Basset Telecom Report

The importance of **quantifying** fraud

Being able to quantify fraud and measure the damages related to fraud, enables organizations to realize the losses due to fraud and take appropriate actions. But it also requires a focused leadership and an organization in place that have the know-how to act proactively and quickly when fraud attacks occur.

How much fraud is there out there? And how can operators be sure they have the problem under control? It is true to say that nobody really knows the full extent of fraud. Operators, who claim that they have not been exposed to fraud, either lie, or have not yet been able to detect it. In general, operators do not publish statistics on fraud, and industry associations or national government agencies can only rely on what the operators are reporting.[Ref1] This is why the global telecommunications fraud statistics only can be an estimate.

ITU estimates that operators' aggregated yearly loss, on a global basis, is approximately 6 per cent of the aggregated turnover. [Ref 2] Other industry organizations claim that the total loss is 3 per cent, or even as high as 10 per cent. Translating this in to money means that operators loose perhaps 30, 40, or more than 50 billon USD, per year. The amount of money is so high that the FBI in the US estimates that mobile phone crime is even more lucrative than drug trafficking. [Ref3]

However, these 30, 40 and 50 billion USD that we usually consider as the industry fraud loss statistics are quite elusive, because as you dig further into the methods of quantification, it can be seen that calculations are based on subjective and individual standards. In other words, trusting fraud loss percentage and monetary figures on either industry or organizational level is difficult since the standards of quantifying fraud is still missing.

HOW TO QUANTIFY FRAUD

Currently when operators measure the impact of a fraud case, the monetary estimation related to the case is often only direct costs, i.e. costs related to interconnect, roaming or 3rd party providers. But there are more cost areas out there that should be taken into consideration, these cost components can be grouped into the category of indirect costs. Indirect costs include efforts made by different departments i.e. fraud- and billing department, customer service and operations, or alternatively the value of the lost opportunity, etc.

Although some industry associations are trying set up standards or frameworks to help operators in measuring and classifying fraud, which can be very helpful, we doubt to what extent unified norm are possible. Our reasoning is that, according to experience, all operators are independent and driven by their own business strategies and risk appetite. This means all standards, if there are any, need to be catered to the level that they can perform their own quantification and analysis. The responsibility lies on the operator to take advantage of the standard definitions provided by industry associations.

WHO IS THE OWNER OF QUANTIFYING FRAUD?

To achieve the appropriate level of fraud quantification, it is important that the right person within the organization owns the function and that he or she has the proper level of overview. Depending on whom you ask, you usually receive different answers based on which function this person holds. If the network team is responsible for quantifying fraud, the result would be presented and measured in traffic minutes; while when the fraud department is taking the drive, the result would be presented as monetary direct costs related to the specific fraud case.

Our recommendation is that the only person that can and should be ultimately responsible for quantifying fraud is the company CFO. The reason is because the CFO has a wide range of responsibilities; from financial planning, record keeping, reporting financial risks to management. This enables the CFO to have the right overview to handle fraud loss quantification cross-functionally, and ensures that all company aspects that needs to be considered are included in the calculation, both direct and indirect costs.

An operator must be driven to measure and quantify fraud for the benefit of the company; and only at C-level this view is visible.

An operator must be driven to measure and quantify fraud for the benefit of the company; and only at C-level this view is visible. First of all, surely we shouldn't compare apples and pears. The operators need to create a long-term strategy which states what should be quantified, how it should be classified and what KPI's that should be used to present it. By performing an as-is evaluation it will allow the operator to come to a current situation analysis, this as a starting point for measuring the result of their efforts. Without a starting point it is not possible to see the future result of the actions taken. This can make the analysis of the quantification false or misleading. For group operators, where the quantification is spread across countries, cultures and managers, it is even more important that it is performed on a group level, allowing different operations to measure and compare fraud cases identically.

Another important purpose of fraud quantification is to understand the break-even level Ref: Graph page 6 which shows when your efforts to combat fraud exceed the monetary value secured. How should you set your goals in combating fraud? And for how long should you continue to chase the last few fraud cases that might cost more than what could be actually saved? And the only person that is able to maneuver the trade-off is the CFO, as he or she is supposed to decide what financial risk the company is prepared to take as it sits within this role to decide what financial risk the company is prepared to take.

To turn fraud losses into increased profit all starts with a structured model of quantifying fraud owned by the right person within the organization. According to our beliefs and research it has shown that this is best done by the CFO.

To turn fraud losses into increased profit all starts with a structured model of quantifying fraud owned by the right person within the organization. According to our beliefs and research it has shown that this is best done by the CFO.

THE IMPORTANCE OF A FRAUD STRATEGY

Let's face it; there are amongst many, two key reasons why all operators should set up a fraud strategy:

1. **Rational:** To justify the departments function and staffing. Perhaps even increase it.
2. **Personal:** Increased visibility is appreciated and recognized within the organization and by being in control makes you sleep better at night.

There is a challenge in creating and maintaining the reports and KPIs. It involves quite a lot of work and it is important to keep a certain structure. This is why operators need to develop a strategy. A strategy that helps to set a plan and organize the necessary tasks. Why not just use the common KPIs in the market and stick with that, you may think. And the answer to that is simply: Because it's wrong.

It is probably better than not doing anything at all, but once again; Is it really what is in line with your company's expectations? There is a clear risk of not having a correct strategy, which is confirmed by the below statements:

- **You** are not focused and do not know how or when to evolve your strategy. The strategy helps you to focus short and long term. It allows you to review the strategy on a yearly basis in order to ensure the strategy is in line with the company's expectations.
- **You** are actually only reporting to yourself. Even if you pass on the reports to upper management, it won't be the information they expect.It will only be a useless report.
- **You** do not have the complete picture. And without a strategy you do not know where to aim and will not know if the focus and efforts are effective.
- **You** do not know if or when the targets are met.

By setting up a proper strategy you will see that it is well spent time. From a C-level perspective it sets the structure and goals for what the fraud department will achieve and the strategy can be set together between the fraud manager and the CFO. Concerning which KPIs and reports to extract, consider the following:

- **Requirements:** What are the company's requirements of the fraud department and how can it be realized into something measurable?
- **Audience:** Who are you presenting this to? Who are the stakeholders?
- **Form:** How does the audience use the information and will it be summarized into another report and passed on?
- **Targets:** Define targets and milestones that can be measured. These are the items all activities should strive to achieve over time.

The result from the bullets above is enough to build a strategy around which KPIs and reports to maintain. The strategy has now become a tool for which milestones to achieve during a longer period. Of course the exact content is still to be worked on and it is vital to have a well-structured and defined fraud classification.

THE ISSUE OF FRAUD CLASSIFICATION

After deciding the owner of fraud quantification and defining the strategy, the next step is to get to the actions. How to start? Most organizations would probably start by drafting a strategic plan. However, while a formal fraud mapping strategy can look good on paper when presented to the management, a very important question is often forgotten before proceeding: how can the fraud team conduct accurate fraud quantification without clearly defining what it is they're dealing with? And the pitiful fact in the industry is that it's a complete mess when it comes to fraud classification and terminology. During modern fraud management's more than 15-years of development, no rules or accepted industry standards have been established on this matter. The result is that fraud practitioners often apply fraud term randomly in different manner. For example, the following case can be applied in any of or all of the fraud types: subscription fraud, roaming fraud, PRS or IRSF…

The Case:

A fraudster obtains service in *Operator A* using a fake identity, travels aboard and generates thousands of calls in the network of *Operator B* to a PRS number he owns in another country.

And a subsequent impact is that when the fraud team tries to note down some fraud cases for the purpose of intelligence gathering, knowledge sharing, trending, benchmarking or reporting, they may end up talking in different languages, thus it does not lend itself to understanding or quantifying what the underlying threats are. It can also lead to double counting one fraud case when reporting. Therefore, we believe that until the step of fraud classification is completed and aligned within the organization, any efforts to try to quantify fraud and implement controls will remain fruitless.

A more alarming fact is that this problem is usually ignored or considered minor importance by the fraud team, but it has to be addressed if quality operational and management reporting on fraud loss is wanted. We suggests operators to start addressing this problem by designing a policy norm on rules for determining fraud type. And test analysis would be required with simple examples to check for consistency.

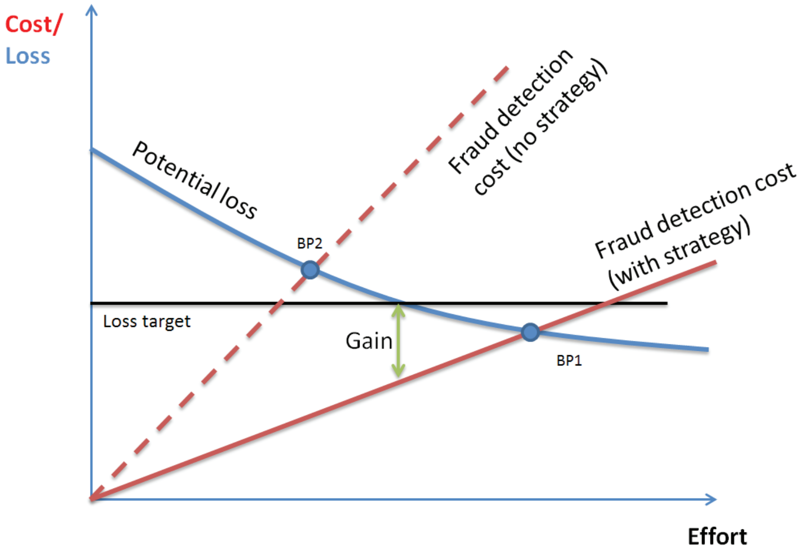
THE COST VS REWARD

An important aspect of a fraud strategy, as mentioned above, is to define the target. And a target must be set so that it includes both the potential gain and the fully loaded cost.

Potential gain: in this value one shall include the fraud loss (maybe also including leakage) that will be saved/avoided by implementing the fraud detection measures included in the strategy.

Fully loaded cost: summarize all costs involved with fraud detection, such as fraud staff salaries, training cost, time value contributed by staff in other departments (e.g. networking), and cost of tools and so on.

In a very simplified graph the y-axis represents value ($) and the x-axis the efforts put in. The fraud loss will decrease when more effort is put into the detection, and likewise the fully loaded cost will increase with the efforts taken even. This creates a typical "break-point" graph as shown in the picture on next page:



Two break-points are visualized: one (BP1) where the operator has implemented a fraud detection strategy – and therefore works more efficiently = flattening the curve. The other break-point (BP2) represents a scenario when no clear strategy is in place – and most likely increases the relative cost (haphazard investments, temporary or inefficient staff, long term consultants etc.).

However the main point of the graph is to show that a target can only be defined after calculating/ estimating the two curves; potential loss and total cost. Otherwise the cost may overshadow the net gain (as in BP2). In contrast, a correctly set target as part of an implemented strategy will instead result in the green arrow “Gain”.

IN CONCLUSION:

- Trusting fraud loss percentage and monetary figures on either industry or organizational level is difficult since the standards of quantifying fraud is still missing.
- The monetary estimation related to the case is often only direct costs, i.e. costs related to interconnect, roaming or 3rd party providers. But there are more cost areas out there to be taken into considerations, and those cost components can be grouped into the category of indirect costs.
- To turn fraud losses into increased profit all starts with a structured model of quantifying fraud owned by the right person within the organization. According to our beliefs and research it has shown that this is best done by the CFO.
- An important aspect of a fraud strategy, as mentioned above, is to define the target. And a target must be set so that it includes both the potential gain and the fully loaded cost.

REFERENCES

Ref 1 *TIA's 2011 ICT Market Review & Forecast*

Ref 2 *TIA's 2011 ICT Market Review & Forecast*, ITU, ENISA

Ref 3 *Government Technology's Digital Communities*, www.govtech.com/dc/628001

BASSET TELECOM REPORTS

Basset Telecom Report is an annual series of White Papers. They provide an overall summary of the challenges operators are facing in the next generation network marketplace, and what operators need to consider and understand in order to be an effective, attractive and profitable player. The Basset Telecom Report consists of four white papers, covering the following specific areas: Roaming, Interconnect, Fraud in the next generation networks and Quantifying fraud in the next generation networks.

BASSET

Basset is a global provider of Business Support Systems for telecom operators within inter-operator billing and revenue assurance. As an advisor we are committed to help operators get more out of their business by providing solutions within inter-operator billing and revenue assurance that ensures operators get paid for every transaction in their network.

Basset serves more than 70 customers in 65 countries. Basset helps several operators growing their business and reach operational excellence in more than one domain. Among Basset's customers are Zain, Telefonica, Millicom, Globe Telecom, Etisalat, Tele2, Cable & Wireless, Vodafone, Orange and Airtel. Working with so many operators around the world has given Basset the experience that makes them the ideal partner when operators want to grow their businesses.

Basset is a part of the Kinnevik Industrial Group, which was founded in 1936, and is one of the largest listed investment companies in Europe. Please visit: www.bassetglobal.com for more information.

Phone: +46 (0)8 562 676 00
Fax: +46 (0)8 28 62 31
Löfströms Allé 6C PO Box 1156
SE-172 23 Sundbyberg Sweden
www.bassetglobal.com