a payphone.
Stolen Line Unknown		▲	Limited to providing an unassigned number to a user that does not have an account with the network. Unless gross negligence has occurred (dial tone available on a spare cable pair outside the switch building), this can only occur with the assistance of the network's personnel.

Fraud Type	GSM	FL	Description
MSISDN/IMSI Pair	▲		Entails coupling an unregistered MSISDN to an IMSI of a customer. Payment is avoided as the MSISDN is not recognised as a prepaid or contract customer. The action takes place on the HLR and is only possible with the assistance of the network's personnel.
Call Forwarding Manipulation	▲	▲	Consists of setting up a local number to forward calls to an international destination. A local A number dials the call forwarding set B number (CFWD) which forwards the call to the C number.

Fraud Type	GSM	FL	Description
Call Back Operators	▲	▲	<p>Involves getting cheaper international calls from a call back operator (usually in another country). The call back operator has to have a switching capability (PABX) connected to a network (PSTN). It can be done from within own country as well – in this case there is a high risk that the call back operation will actually culminate in subscription fraud on the grand scale. Revenue loss occurs twofold, loss of o/g call cost plus i/c interconnect call settlement.</p> <p>Initiating a 'called back' call can be achieved by:</p> <ol style="list-style-type: none"> <li>Dialling out – being identified by CLI – call terminated without answer- call back to identified CLI with dial tone</li> <li>Regular dial tone availability – call back operator extends dial tone via calls at fixed times</li> <li>Call booked via other channels (e.g. email) – followed by long duration incoming calls from a single international number</li> <li>Call initiated via international toll free number</li> </ol>

Fraud Type	GSM	FL	Description
Conference Call Manipulation	▲	▲	Only possible if the network's billing system is not able to bill for conference calls. In this case a call is made to a local B number followed by a second simultaneous call to high cost destination (national or international). The second high cost call is not billed.
International Roaming Manipulation	▲		Roaming subscriber makes calls on another network as a visitor (roaming subscriber). Call charges are routed via TAP files to the subscriber's home network. This fraud is similar to subscription fraud in that the perpetrator has no intention to pay for services used. The time delay of high call rate identification and notification to home network when roaming on another network is exploited by fraudsters. Prevalent among customers who get new service and immediately thereafter use service as a roamer on another network.

Fraud Type	GSM	FL	Description
SIM Cloning	▲		Cloning is the process of replicating an existing customer's hardware or frimsware, allowing calls to be made on their account. The legitimate customer will not become aware of the deception until they receive an inflated bill at the end of the month and so cloned phones are often sold with a 30 day guarantee.
Premium Rate Service	▲	▲	The owner of the premium rate service receives revenue from users calling in to the number. Therefore fraud will involve a high number of calls made to the PRS number from a network customer's line without their knowledge or from a number where there is no intention to pay for the o/g calls. O/g calls can be made using auto-dialers.

To detect and prevent fraud, there is a need for optimal use of internal systems & intelligence such as pre-paid and Post Paid Billing Systems; customer Service Databases; mediation technologies; data warehouses; SS7 interfaces like INs (Intelligent Network) modules, SCP (Service Control Points); alarms from network; alarms from FMS systems; accounting systems; training; tips. External knowledge and experience could also be used such as other carriers, associations, vendors and consultants; use on-line data exchanges; Law Enforcement Agencies.

### 13. Tools and Techniques

The common FMS techniques are rules based detection, rules discovery techniques, customer specifics and behaviour specific, neural networks, audits, use of pins prior to placing a call (80 –96% drop in fraud), setting limits on dialling capabilities (ie home area only) and roaming exchange services

The common FMS tools & technologies are radio frequency finger printing, authentication (symmetrical keys in phone and base station), digital systems with encryption, various probes, IP mediation and billing mediation systems can assist in collecting the data, PKI (public keys), SS7 surveillance, anti-virus and anti-trojan software, firewalls, encryption, water marking and digital signatures.

Waveroad SecuriT  
4710 St-Ambroise st, suite 264  
Montreal, Qc  
H4C 2C7  
Tel: 514.935.2020  
www.waveroad.com