Classification, Detection and Prosecution of Fraud on Mobile Networks

Phil Gosset[(1)] and Mark Hyland[(2)]

(1) Vodafone Ltd, The Courtyard, 2-4 London Road, Newbury, Berkshire, RG14 1JX, England

(2) ICRI, KU Leuven, Tiensestraat 41, B-3000 Leuven, Belgium

Abstract

This paper provides an overview of fraud classification, detection and prosecution in the mobile domain. It objectively generalises what is otherwise a very subjective field, by dividing frauds into one of four groups, namely Contractual fraud, Hacking fraud, Technical fraud and Procedural fraud. This approach simplifies the following discussion. The legal work here largely relates to the UK, although the discussions are thought to be generally applicable.

Introduction

Fraud is a constantly evolving, many-facetted creature. When the first analogue mobile communications networks were launched, weaknesses in the security, particularly the lack of encryption of both the voice channel and the authentication data made the networks susceptible to eavesdropping and cloning. As the technology evolved from Analogue to Digital (GSM), so the nature of fraud changed as it became more difficult (and more importantly expensive) to eavesdrop and clone, and this led to a shift away from technical fraud towards more procedural and contractual types of fraud. However the possibility of technical fraud cannot be ruled out forever in GSM - as one door is closed on a fraudster, so the fraudster will attempt to open others.

It is estimated that the global mobile communication industry currently loses $25 billion per annum due to fraud. This makes the detection, prosecution and prevention of fraudulent activity important objectives for the mobile communications industry. If these objectives are to be achieved, it is clear that additional security steps need to be taken in GSM and future UMTS systems to make them less vulnerable.

However, in discussing fraud, the many small differences that exist between different examples make any attempt at a complete discussion of fraud problematic. In addition to this, there is no agreed definition of what is meant by fraud. To move this discussion forward, both of these issues will be addressed, and a definition and classification of frauds will be proposed.

The final part of this document will address some of the legal issues associated with fraud prosecution, the presentation of electronic data as evidence in UK courts, and the impact roaming will make.

Definition of fraud

What is fraud? On a simple level, it can be described as any activity by which service is obtained without intention of paying. Organisations sometimes calculate how much money they lose through fraud by defining it as the money that is lost on accounts where no payment in received. However, for detection purposes, such a definition is of little use, as using this definition fraud can only be detected once it has occurred. In fact, specifying what is fraud may be impossible, as the differences between fraudulent and non-fraudulent behaviour may be indefinably small. However, what can be used for specifying fraud are examples of fraudulent behaviour. When asking the question again, "what is fraud?", it is these examples that provide the answer.

Classification

As fraud can exist across the full range of mobile telecommunications business, discussing every example of fraud is inefficient, so this paper will simply define four fraud groups to clarify the discussion. The four groups are here defined as:

1) **Contractual Fraud** - all frauds in this category generate revenue through the normal use of a service whilst having no intention of paying for use. Examples of such fraud are Subscription fraud and Premium Rate fraud.
   Subscription fraud can take many guises, but can be divided into two classes, one where people enter the contract with no desire to pay for service, and the other where people decide part way through a contract that they will no longer pay for service. The latter case usually results in a dramatic change in usage behaviour. However, the former case has no usage history to compare the initial heavy usage against. In this case additional subscriber information is required to try and assess the risk associated with the subscriber.
   Premium Rate Fraud involves two actions - the setting up of a Premium Rate Service, and the acquiring of a number of phones to call this number. The actual mechanism used for perpetrating the fraud will depend upon the payment scheme used for the Premium Rate Service. If the Premium Rate Service receives a share of the revenue generated for the Network, then the phones will make long duration calls to the Premium Rate number. If the Premium Rate Service receives money from the network according to the number of calls received by the Service, then the phones will make a high number of short duration calls. The phones that have been calling this number will then not have their bills paid. The signature of such fraud is therefore dependent on the payment scheme used for the Service, but will be a number of high risk phones either making repeated long duration calls or many short duration calls to certain Premium Rate numbers.

2) **Hacking fraud** - all frauds in this category generate revenue for the fraudster by breaking into insecure systems, and exploiting or selling on any available functionality. Examples of such fraud are PABX fraud and Network attack.
   In PABX fraud, a fraudster repeatedly calls a PABX, trying to get access to an outside line. Once the fraudster has access to this, they can then dial out, making high value calls, whilst only paying for the low value PABX access call. Often, such attacks are associated with the use of cloned phones, so that even these low cost legs are not paid for.
   In Network attacks, computer networks are attacked through the access modems that are used for remote management or support. Once a modem is hit, the fraudster then tries to break into the network and configure certain machines for his own end. Such frauds are characterised by rapid short calls to the same number in the case of PABX fraud, or short calls to sequential numbers in the case of Network fraud, and it is this behaviour that has to be detected.

3) **Technical fraud** - all frauds in this category involve attacks against weaknesses in the technology of the mobile system. Such frauds typically need some initial technical knowledge and ability, although once a weakness has been discovered this information is often quickly distributed in a form that non-technical people can use. Examples of such fraud are Cloning, Technical Internal fraud.
   In cloning fraud, the phone's authentication parameters are copied onto another handset, so that the network believes that it is the original handset that is being authenticated.
   In Technical Internal Fraud, fraudulent employees may alter certain internal information to allow certain users reduced cost access to services. The usage behaviour in these frauds depends on how long the fraud is expected to remain undetected. In the situation where the Fraudster believes that the fraud can be hidden for a long time, then the best approach would be to exhibit normal usage behaviour, as no attention is then drawn to it. However, if the fraud has a short lifetime, then the best approach is to make as much use of the service as possible until it is stopped.

4) **Procedural fraud** - all frauds in this category involve attacks against the procedures implemented to minimise exposure to fraud, and often attack the weaknesses in the business procedures used to grant access to the system. Examples of such fraud are Roaming fraud, Voucher ID duplication, and Faulty vouchers.

   In the case of Roaming fraud, the billing procedure may mean that the Subscriber is billed a long time after the calls were made, in which case the subscriber may no longer be billable. Another aspect of this may be that the subscriber has been identified as a fraudulent roamer, but an error in the procedure of terminating his subscription means that he is able to continue making calls whilst roaming.

   In the case of Voucher fraud, there may be problems associated with the procedures used to produce, distribute, activate and de-activate the PAYT vouchers. If the voucher information can be distributed to a number of people who attempt to activate the voucher at the same time, then if the procedure provides a time window between the phone account being credited and the voucher being de-activated, this may allow a number of people to use the same voucher. Such frauds usually display normal behaviour, and can only be countered by tightening up the procedures involved.

Detection

There are many different approaches and combinations of approaches that are available for the detection of fraud. To simplify this discussion, three general approaches will be discussed here: learnt, taught, and investigative.

1) The **learnt** approach is typified by the use of unsupervised neural networks, where the fraud detection tool itself learns what is the expected behaviour for each user. The learnt approach is useful for detecting *changes* in behaviour, and hence is most efficient at detecting Subscription and Hacking fraud.
2) The **taught** approach is typified by the use of supervised neural networks or rule-based fraud tools. Such tools are taught what fraudulent behaviour looks like, and then try to discover behaviours that are in some way similar to these frauds. The taught approach is useful for detecting signatures of fraud, and hence is useful in detecting Subscription and Hacking fraud. In addition, once a technical fraud is discovered, these can sometimes be detected using the taught approach.
3) The **investigative** approach looks for weaknesses in procedures and technical specifications. Clearly such an approach is useful in countering technical and procedural fraud.

Learnt

In the learnt approach, a tool will learn what is typical behaviour, and raise an alarm on any large variations from this behaviour. In addition, the tool will generally evolve this typical behaviour over time as the Users behaviour changes. The tool's ability to monitor the behaviour of the User makes it very useful for detecting frauds about which nothing is known, as in nearly all cases of hacking or contractual fraud, these will result in changes of behaviour. If little is known about the fraud that exists in a system, this is a good tool to begin obtaining examples of fraudulent behaviour.

However, there are a number of drawbacks with such an approach. It is not possible to teach such a tool what to look for, and if the evolution parameters are not set correctly, clever fraudsters will learn how to 'ramp up' usage so as not to trigger an alarm.

An example of such a tool is the Unsupervised Neural Network. Here, the inputs to the tool are measured to determine a set of parameters that describe the behaviour of the User. The tool will typically maintain a measure of recent behaviour and longer term behaviour, and is then able to assess the current behaviour against both recent and long term behaviour profiles. These profiles will evolve in time according to some evolution parameters that will either be dependent on time or the number of calls.

Taught

In the taught approach, examples of fraud have been obtained. These are then used to 'teach' the tool what it is looking for. In the case of a Rule Based System, the fraud examples are analysed for their fraud signatures,

and these are then translated into rules using thresholds or relative measures. In the case of a Supervised Neural Network, examples of fraud are used along with examples of non-fraudulent behaviour to teach the tool which behaviours are good and which are fraudulent. Both approaches should identify behaviours in some sense similar to the fraud examples used as fraudulent, and behaviours in some sense similar to good behaviour should be deemed non-fraudulent.

There are some differences between the Rule Based and Supervised Neural Network approach that should be noted. In the case of the Rule Based system, work has to be done at the beginning of the fraud process to identify the signatures and thereby the rules required to detect fraud. However, having done this work, the meaning of and reason for any alarm is immediately apparent. For example, if calls of duration greater than 1,000 hours is a good indicator of fraud, then an alarm raised by a Rule Based system will say that this alarm was raised because the call duration was greater than 1,000 hours.

In the case of the Supervised Neural Network, far less work has to be done at the beginning of the fraud process, as the tool simply needs to be taught against good and bad behaviour. However, any alarm that is raised will simply inform you that the Users behaviour is some measure of distance away from a fraudulent example. The analysis then has to be performed at the end of the process, by doing some further exploration of the behaviour. Although some Supervised Neural Network tools simplify this process, it is still more labour intensive than a Rule Based approach.

However, both of these approaches have the drawback that new types of fraud are not being looked for, and may therefore remain undetected by the 'taught' tool whilst it may be detected by the 'learnt' tool.

Investigative

The investigative approach is, as it suggests, a matter of auditing the procedures and technology that is employed. This can be performed either internally or by using an external company. Such an approach is extremely useful, and will become more important as exploiting procedural and technical frauds become more attractive.

One example of its usefulness is in ensuring that an employee cannot modify a database on your network so as to grant credit or free usage to certain subscribers. Another is that the machines on your network can not be accessed remotely in an unauthorised way. As cloning becomes more expensive, such approaches to obtaining fraudulent access to services will become more attractive.

Prosecution

Once a fraudster has been detected, and if it makes good business sense, the next step is to prosecute the fraudster. The principal piece of legislation used in the UK to prosecute cellular fraud is the Telecommunications Act 1984 (the 1984 Act), as amended by the Telecommunications (Fraud) Act 1997 (the 1997 Act). Section 42 of the 1984 Act covers fraudulent use of a telecommunications system. It creates the specific offence of dishonestly obtaining a telecommunications service. The 1997 Act amends the 1984 Act by incorporating a new section (Sct. 42A) into the 1984 Act. Section 42A states that a person shall be guilty of an offence if he has in his custody or under his control “anything which may be used for the purpose of obtaining a telecommunications service” if he intends to use the thing to obtain such a service dishonestly or dishonestly allows the thing to be used to obtain a telecommunications service or for a purpose connected with the dishonest dealing of such a service. Section 42A has clearly been broadly drafted. The use of the term “anything” ensures that the legislation will not become redundant due to technological advances. In addition, the 1997 Act makes a person guilty of an offence where he supplies or offers to supply something to another, and he knows or believes that that person intends to use it dishonestly to obtain a telecommunications service or dishonestly to allow it to be used to obtain such a service or for a purpose connected with the dishonest obtaining of such a service. Fraudsters may be convicted summarily or on indictment under Section 42A. The former carries a maximum term of imprisonment of six months while the latter carries a maximum term of five years. In both cases, a fine may be imposed instead of, or, in addition to, a term of imprisonment. The 1997 Act is an example of fraud legislation which is sector specific. It applies to telecommunications services in

general and therefore may be invoked against cellular fraudsters by both law enforcement authorities and private entities such as network operators and service providers.

Presenting the evidence in court

In the UK, electronic data e.g. call data is admissible as evidence in criminal proceedings under the provisions of the Police and Criminal Evidence Act 1984 and the Criminal Justice Act 1988.

1) The Police and Criminal Evidence Act 1984 (PACE)
   Section 69 (1) of PACE provides that computer-generated documents may be admissible as evidence where there was no improper use of the computer and it was operating properly at all material times. Even if the computer was not operating properly, this will not affect the admissibility of documents produced by it provided the malfunctioning did not affect the production of the document or the accuracy of its contents. Section 69 imposes a burden of proof on the party seeking to submit computer-generated documents in court. This burden is relatively easily discharged by the party providing the court with a certificate signed by the person occupying a responsible position in relation to the operation of the computer. The certificate identifies the document containing the statement and describes the manner in which it was produced. It also gives particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer.
   Lastly, it deals with any of the matters mentioned in section 69 (1) e.g. confirming that there was no improper use of the computer or that the computer was operating properly at all material times.
2) The Criminal Justice Act 1988 (CJA)
   Section 24 (1) of the CJA is subject to Section 69 of PACE and provides that a statement in a document shall be admissible in criminal proceedings if the document was created or received by a person in the course of a trade, business, profession or other occupation and the information contained in the document was supplied by a person (whether or not the maker of the statement) who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with. The term "document" is given a very broad meaning so as to include film, tape recordings and computer disks by virtue of Section 10 of the Civil Evidence Act 1968 (incorporated into the CJA by Schedule 2, paragraph 5).

Roaming

Roaming is the use of one's mobile phone abroad. Roaming fraud raises difficult questions for lawyers. This is linked to the fact that criminal law, generally speaking, is territorial in nature i.e. a national court can only assume jurisdiction if the criminal act has taken place *on* national territory. This poses a problem since often the fraudster has made calls abroad and has *remained* abroad without paying his bill. If the fraudulent act is taken to be the calls made abroad (without any intention of paying for them), the courts in the state where the original subscription was taken out will not have jurisdiction to try the case since the criminal acts were not carried out on national territory. This is problematic for the home mobile operator (suffering financial losses) since it cannot be sure that a court in its country will get jurisdiction of the case because of the territoriality principle. If any court does assume jurisdiction in this case, it will be a foreign court applying law unfamiliar to the home operator.

Another important field of law is relevant where roaming or trans-national fraud is at issue. This is the field of private international law. This law relates essentially to the area of conflicts of laws. It is used to determine which court has jurisdiction when two or more courts from different countries claim jurisdiction of the same case. Two important European conventions govern this complex field of law. These are the Brussels convention of 1968 and the Lugano convention of 1988. The legal scope of these conventions is limited to civil and commercial matters, thereby making them relevant when an operator wishes to sue under the terms of its contract with the (fraudulent) subscriber.

The Brussels Convention is relevant for EU Member States. Title II of the Convention contains the jurisdiction rules. The principal rule is that a defendant who is domiciled in a contracting state (to the Brussels Convention) may normally be sued in the courts of that state. This rule is important in the case of roaming fraud since the fraudster may *become* domiciled in the roamed state thereby allowing courts in that state to take jurisdiction of the case.

It is important to note however that there is a special jurisdiction rule contained in article 5 of the Brussels Convention. Article 5 (1) concerns matters relating to a contract. It provides that in matters relating to a contract a person who is domiciled in a contracting state may be sued in another contracting state if that is the place of performance of the obligation in question. Sometimes the place of performance is specified clearly in the subscription contract. If so, the courts of that country will have jurisdiction. If England is deemed the place of performance of the obligation, then an English court will assume jurisdiction of the case no matter where the defendant (fraudster) is currently living. This is advantageous for the English operator since a "local" court that applies laws with which the operator is familiar assumes jurisdiction.

Conclusion

This paper presents a grouping of fraud. It is proposed that all frauds can be meaningfully grouped into Contractual, Hacking, Technical or Procedural fraud. It is hoped that this approach simplifies their discussion.
In addition, the three different approaches that are used in fraud detection, namely tools that learn, tools that are taught, and investigations are discussed. The strengths and weaknesses of each approach are also discussed.
The detection of the four different groupings of fraud each requires a different approach. The tools useful for each approach have their own strength and weaknesses, and it is only by evaluating and prioritising the fraud in each given situation that the appropriate solution can be defined.
For prosecution purposes, the UK has strong legislation that can be used to counteract telecommunications fraud. Sector-specific legislation, an example of which is the 1997 Act in the UK, should be enacted in the other Member States of the EU. This would make prosecuting cellular fraud in the EU more straightforward, and do away with the use of general (non-sector specific) legislation for prosecution services. The issue of roaming fraud remains problematic though since criminal law is territorial in nature, no harmonised set of localisation rules has been formulated at EU level and the field of private international law is a particularly complex and difficult law to apply.