Fraud Management Issues for Smaller Communications Service Providers?

The mobile telecommunications market today is becoming more and more competitive, largely driven by the necessity of all CSP's to maintain market share, reduce churn, and to satisfy customers demand for the many new product and service offerings that today's new technologies allow. The ability of the larger tier 1 operators to react to this competitive environment by bundling services, using commercial relationships to develop and provide more services at less cost, and utilise their large Sales and Marketing teams to target certain market segments, can to a certain extent force smaller tier 2 and 3 CSP's to take more risk to get their own service offerings into the marketplace.

In addition to the increased risk faced by small CSP's to maintain their own market share, the challenge to reduce costs in the face of declining revenues, while maintaining service levels across the business can be a difficult one. The environment created by the growing competitive nature of our business has become ideal for the fraudster to exploit. The new technologies now being developed, along with the many products and services making use of increased connectivity, faster download speeds and multiple calling options all provide new opportunities for fraudsters to improve their own revenues.

This is particularly relevant to small CSP's or those new to the market. Much of our fraud is organised, and carefully planned by the organised fraud groups leaders, who are well aware that it is not uncommon for a smaller CSP to overlook, or delay introducing some basic fraud or revenue protection tools in their rush to get their offerings to market. It is known that often within days of a new product or service being released, Fraudsters will be carrying out their own penetration testing to determine just how they can exploit these for their fraudulent purposes. In many cases this testing will include routing their fraudulent calls through a number of CSP's networks and services to delay or confuse fraud identification and maximise their own profit. This may include for example using conference calling in one network, international call forwarding in another with PBX fraud in the 3rd, all designed to avoid detection for as long as possible. Fraudsters know that an extra hour of calling before a Simcard is terminated, when they have twenty or thirty of these in their possession, all making 6 simultaneous calls to a high cost termination number, makes the time they devoted to planning their fraud operation worthwhile.

Another issue working in the fraudsters favour is the resource and cost constraints often placed on smaller CSP's when developing their fraud management strategy. When demand for Capex and Opex budget is high, and exceeds that available for distribution within the business, fraud control may not be seen as a priority within many smaller CSP's and it is simply not possible to provide the same detection capabilities as a well-equipped Tier 1 provider.

The Impact of Fraud in Telecoms:

Recent surveys on fraud such as the CFCA fraud loss survey (2011) highlight how fraud is still a major issue for CSP's with 89% of the respondents stating that fraud losses had increased or stayed the same within their own organizations year on year. The headline figure for the industry extrapolated from the results of the survey show an average estimated loss of 1.88% of revenue to fraud.

However the percentage loss for smaller CSP's will in many cases be much higher than this, as that average figure is lowered by the influence of the major tier one European and US carriers, who make significant investment on fraud management tools and resources, so can maintain fraud losses below 0.25% of revenue on an annual basis.

Many smaller tier 2 and 3 CSP's, new entrants and those in emerging markets have reported losses of between 4-6% of revenues from fraud, figures which can have a significant impact on a smaller CSP trying to maximise profits and their growth potential.

The most common (and highest financial impact) frauds highlighted by the CFCA survey were;

- International revenue Share fraud (IRSF)
- By-Pass (Simbox) fraud
- Subscription/ID fraud
- PBX fraud

These types of fraud are the 'fraud of preference' for fraudsters as they generally result in extremely high fraud losses for an operator (and income for the Fraudster) within a very short time period.

Reported fraud incidents consistently show that even over short time periods, these events can result in losses of hundreds of thousands, or in extreme cases, millions of dollars to a CSP. While fraud losses at this level are significant for any CSP, many larger Tier 1 operators can manage the impact of them, however an incident on a similar scale targeting a small CSP is likely to result in a more serious financial impact, sometimes taking years to recover from.

It is known that Fraudsters will often target smaller CSP's, knowing that their internal resources, processes and fraud detection systems are generally not as robust and effective as in most larger operators, and consequently allow fraudulent activity to continue longer to maximise their profits.

Subscription and ID fraud impact all mobile operators but this impact can often result in greater damage to the smaller CSP who will often rely on their brand reputation, particularly as it relates to customer service as a service differentiator. Subscription and ID fraud is often an enabler for more serious frauds, and generally impact an existing customer somewhere during that fraud lifecycle. Generally a customer who is a victim to this fraud will question why their CSP allowed their identity to be used to facilitate this fraud, with the end result being increased churn, decreased ARPU and increased brand damage. The wireless industry provides unique opportunities for the fraudster when compared to the traditional fixed area of the business. We provide one or more high value handsets to a customer in circumstances that do not require a visit to his or her home address to confirm their residence, we allow them to take this handset roaming to locations where high roaming charges apply, but roaming call records may be delayed in delivery to the CSP, and we allow services such as International Call Forwarding and conference calling to assist a fraudster to inflate

their fraudulent income. Regretfully, some CSP's, knowing these risks, will not make the budget and resource available to manage them. On many occasions the fraud losses relating to just one attack could have funded the necessary fraud detection capability, such as that offered by a number of vendors, to significantly reduce these losses.

Fraud Management and the Smaller CSP's

Historically, smaller CSP's have not necessarily built fraud management departments during their initial establishment due to cost and resourcing issues. Often this function would be established after a significant fraud event has been experienced, or following an audit recommendation.

In establishing this function within an organisation, a smaller CSP must be careful not to believe they can simply assign a part time resource, with no fraud management strategy or effective fraud detection tools to manage this risk. To effectively manage fraud, any CSP must also be prepared to invest in the technology tools to support their fraud manager. A key focus in smaller CSP's should be deciding how to implement an effective fraud management operation with limited resources and budget. Generally it is believed that a fully functional third party fraud management system is too expensive, complicated and ineffective without the appropriate resources to manage it. This is often true as most third party fraud management systems are designed to manage fraud in large complex tier one environments where adequate resource and support infrastructures are in place. It is often the case within a smaller CSP that any detection methodology that is in place is based around basic network reports or a simple self-built alert system, as the operator avoids the "third party" option due to the perceived impacts on resources and budgets.

This approach can result in the fraud manager being swamped with inaccurate, late or irrelevant information that needs to be deciphered and understood in order to detect any possible issues. This can increase the CSP's fraud risk as these circumstances can result in delays in discovering a fraud incident, along with new fraud scenario's being missed.

The Smaller CSP's Fraud Managers' Challenges

The Fraud Manager within a small CSP has a challenging role, being expected to balance limited resource and budget to manage his organisations response to the complex and numerous types of fraud perpetrated against him, often by organised crime groups who have large budgets, unlimited resources and operate 24x7 without rules.

In developing their strategy, the Fraud Manager must fully understand the various types of fraud risk experienced in the industry to ensure that all aspects of the prevention, detection and investigation phases of these fraud types can be managed.

While implementing controls and strengthening systems to protect as much as possible against known fraud attacks, history has shown us that a CSP is unlikely to ever reach the point where they can announce to the business that they have identified and managed every fraud risk. While organised fraudsters are constantly probing our products and services to find yet another way of defrauding us that we have probably never even thought of the industry continues to develop and release new products and services which provide new opportunities for the fraudsters to exploit.

While the prevention aspect of fraud management is important, the detection element is equally important. If the Fraud Manager is going to accept that they are unable to identify and manage every fraud risk before it is exploited by the fraudster, then we must rely on effective fraud monitoring or detection tools to allow us to identify a fraud incident as soon as possible after it starts, find out what control weaknesses allowed it, then work with the business to block this vulnerability to prevent a reoccurrence.

We have already discussed how many fraud monitoring solutions in the market place are designed at Tier one levels, and by reason of total implementation and operating cost (including resource) are unsuited to many tier 2 or 3 operators. A common approach by many smaller CSP's once they realise that a traditional Fraud Management System is unsuited to an organisation of their size is to then develop in-house reporting or other basic alerting systems to manage their fraud detection.

For reasons already discussed, in-house reporting as a fraud detection tool is not always an effective strategy because of incomplete data, being resource intensive, not timely and generally inefficient. It's continued benefit also generally relies on one or two people who were involved in designing and developing the system being available to support it.

There are vendors now who have identified the fraud and RA requirements of smaller CSP's and for these operators with limited in-house fraud and RA expertise, there are also industry anti-fraud consultants who can fully explore your business needs and recommend suitable solutions.

Colin Yates
November 2012
colin@yatesfraudconsulting.com