Combating Existing and Future Fraud Threats

A look into emerging fraud threats in a next-generation environment and best practices to counter them
Introduction

The telecommunications industry has been evolving rapidly through generations and so has telecom fraud. Telecom fraud is alive, well, and on the increase. As new technologies are introduced in the telecommunications world it also brings with it unprecedented levels of fraud. Now the latest to hit is the NGN (Next Generation Networks) fraud and telecom operators need to brace themselves to combat all emerging and future fraud threats.

Prior to the arrival of NGN, every generation, evolution, revolution and technological advance in telecommunications was seen as the ‘Next Generation Network’ (NGN) fraud. Right from the ‘Plain Old Telephone Systems’ (POTS) with its wire-tapping, account fraud, and multi-colored box attacks, through mobile telecommunications fraud to eavesdropping (on the air interface) and cloning in the early mobile analogue networks (e.g. TACS, AMPS, etc). These however jolted system developers and standards bodies to take more care when developing systems in future. Losses (both directly to fraud and indirectly to brand damage) were high.

The second generation (GSM, D-AMPS, PCS, etc) brought the first wave of digital technology, a degree of global standardization, improved security, affordable handsets and the ability to roam almost anywhere in the world. It also acted as a catalyst for Roaming fraud, Call-selling, PRS fraud, SIM-Boxing, Pack-Splitting, Dealer frauds, and a host of other abuses.

Lessons were learnt from the introduction of 2G. Next Generation Networks were better and more resistant to abuse, standardization was comprehensive, security was good, and threat scenarios were studied in some depth. The roll-out of the first ‘3G’ networks was markedly different to earlier generations; it did not comprise the arrival of a single network or technology and it did not offer radically new service capabilities. Instead it brought with it the merging of an enormous variety of new technologies, capabilities and efficiencies in the form of l-mode, UMTS, ADSL / Broadband, WiFi / WiMax, IPTV, Fixed and Mobile Convergence, a transition to IP, enhanced device capabilities, and M-Commerce. There was no sudden big bang but just waves of new opportunities. In spite of the apparent opportunities no catastrophic new fraud types emerged, and Fraud Managers slept reasonably well. There was no innovation and ingenuity to abuse the new technologies.

The truth is the fraudsters had no immediate inclination to discover and develop new means to commit fraud, possibly because the new emerging services were not that different. Subscription fraud continued, as did IRSF, PRS fraud, pack-splitting, dealer fraud, Call selling, SIM-boxing and just about every other type of existing fraud. There were no major surprises, no novel new attacks or fundamentally new types of fraud to worry about.

Whilst we’re still bracing ourselves and waiting for that ‘big bang’ NGN fraud to hit, the fraud landscape has changed significantly enough to require some dedicated focus of Fraud Managers and Fraud System Vendors alike. The introduction of new technologies continues it’s relentless march with concepts such as Cloud, converged content services, further 3rd party service enablement, increasing open-ness and of course, 4G. Perhaps the important change that the next generation has brought so far, is a fundamental shift from traditional ‘closed’ networks to the era of open networks, easy access and technology agnosticism. In summary, there are now infinitely more ways available to commit all of the existing frauds.
NGN Fraud
The term NGN fraud is commonly used in conjunction with frauds associated with technologies and services such as:

- IP networks;
- 3G (UMTS, i-Mode, etc) networks;
- data and content services;
- m-commerce,
- powerful feature-rich devices;
- exploitation of open access mediums and architectures;
- anything outside the 'normal' traditional mainstream usage-based telecom frauds

These frauds are here today and are perpetrated against the networks and technologies of today but their existence is not new. Operators have been dealing with them for a number of years now, and the best fraud system vendors have been offering solutions to combat them for just as long.

NGN fraud is basically associated with two categories of fraud

- **Recent or emerging fraud threats** - Typical examples are Wangiri, PRS Content, SMS-Spoofing, and SIM-Boxing/Bypass Fraud. These have recently emerged, are widespread and independent of the above mentioned NGN technologies and services

- **Future Fraud Threats** – These are fraud threats that have not been exploited so far, but might be in the near future, if/when new weaknesses arise in today's technologies/services or future technologies/services. It is important to understand such threats and develop suitable counter measures for them.

A more detailed description to recent, emerging and future fraud threats is covered in the following sections.

**Recent and Emerging Fraud Trends**

**Content Sell Fraud**

The fraudster replicates and re-sells premium content, such as video or music files, at a fraction of the normal rate. This includes content resale (pirating) and IP infringement.

**Content Artificial Inflation Fraud (AIT)**

Content AIT is similar to traditional premium rate service (PRS) AIT attacks, but is increasingly associated with content downloads. This revenue-depleting fraud leaves the operator unable to collect fees from the fraudulent service use, but can be (unless appropriate interoperator/governmental mechanisms are in place to mitigate it) obliged to pay the content provider.

Also sometimes referred to as Content partner fraud.
Click Fraud
In addition to content AIT, AIT also can manifest itself as a specific type of internet-based fraud—commonly known as 'click fraud'. The fraudulent PRS content provider drives traffic to a paid content Website. This may be done manually, or by injecting phishing, malware to automatically use the service or hacking an operator's network to divert traffic to a content service, similar in nature to older auto-dialer attacks.

Crossover Fraud
Fraudster sends a "Trojan" to legitimate 3G subscribers. The Trojan causes the mobile devices of subscribers to automatically use service without the subscriber's authority or knowledge. This is commonly used to make premium rate calls that inflate revenues to the fraudster's own service. An alternative example (from Japan) is where a trojan was released causing users devices to automatically dial the emergency services.

Subscription and/or Identity Theft
Obtaining a usable identity is still a major factor in perpetrating many NGN frauds. Even with the degree of anonymity in the IP world, fraudsters will still obtain details to make transactions appear as if they originated from a valid customer. The increasing ease with which credentials can now be obtained is fueling subscription fraud and identity theft. For example, web based transactions, emails, social web sites, chat rooms and many other new generation methods can be used to obtain details.

IP Frauds
As increasing numbers of networks (and customers) are adopting VoIP, Hackers and criminals will therefore be enticed to capitalize on any weaknesses in the technology. VoIP is merely a transport protocol running on a data network. From a security viewpoint, this means that it is susceptible to all the attacks commonly targeted against data networks, even if they are not explicitly targeting voice over IP.

VoIP Bypass
VoIP bypass fraud involves diverting legitimate fixed-line or mobile originating voice traffic into VoIP sessions. This results in a loss of revenue for the terminating operator, this method may also be used to conduct “Dark Arbitrage”, “Gray Routing”, or a host of other, essentially identical, but impressive sounding frauds.

(IP) Denial-of-Service (DoS) and Flooding Attacks
Switches and gateways in a VoIP network can be vulnerable to external hacking attempts. In a DoS attack, the hacker gains access to IP address information of certain switches and targets them, leading to disruption of calls. One particular DoS attack is characterized by flooding of voice channels with de-authentication packets that terminate all VoWLAN handset associations to access points. This continually disconnects all handsets from the network.

IP Spoofing
Use of IP spoofing (substitution of identity information is becoming more common, often to aid other frauds by offering anonymity to the fraudster.)
Spamming/Phishing
Spamming and phishing refer to messages (usually randomly) sent out, typically to trick customers into disclosing credit card numbers, account passwords or banking information, or to prompt them to call a PRS service for example. Such e-mail/SMS/MMS messages often purport to be from well-known companies (spoofed address).
Spam over Internet Telephony (SPIT) consists of unsolicited bulk messages that are broadcast to phones connected to the VoIP WLAN network. Fraudsters send voice messages (such as PRS call-back or marketing spam) in bulk. Methods include hacking into a computer used to route VoIP calls to target a large number of subscribers.
Phishing is typically split into two categories:

- **Selective Phishing** – aimed at a specific group of individuals such as key workers within a company who may be dealing with customer details or financial data.
- **Broadcast Attack** – aimed at anyone randomly selected from a large group of individuals.

Thousands of phishing scams currently exist, each attempting to lure customers into visiting a fraudster’s website and entering personal information.

Money laundering
With the increase in m-commerce applications, micro-payments, and e-wallet/purse implementations, many new opportunities are opening up for money laundering. For example, use of phishing type emails to recruit persons to help with money transfers i.e. messages to recruit financial couriers in order to transfer their funds from one world location to another. Money laundering may also be conducted in a virtual IP environment, although recent controls are making this much more difficult e.g. “Second Life” where Linden Dollars could be exchanged for actual currency allowing movement of money.

Illegal Exchange of Content
Creation of Bulletin Boards, Chat Rooms (IRC - Internet Relay Chats) or Theme Forums to broadcast obscene, abusive content, distasteful material (illegal gambling; xenophobia; money-making schemes; promoting drugs; terrorism; prostitution; cracking of mobile services; piracy, etc) or even for trading personal details (stolen credit card details; PIN numbers; prepaid recharge vouchers codes, etc). For example, Phishers using IRC to offer credit card names addresses and card numbers or codes.

Malware
This general term applies to software that secretly installs viruses, key-loggers, etc - or malicious code executed on a computing device. It is another emerging fraud category that involves infecting devices with viruses and Trojans resulting in unauthorized actions. This might include making calls, deleting or stealing data. Once installed, unknown to the subscriber, a number of activities can take place, such as connections to PRS numbers, blocking calls, sending bulk SMS, or forcing legitimate services to fail.

- **Viruses** - malicious software designed to cause damage to a single terminal, computer or server, assuming the form of a virus that reproduce itself to other terminals, computers, servers or networks.
- **Trojans** - programs designed to be installed at the customer terminal when a file is received or an infected website visited.
- **Worms** - Worms are a variant of viruses, usually transmitted across a network, that duplicate themselves repeatedly...
potentially infecting their way through an entire network infrastructure.

- Spyware / Adware - Spyware is a malicious software installed on a specific terminal (computer; laptop; 3G handset; PDA; smart phone, etc) usually without the user's knowledge or authorization, along with Adware to scan files on hard drives or at the terminal / USIM memory; to make changes to default computer / terminal configuration and to extract and gather information to send it back to a host server. The fraudster uses the data to sell it to an advertiser (marketing reasons), to any other third party or to trade identities and customer financial details through the Internet.

**Pharming**

A serious and growing new internet threat where malware is used to misdirect users from legitimate site to a fraudulent site or proxy server without the victim's knowledge. Users are induced to visit the fake website that appears legitimate, and divulge personal and sensitive information such as bank account details, passwords, PIN numbers, Credit Card codes, etc.

Pharming is possible in a number of different ways:

- By DNS - Domain Name System / Server hijacking or poisoning. Hackers exploit security vulnerability at a DNS, hijacks the victim's DNS server, then changes the real IP address of the targeted web site to an IP address belonging to a faked one and finally redirects all the traffic from the real to the fraudulent web site (by entering the real web address URL victims are automatically redirected to the fake website);
- By installing a Malware (Virus or Trojan Horse) at the victim's terminals;
- By compromising the user's firewall or router.

**Brand Integrity Threats**

Online criminals can use names and logos of operators in order to promote fraudulent attacks against company's assets and reputation. Real, false or faked operators branded products and services are sold over the net and paid remotely (for example by Credit Card) for goods not delivered at all or distributed not according to the original proposition or format. Usually this is perpetrated through direct messaging or spamming customers by email, SMS, MMS or Instant Messaging. In the case of email for example it could also link customers to the genuine operator website to improve authenticity of the attack. The main goal of fraudster is: a) to extort cash directly by using company branded products and services plus name and logo; b) to extract personal information, which will include information related with Credit Card Numbers or other personal information.

**Financial Advance Fee Fraud**

One of the most common frauds attempted by email against customers or company employees is Advanced Fee Fraud. Two typical schemes are as follows:

1) Email messages are sent from 3rd world countries purporting to come from high-ranking dignitaries, former government officials, former presidents or ministers, bankers or lawyer, who outlines a profit scheme whereby a large sum of money can be shared with the email receiver. The claimed origin of this money may be forgotten bank deposits, funds belonging to a former political regime or simply private capital that needs to be transferred out of the country and invested abroad. The email receiver is lured by promises of a generous percentage of cash in return for assistance in executing the scheme by helping to transfer the money. Then the victim contacts the fraudster to provide by phone, fax or
email the bank account personal details into which the funds are to be transferred. After this stage upfront or advance fees are requested to the victim (starting as small amounts but evolving to large ones) to cover taxes, legal or transaction fees or bribes, in order that a successful completion of the scheme can be achieved. After requested to pay those advance amounts in order to facilitate the money transfer and to receive the corresponding share compensation, the victim concludes that no money has been transferred and only his money was thrown away to some fraudster scheme.

2) Fake lottery win alerts are sent by email. The victim is sent an email congratulating him on winning a huge sum in a lottery, usually somewhere in the world and the winner must pay a “small fee” in order to authorize the transfer of the money. Once this small fee has been paid, the winner never hears from the lottery organizers again.

Next Generation services have given new access methods to this traditional fraud.

Credit card Fraud
Credit card fraud has been growing steadily for a number of years, especially where card not present (CNP) transactions take place with stolen or compromised cards and subsequent charge-backs occur.

M-commerce related Frauds
Increasing opportunities and exploitation of m-commerce type services are opening the doors to Micro-payment frauds, including large-scale theft of (cheap) products, money laundering, and transaction denial. Opportunities are also emerging for using stolen or compromised handsets to buy goods or make financial transactions/transfers or simply maliciously depleting funds from the account holder e.g. e-purse, wallet, or bank account (via banking application).

M-Commerce could (or perhaps has) become more susceptible to fraud, due to tightening up of security and more attention to fraud threats being afforded in other Industry sectors (e.g. online retail).

Hacking
Hacking has had a large following for many years, either for financial gain, or simply for kudos/fame/notoriety/etc? Any new technology (especially one in the mainstream public eye) is susceptible to hacking and NGN is no different.

Future Fraud Threats
Future fraud threats will always be present. With the arrival of new technologies and services an explicit threat assessment needs to be carried out to uncover any major new threats, which can then be dealt with or mitigated. ‘NGN’ is usually motivated by the need for better utilization of resources, more flexible service offerings and capabilities supported, cheaper deployments, etc. To ensure that we are not caught off guard, it is important that we build future-proof fraud management systems, in order to deal with these threats as and when they materialize.

There will always be an NGN on the horizon which is likely to bring more flexibility for service and product creation, more breadth in service delivery, or more efficient use of resources (e.g. spectrum). This means that there will always be scope for fraud. There will always aspects of technology development that any well-to-do fraudster will have a close look at with a view to exploiting. For example:

- Faster service creation and deployment;
- More diversity and take-up of m-commerce applications;
- Introduction of any radically new pricing and charging mechanisms;
NGN fraud is basically associated with two categories of fraud offering solutions to combat them for just as long.

Typical examples are Wangiri, PRS Content, SMS-Spoofing, and Use of IP Spoofing (substitution of identity information is becoming more common, often to aid other frauds by offering in a loss of revenue for the terminating operator, this method may also be used to conduct “Dark Arbitrage”, “Gray Routing”, VoIP bypass fraud involves diverting legitimate fixed-line or mobile originating voice traffic into VoIP sessions. This results in a decrease of fraudster’s service revenue. An alternative example (from Japan) is where a trojan was released automatically use service without the subscriber’s authority or knowledge. This is commonly used to make premium rate calls that infringe revenues to the fraudster’s own service. An alternative example (from Japan) is where trojan was released automatically use service without the subscriber’s authority or knowledge. This is commonly used to make premium rate calls that infringe revenues to the fraudster’s own service.

Security viewpoint, this means that it is susceptible to all the attacks commonly targeted against data networks, even if use of next generation services, mean less scope and less motivation for fraud.

Meeting the Challenge – ROC Fraud Management

This section shows the capabilities that ROC Fraud Management has to combat emerging and future fraud threats. ROC Fraud Management has features which make it the best solution for tackling NGN threats on the market, both today and in the future.

a) Sound, Flexible and Modular architecture

ROC Fraud Management has a solid architectural basis, which makes it scalable and capable of meeting increasing volumes without limit. Next Generation services are multiplying and so is the volume of transaction records. Downloads, online gaming, messaging and other services can produce a vast increase in data volume. It is therefore necessary that the FMS has the scalability to process very large data volumes. ROC Fraud Management is able to scale from low volumes for small operators to very high volumes of a tier 1 operator for example. This scalability gives the operator confidence that the future volumes can be supported. ROC Fraud Management’s flexible and modular architecture enables to build and adapt new capabilities on top of the existing platform without having to re-architect the system. Next Generation Services can be significantly different compared to traditional voice and data transactions. The solution allows the fraud analyst to create a rule through the GUI screens which takes immediate effect. The rules can be on any type of service and are tailored to provide thresholds which are relevant for the new services. The Smart Pattern capability and advanced rule logic allows rules to be combined to target very specific behavior and alert the analyst.

b) Data Input Flexibility

ROC Fraud Management can take in and use any form of information (data). Its flexible ETL layer allows processing of usage records for NGN services and allows the solution in detecting NGN frauds using rules and other advanced analytic techniques. Next Generation is introducing new services rapidly which in turn provide new event records and customer data attributes. It is necessary to have a system in place which is able to introduce a new record type for analysis quickly in order to perform fraud analysis on the service or customer. ROC Fraud Management uses the Diamond, Extract Transfer & Load component to add or amend service event records using only configuration. New record types can be decoded, enriched and output all via the use of the GUI configuration.

c) Powerful and flexible detection techniques

ROC Fraud Management uses techniques such as rules, profiles, analytics, and Artificial Intelligence technology to adapt to emerging behavioral trends. Rules based analysis provides fast prevention and detection. As soon as the potential for fraud...
has been identified by the Fraud Analysts or a weakness identified it is necessary to introduce a new rule quickly to ensure alarms are raised for this new fraud type. ROC Fraud Management uses its rules technology and powerful GUI to enable the immediate creation and effectiveness of new rules or amended thresholds.

Some common services monitored for fraud detection in a 3G environment are

- Video Calls
- Mobile to Web Call
- Web Call to Mobile

**d) Powerful prevention techniques**

ROC Fraud Management is focused on fraud prevention and offers many optimal detection and preventative capabilities:

Reducing Fraud free-run time

- Enabling real-time reactions to identified fraud cases through
  - in-line service controls
  - Transaction controls
- Active Probes and/or Web Services
- Pre-qualification of fraud alerts through advances AI techniques to prioritize investigation of most likely fraud cases

*Eliminating known fraudsters*

Pre- and Post-acquisition profiling to identify potential fraudsters

- Fraudster profiling to prevent potential/ known fraudsters from entering the network
- Hot listing of fraudsters/ credit cards/ equipments

*Augmenting internal controls for fraud prevention*

Reinforcing internal controls/ processes

- Strengthened internal controls through enhanced auditing and logging
- Data privacy controls and enhanced security and user management

*Continual FM Process Improvement*

Improving FMS performance through monitoring and periodical reviews

- Improving FMS performance continually through Cognitive Analytics Program and Subex’s Consultancy Services
- Rule Test facility for improving rule performance

Knowledge Sharing

- Inter-operator collaboration through Subex User Forum and User conferences to share fraud-related information/ best practices
White Paper  Combating Existing and Future Fraud Threats

ROC Fraud Management allows Wireline and Wireless, Satellite, IPTV, 2G and 3G telecom operators to detect and investigate both traditional and next-generation frauds in order to prevent and minimize revenue leakage. The solution enables operators to guard against malicious fraud attacks on next-generation services with greater efficiency, increases analyst productivity in the next-generation environment without increasing operational cost. Suitable authorized Fraud Analysts can change configuration of the software, thereby enabling the operator staff to be self-sufficient and provide immediate protection. Rules can be configured in accordance with customer specifications and monitor any aspect of service.
About Subex
Subex Limited is a leading global provider of Business Support Systems (BSS) that empowers communications service providers (CSPs) to achieve competitive advantage through Business Optimization - thereby enabling them to improve their operational efficiency to deliver enhanced service experiences to subscribers.

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

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

Subex’s customers include 28 of top 50 operators worldwide* and 33 of the world’s 50 biggest# telecommunications service providers. The company has more than 300 installations across 70 countries.

*GTB Carrier Guide, 2011
#Forbes’ Global 2000 list, 2011