Telecoms Fraud Management
Who is winning the Battle?

A Praesidium Business Consultancy White Paper

MARCH 2011

WeDo technologies
Assuring your Business for the Future

praesidium
WeDo technologies • Consulting division

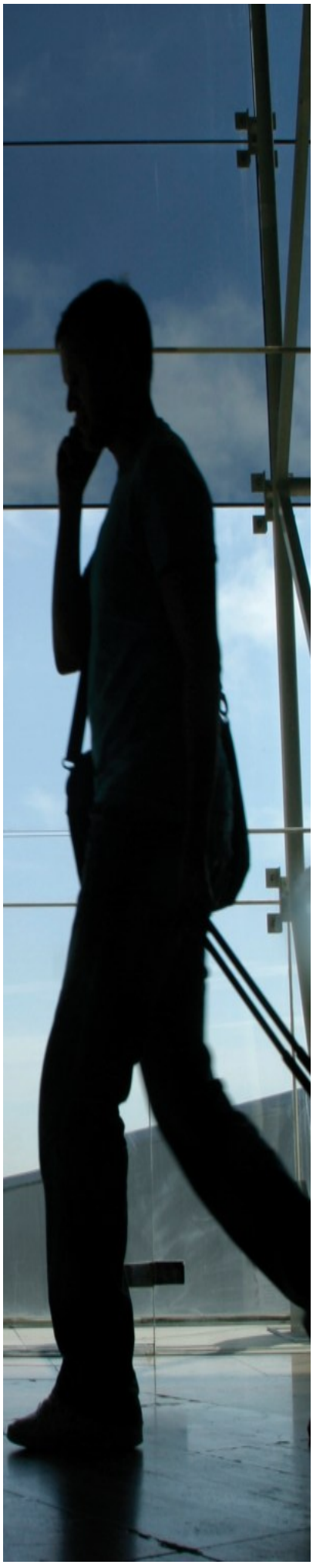


Table of Contents

Telecoms Fraud Management - Who is winning the Battle?

Fraud management within most Communication Service Providers (CSP) is now an established Risk Management discipline. It evolved from being an activity performed within Customer Care or Credit Control that was primarily directed at customer airtime monitoring. It is now recognised as a business risk that requires its own fully qualified and trained resources who have access to leading technological solutions to effectively manage the control, prevention, detection and investigation of illegal acts committed against the business.

Essentially 'fraud' means different things to different people and cultures globally. At it's core, is the basic principle that fraud is all about the "intent" to commit an illegal act and revolves around this dishonesty, deceit and intent to obtain a product or service illegally. Telecoms fraudsters are becoming more innovative in their techniques and the services and products they target. CSPs sometimes forget that highly organised fraudsters are actually running their own business and have their own 'customers'.

Highly organised fraudsters are actually running their own business and have their own 'customers'.

This business approach to committing fraud, especially across international boundaries, relies heavily on the CSPs inability to respond and recover in a timely manner. In all cases, the odds of being successful heavily favour the fraudsters as they know and determine exactly when the fraud hit will take place.

It is essential for the CSP to continually consider the fraud risk as it is not a single event, but something that must be continuously assessed as the business evolves. Præsidium often indentifies CSPs who are set in their ways or have consistently weak methods of controlling fraud exposure or they simply do not understand the fraud phenomenon. CSPs will either adopt a 'wait and see approach', or they take a 'this is how we have always done it' approach. They will rely heavily on existing practices to protect the various revenue streams without ever thinking how a fraudster actually operates and would defraud them.

How Big is the Problem?

In recent years, the telecoms industry has witnessed more well organised and financed criminal gangs operating across international boundaries who target specific telecoms services to maximise their revenues. The industry quotes fraud losses in the $ Billions globally through industry bodies such as the GSM Fraud Forum or Communication Fraud Control Association (CFCA), although no accurate industry figures are disclosed due to commercial sensitivity.

One fact is certain, that telecoms fraud has steadily climbed over the years and is definitely on the increase.

One fact is certain, telecoms fraud has steadily climbed over the years and is definitely on the increase. CSPs are still reluctant to provide information on the true levels of fraud being suffered or are not in a position to actually determine the extent of losses. The problem is not being adequately controlled and the level of concerted fraudulent attacks is actually increasing and not decreasing. Fraudsters were previously considered to be 'opportunists', but experience shows they are now seeking out their prey by targeting specific CSPs or services that provide the greatest revenue return but at a substantial cost to the CSP.
Fraud loss is not something that is recoverable, it is not like a revenue leakage issue that can be corrected or easily recovered from once detected. Fraud is a continuous battle with ever changing rules of engagement, and therefore effective fraud management requires a specific mindset, approach and strategy.

Telecoms Fraud Types

The types and severity of fraud attacks will primarily revolve around the market environment the CSP is operating within and will relate to the range of products and services being offered or planned for. CSPs have business plans in place to determine the innovative products they will provide to the respective customer segments (corporate, business and residential). The criminal fraternity are also actively determining their own 'business strategy' for defrauding what is provided.

Fraudsters will predominantly target the softer option – the easy target.

Fraudsters will attempt to maximise their revenues by either performing; a concerted fraudulent attack, e.g. combining roaming fraud with international revenue share to premium rate service (PRS) or, a prolonged attack across a range of products or services, e.g. organised subscription fraud linked to handset subsidy abuse.
What needs to be factored in when considering a CSP's exposure, is that fraudsters will predominantly target the softer option – the easy target. They will have performed their own assessment of the business culture towards fraud and validated the customer take-on procedures. They will ensure they identify weaknesses within the CSPs operating procedures to ensure they can maximise their fraudulent revenue generating opportunities.

A Successful Fraud Management Strategy

What needs to be considered is that fraud can result from failures within technology, the method used to deploy and deliver services or through organisational and procedural weaknesses. However, these very same areas of concern should also be the key elements for formulating the defence mechanisms as there is no single solution to the fraud problem. What is needed is a balanced approach that takes into consideration Technology, People and Processes working together to create an effective Fraud Strategy. The purpose of a Fraud Strategy is to ensure an appropriate mix of people, processes and tools are in place, supported by Executive Level Management. This will enable effective defence mechanisms to be deployed in the right places at the right time.
Based on Præsidium's extensive international experience of assessing the fraud risk across all technologies in CSPs ranging from Tier 1 to Tier 3, there is still a degree of uncertainty with regard to what exactly constitutes fraudulent behaviour.

This position reflects largely on the areas Fraud Teams are asked to focus on, their overall remit and areas of responsibility and on the level of authority they have to act in the best interests of the business. These considerations differ greatly from CSP to CSP and even considering different Telecoms Group approaches to managing fraud – there is no definitive right or wrong way. CSPs will not find a defined template or an all-encompassing industry model. There is definitely not a 'one size fits all' model for fraud management.

Within the industry, there are common fraud types and incidents being reported and these will come from a number of different fraud scenarios including:

· Subscription Fraud	· Financial Fraud
· Internal Fraud	· Dealer Fraud
· Technical Fraud	· SMS/MMS Fraud
· Prepaid Fraud	· Voicemail Fraud
· Value-added Services Fraud	· Call Forwarding/Diversion Fraud
· Social Engineering	· Theft of SIMs/Handsets/Cards/Packs
· Roaming Fraud	· SIM Cloning
· Audiotext/Premium Rate Fraud	· Bypass/GSM Gateways/SIM Boxing
· International Dial Fraud	· International Revenue Share Fraud
· Payment Fraud	· Interconnect Fraud
· PBX Fraud	· E & MCommerce Fraud
· 3rd Party Fraud	· Modem Hijacking

The purpose of a Fraud Strategy is to ensure an appropriate mix of people, processes and tools are in place, supported by Executive Level Management.

The approach must take into consideration the requirements of the business model when determining and subsequently deploying a coherent fraud strategy. What is essential either within a CSP or across a Group strategy is to encourage centralised reporting and accurate visibility of fraud threats and risks. To achieve this, it is critically important to have a common understanding of exactly what constitutes a fraud threat to the business and to define who has responsibility for managing that risk. CSPs who have a fragmented approach fundamentally fail to provide the required levels of protection.

Effective fraud management is the process of ensuring the control, detection, investigation and ultimately prevention of fraud risk – no CSP will ever be 100% 'fraud free' - it is a cost of doing business in a highly competitive environment. The ultimate aim for ensuring effective fraud control is to ensure that a common understanding for the fraud strategy is defined regarding the fraud risks the CSP or Group are facing and the best methods for mitigating these risks via technology, processes and people. An effective strategy will typically involve common organisational and reporting structures e.g. Fraud Team reporting to the CFO and more increasingly merging with the Revenue Assurance Department or within a broader risk management structure deploying Enterprise Risk Management.

There is definitely not a 'one size fits all' model for fraud management.

There are others looking at the technology changes envisaged and identifying synergies with security management, and considering longer term what their response will need to encompass. Whatever approach is taken, it is important to consider the relevant skill sets of the fraud management personnel and how these will need to be enhanced to meet the increasing technically proficient criminal element. Whatever strategy is defined, there are some core requirements that must be considered and communicated across the business to ensure a focused and concerted response is implemented:

Empowerment
For effective fraud management, it is imperative that Fraud Teams are empowered to act in the best interests of the business to proactively identify fraud and protect various revenue streams in a timely manner. This fundamental requirement has to be mandated 'Top Down' from the Executive Level and fully understood by the business divisions. Failure to respond to concerted and organised fraudulent attacks will result in substantial financial losses, negative public relations and potential share value falls.

Failure to respond to concerted and organised fraudulent attacks will result in substantial financial losses, negative public relations and potential share value falls

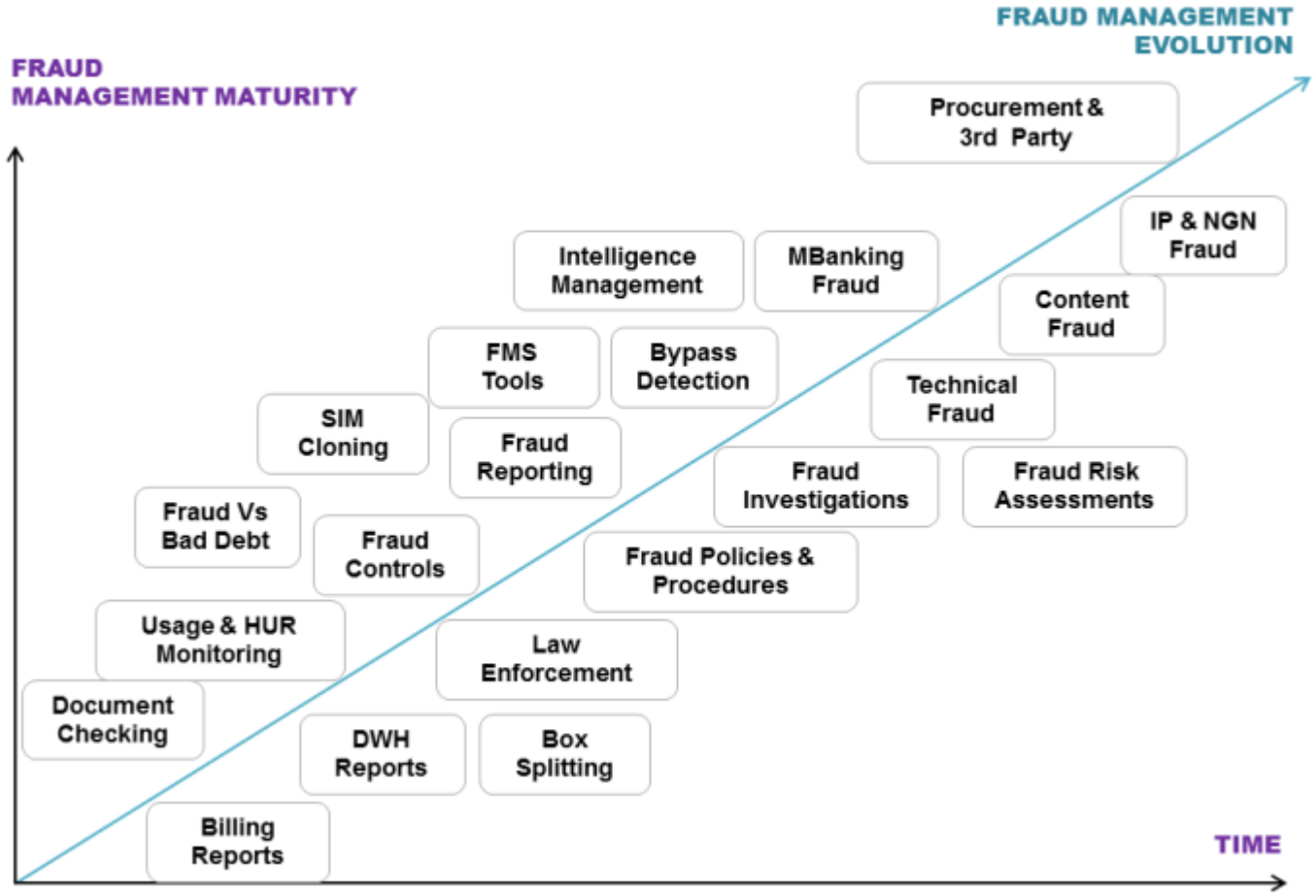
Controls Coverage
Fraud Teams essentially require visibility and access to information to be effective. They are heavily dependent on their own organisational structure and the potential for instances of fraud being notified to them by external entities, such as: customer complaints, media reports, other operators, intelligence sources or industry forums. All too often, Fraud Teams have no real visibility in a particular business area that can signal a fraud concern or alarm on suspicious behaviour. An efficient and effective Fraud Team must have a clear understanding on which areas of the business are effectively controlled and which ones are not. A fraud type that is being 'monitored' still requires specific intelligence about that particular situation and active controls to highlight suspicious activity. Therefore, defining fraud coverage is a key requirement.

Ownership
A fraud situation must have a clear owner, who is fully authorized and empowered to deal with the issue in an effective and timely manner. For the simplest frauds, this is normally straightforward (i.e. responsibility resides with the local Fraud Team to suspend a fraudulent customer for airtime abuse). However, in cases of serious and concerted fraud attacks, the organization can sometimes go into a state of 'shock' without appropriate guidelines on how to effectively react and who should take responsibility for dealing with the situation.

Concerted frauds cases will increase financial exposure with escalating losses while the business is still determining an appropriate response and definitive course of action.

All too often, concerted fraud cases will increase financial exposure with escalating losses being experienced while the business is still determining an appropriate response and definitive course of action. Therefore, defining overall ownership for taking direct action is a key requirement.

(Continued on page 6)



FRAUD MANAGEMENT EVOLUTION DIAGRAM

Responsibility Gap
In some situations, there is a fine line between who has responsibility for responding to an attack, as it could fall under the responsibility of the Fraud Team, Internal Audit, Network Security or Information Security. In complex frauds, these different functions must collaborate to determine who will detect, investigate and resolve the case.

While this is a positive initiative, it also has a side effect, where it can sometimes create confusion regarding who exactly is responsible for what.
A classic example would be handling Technical frauds. In many CSPs, Fraud Teams assume this responsibility will fall within the Technical Department, and the Technical Department will assume the Fraud Team is in charge of all fraud risks.

Remit & responsibility of the Fraud Team must remain clear in order to highlight any 'responsibility gaps' – areas outside their competence or under other risk functions.

Fraud Management Evolution

The diagram above is not intended to cover all aspects of fraud management, but highlights how the scope of activities has continuously increased and developed over time and is inextricably linked with the range of products and services a CSP launches. It also demonstrates there are far more areas for Fraud Teams to be concerned about which have little relationship with the invoice value – new products and services, Intelligence Gathering, Bypass, Content, M-Banking risks amongst others.

In some CSPs, while the main revenue sources may come from Prepaid, there are still few controls in that area with the attitude that prepaid is 'fraud free'

Essentially, most CSPs started with the creation of a Credit & Collections Department, in charge of ensuring that postpaid customers spend was controlled and their invoices paid on time.
These old working practices and principles still apply, creating big responsibility gaps and therefore, increased fraud risk. In some CSPs, while the main revenue sources may come from Prepaid, there are still few controls in that area with the attitude that prepaid is 'fraud free' still being frequently quoted! CSPs fail to consider end to end prepaid risks to determine the required levels of protection.

While the type of products and services continue to evolve, fraud management aspects will be different and have a more technical component. A failure to encompass the full range of products and services or the full areas of a product (especially prepaid) in the Fraud Management scope of activities will result in unavoidable financial losses.

People, Processes and Technology

To effectively manage fraud and underpin the implementation of an effective strategy, there are 3 key elements that must be aligned – the *people* employed to detect and prevent fraud, developing clearly defined *processes* and the use of effective *technology*. *By* combining these elements into their fraud management requirements CSPs will have an ability and realistic opportunity to win the battle.

People
Fraudsters are basically people who deploy different tactics and techniques to defraud a CSP; they look for inherent weaknesses, exploit gaps in business processes or will look to attack from within the CSP via internal fraud. Therefore the personnel within a CSP must be viewed as being one of the main business assets in protecting the business. This definitely applies to the Fraud Team where having relevant expertise is paramount. However, actually recruiting qualified and experienced fraud professionals can be a difficult task, especially in countries where fraud functions are relatively new disciplines. This means an ability to source the correct personnel is a difficult task when local fraud knowledge is scarce.

Recruiting experienced fraud personnel can be a difficult task, especially in countries where fraud functions are relatively new areas.

So how can fraud be effectively managed without experienced resources?
There are two main ways to approach this position, firstly identify people within the business who have the right 'mindset' to effectively detect and prevent fraud. Key skills requirements include an enquiring and analytical mind, being inquisitive by nature with good communication skills and more importantly providing them with defined training.
This training must ensure they become proficient in appreciating the range of different frauds, the various techniques used and the rationale and behaviour of a fraudster. Ultimately they must be trained to 'think like a fraudster'. The other route is to consider deploying a managed service for fraud management as a cost effective alternative to employing personnel and deploying tools. By utilising the services of companies such as Præsidium, who employ highly experienced fraud professionals, coupled with the ability to detect and manage fraud events via WeDo's Fraud Management System - RAID:FMS, CSPs can obtain a quick and effective response to managing fraud. Compared with the cost and time required to recruit and train personnel to be fraud specialists, coupled with Capex costs and the time needed to deploy a state of the art fraud solution, it is clear why the business case for using managed services makes complete financial sense for certain CSPs.

Process
There is clear evidence that robust and enforced business processes contribute to effectively controlling fraud exposure. However, defined fraud control frameworks and supporting processes for managing fraud need to be customised to the CSPs situation due to the complex and ever changing nature of both the products and services offered and frauds perpetrated. Processes must be defined initially at a strategic level to demonstrate the key stages of detecting, managing and preventing fraud.

Processes must be defined initially at a strategic level to demonstrate the key stages of detecting, managing and preventing fraud.

These should then be filtered down to create tactical tasks as the fraud organisation matures to ensure clear working practices are followed. Over time the processes should be further developed to ensure effective fraud reporting structures are implemented, together with the capability to measure and report on losses being experienced.

Tools
The final element to support the fraud control environment is to deploy and utilise technology for early detection and prevention of fraud relating to the specific CSP technology deployed. This can range from bespoke solutions developed in-house, for example, on the back of the billing system or data warehouse to state-of–the-art commercial FMS, through to bypass detection technology and analytical software tools.

The most critical aspect of deploying technology is selecting tools that will not only fit the current fraud management requirements but also take into consideration the CSPs requirements for the next 3 to 5 years. Coupled with this, is selecting a preferred vendor who will partner the CSP, provide strong support and will be forward thinking in its approach to fraud management. The vendor must possess and demonstrate that they have the necessary knowledge and expertise in fraud management to develop their system. They must also understand the complexities of fraud management for advanced products and services and the risks associated with deploying new technologies.

Fraud Management System (FMS)

An FMS is a specific tool designed to quickly and effectively detect, manage and report on fraudulent events (internally or externally) which ultimately impacts the revenue and cost streams of the business. No FMS has the capability of providing an 'all-in-one' solution – to be effective, the FMS has to be used in conjunction with Fraud Analysts who possess sufficient skills to understand the FMS output. They must have the information presented to them with effective processes to direct the Fraud Analyst through the investigative stages, but most importantly there must be a clearly defined strategy for the FMS.

To be effective, the FMS has to be used in conjunction with Fraud Analysts that have sufficient skills to understand the FMS output.

Essentially, the FMS processes data from the CSP and its partners and applies a number of different rules, profiles and data analytics to verify if the customer, employee, dealer or third party is using the CSP's network and services to commit fraud. Whilst the FMS is an automated tool that can operate in near real time, all too often the FMS is viewed as the ultimate answer to detecting and managing fraud. There is a misguided view that by purchasing an FMS, there is little more to do than 'press a few buttons' and all your fraud problems will be solved! It is vitally important to understand from the very beginning, that an FMS is essentially a tool that is only as effective as the Fraud Analysts using it.

An FMS has to be regularly 'tuned' and optimised for it to remain effective and reduce 'false positives' (raising alarms that are not actually fraud). It should be used as a tool that provides the initial indicator of a potential fraud. This then leads onto the second stage of further investigation and analysis, to confirm whether the case is fraud. Whilst some FMS can be automated to take the second stage decision of 'fraud' or 'no-fraud', it is this second stage that requires the skills and expertise of Analysts to fully determine the modus operandi of the fraud and to draw the correct conclusions to the case. Therefore, it's the combination of using technology and the skilled fraud professional that is the main armoury a CSP requires for winning the battle against the fraudsters.
There are some key elements of a FMS and how it should be used by the Fraud Team to ensure it is providing the required benefits and levels of detection – the 'hit rate'. It has a number of features and benefits over manual processing of data to monitor customer behavior.

Near Real Time
Most FMS operate in near real time if data is taken directly from the source systems or passed with minimal delay from a mediation platform. This ensures Fraud Analysts are quickly aware of customer airtime related activities which are breaking defined rules, thresholds and profiles in order to act fast in determining if the case is fraudulent.
The quicker the resolution of the case, the less money the CSP will lose, therefore, timeliness of both the data feeds and the generation of alerts and cases themselves are of paramount importance to the success and return on investment of an FMS.

Benefits of a Fraud Management System

Automation
The extraction and processing of the relevant events is performed with little or no human intervention. The FMS has the ability to interface to many different data sources to ensure visibility and coverage of usage on a wide range of products and services.

Volume and Quality of Data
The volume of data a dedicated FMS can process is typically far in excess of any that a homegrown solution developed within a CSP can handle. The quality of data used and monitored within an FMS is also high since it is usually retrieved directly from the sources or a mediation platform. This in turn produces a high level of clarity on what the origin of the data was, therefore assuring that frauds identified are based on accurate and reliable data.

Flexibility
FMS have to be flexible in their ability to take any type of data feed and to create flexible rules on any type of event to address the changing dynamics of fraud today and to address future fraud threats in next generation technologies and products & services. This flexibility is a major asset for the Fraud Analysts as it provides the capability to test and verify various thresholds and alarm settings to maximise their capabilities of fraud detection.

Dashboard
A dashboard view of the level and nature of fraud being detected within the FMS, visible in one screen is a key tool for a Fraud Manager. This allows the Fraud Manager to view key performance indicators (KPIs), assess whether fraud detection targets are being met, and review the performance of the Fraud Analysts to ensure cases are being managed and resolved in a timely manner.
Ultimately this enables the Fraud Manager to determine whether the FMS performance and resources are both operating in line with the fraud strategy and providing the required ROI.

Case Management
An integrated Case Management tool ensures all fraud incidents identified are recorded and tracked in a centralised location. This historical information can then be used to identify organised fraud syndicates and repeat fraudsters, where links are identified between new and old cases. In addition, it ensures that all information relating to a case can be stored for ease of retrieval at a later stage. This is essential when managing fraud where investigation or evidential case papers may be required for legal purposes or for review during internal audits. It also enables the Fraud Manager to track and monitor performance of the Fraud Analyst cases to ensure defined standards and processes are being met and adhered to.

Fraud Management – Can you obtain a return on your Investment?
Taking into consideration all the points highlighted, the primary aim of deploying a Fraud Team within a CSP is to achieve maximum fraud control with minimal expense.

However, the function is an overhead to the business like any other department and includes:
- Cost of resources
- Cost of technology
- Cost of time and resources of other business supporting áreas

Whilst it does not generate any ‘income’, it plays an essential role in ensuring maximum profits by protecting the revenue streams from intentional loss whilst also protecting the CSP’s brand.
The overall investment in fraud management must provide a positive return i.e. a reduction in fraud and a corresponding increase and retention of the company's net profits. In order to achieve a ROI, the Fraud Team has to internally ‘sell and promote’ the benefits and value of its existence to the business. It has to ensure the business and Senior Management view the Fraud Team as a revenue maximising department as opposed to an overhead. The Fraud Team needs to be seen as the in-house experts on fraud management and by taking this approach, support and appreciation of the Fraud Team will increase.
This can be achieved by:
- Selling the concept of fraud from the ‘top down’ – promoting the key benefits and attributes of the Fraud Team
- By aligning the fraud strategy and objectives with those of the company – common goals and objectives
- Educating the business on the role the Fraud Team plays – raising the levels of awareness including successes and where relevant stumbling blocks
- Effective management reporting of the facts and figures – ensuring visibility especially of high impact or organised fraud attacks
- Measuring the success of the department - KPIs to maximise productivity
- Being recognised as Subject Matter Experts in Fraud Management – open door approach

Effective fraud management is not only about controlling, detecting and preventing fraud, it’s also about being able to sell, educate, report and promote the requirement for it throughout the business.
For it to be effective different channels and techniques need to be developed by the Fraud Team.

Effective fraud management is not only about detecting and preventing fraud, it’s also about being able to sell, educate, report and promote the requirement for it throughout the business.

Reporting and Measurement
One critical area where CSPs often fail is in effective fraud reporting and measurement. Without this, a Fraud Team will struggle to justify its existence and to promote its successes. Senior Management are sometimes blind to the real cost and impact fraud is having on the business without this knowledge.
Additionally, as the investment in technology such as that for an FMS is a large Capex expenditure, this must have a sound business case which can only be achieved if reporting on the nature, level and extent of fraud is known.
Qualitative reporting is as important as quantitative where fraud risks are concerned.

Senior Management will want to know and be kept updated on:
- What are the key risks and the cost of fraud loss?
- What has been achieved to reduce the loss?
- What is the benchmarking status?
- What are the projected fraud risks?
- What are the immediate solutions?
- What is the longer term fraud strategy to control the risk?

Reporting and measurement can easily be achieved in a number of ways. Reports, presentations, briefings, email updates can all be used to consolidate fraud findings and losses and present a clear strategic summary on the level of fraud occurring.
Reporting and measurement should also include the concept of categorising fraud to determine the drivers for it i.e. what is motivating the fraudsters to target the business, what types of fraud are occurring, what channels are being used and what are the techniques being applied by the fraudster.

Summary

The battle against fraudsters will never be won due to the fast moving telecoms environment and the drive to launch more complex products and services quickly to attract market share and maintain a competitive advantage.

This will always lead to procedural weaknesses and technical risks being introduced which fraudsters will seize upon at the earliest opportunity to keep their fraudulent ‘business’ activities operational and profits high.

However, CSPs can deploy various defence mechanisms to mitigate against losses and ensure fast detection by ensuring processes are continually reviewed, staff are educated in new fraud trends, new products and services are assessed for fraud and security weaknesses and state of the art technology is used to quickly raise alerts for suspect activity.

The battle against fraudsters will never be won due to the fast moving telecoms environment and the drive to launch more complex products and services quickly to attract market share and maintain a competitive advantage.

Fraud management can be a time consuming and overwhelming activity especially for those CSPs who are not yet mature in the development of fraud control and prevention strategies.

Præsidium is able to support CSPs in this space, having served over 100 CSPs worldwide to review, advise upon and implement fraud management strategies, train fraud personnel, deliver and optimise fraud management systems or deliver the complete fraud management process as an outsourced service.

About Præsidium

Præsidium is a Global Business Assurance consultancy.
Founded in 1997, the company has successfully provided risk management consultancy to more than 100 Communication Service Providers in over 80 countries on 6 continents. Præsidium has gained solid recognition in the market amongst its substantial customer base and among global standards agencies. These include the GSMA Security Group & Fraud Forum, the Telemanagement Forum and ETSI.

Offices:
United Kingdom
Davidson House, Forbury Square,
Reading, RG1 3EU,
Tel: +44 118 900 1054
Fax: +44 118 900 1055

Brazil
Torre Rio Sul, Rua Lauro Muller 116;
27º Andar – Sala 2701
CEP: 22299-900 Botafogo
Rio de Janeiro
Tel: +55 21 2543-5419
Fax: +55 21 2543-5419

Ireland
Maple House,Temple Road, Blackrock,
Co. Dublin
Tel: + 353 (0)1 400 3900
Fax: + 353 (0)1 400 3901

Portugal
Edifício Picoas Plaza
Rua do Viriato, 13E núcleo 6 - 4º andar
1050-233 Lisbon
Tel: + 351 210 111 400
Fax: + 351 210 111 401

Spain
Edifício Cuzco IV
Paseo de la Castellana, 141 8ª planta
28046 Madrid
Tel: + 34 91 572 6400
Fax: + 34 91 572 6641

USA
3333 Warrenville Rd.
Suite 200
Lisle, IL 60532
Tel: +1 630 799 8081
Fax: +1 630 799 8083

On the Web **www.praesidium.com**
General Information **info@praesidium.com**

About WeDo Technologies

WeDo Technologies is the number one preferred supplier for revenue and business assurance software and services.
Present in 15 countries on 5 continents, with more than 100 innovative bluechip customers in more than 70 countries, the company has a solid and envious project management track record of being on-time and within budget while achieving superior customer satisfaction.
Business Assurance RAID®, WeDo Technologies' flagship software suite covering Revenue Assurance, Fraud Management and Business Processes Control has been implemented in a number of different industries where it has delivered significant business results and powerful return on investment.
WeDo Technologies pioneered the telecom revenue assurance space in 2002 and is now breaking new ground in the enlarged business assurance arena in Telecom, while also servicing the Retail, Energy and Finance industries.

Offices:
Portugal _ Lisbon

Portugal _ Braga

Australia _ Sydney

Brazil _ Rio Janeiro

Brazil _ Florianopolis

Chile _ Santiago

Egypt _ Cairo

France _ Paris

Ireland _ Dublin

Malaysia _ Kuala Lumpur

Mexico _ Mexico City

Panama _ Panama City

Poland _ Poznan

Poland _ Warsaw

Singapore _ Singapore

Spain _ Madrid

Spain _ Barcelona

UK _ Reading

USA _ Chicago

On the Web **www.wedotechnologies.com**
General Information **customerservices@wedotechnologies.com**