

THE CHANGING FACE OF FRAUD: PHONE FRAUD

Gillian Dempsey, LLB(Hons) PhD
Department of Commerce
The Australian National University

*Paper presented at the 3rd National Outlook Symposium on Crime in Australia,
Mapping the Boundaries of Australia's Criminal Justice System
convened by the Australian Institute of Criminology
and held in Canberra 22-23 March 1999*

1. Overview: the nature of fraud

Fraud is a dynamic crime that is scarcely mentioned by that name. In statute it exists as concepts such as “misappropriation”, “false pretenses” and “obtaining goods by deceit”. The common denominator among these crimes is obtaining land, goods, services or cash by guile. The incidence of fraud is becoming increasingly difficult to approximate, let alone to quantify. This can be attributed to the changing nature of the economy and the fresh opportunities such change provides for fraud.

When limited to transactions involving physical goods or cash, fraud was “overt” in that, at the very least in hindsight, it could be seen to have occurred. Increasingly information and services are becoming larger components of the economy. Such economic evolution encourages the creation and adoption of new communication technology. New varieties of communication and transaction unfortunately spawn fresh opportunity for fraud. This is particularly so for digital media which has the advantage of being relatively anonymous yet simultaneously capable of wide reception.

1.1 Digital age versus manufacturing age distinction.

Mention of fraud typically conjures images of pyramid schemes, or scams such as executed by Steve Martin in “Dirty Rotten Scoundrels”. Technologically updated versions of “traditional” frauds are now being run. The infamous Nigerian banking scam went digital last year. E-mails were sent to hundreds of people requesting access to their bank accounts and promising significant financial rewards in return. The bank accounts of those who complied were emptied. Fraud of this type represents traditional patterns of deception using new forms of communication, rather than digital age fraud proper. Digital age frauds exhibit several novel characteristics as compared to more traditional fraud:

- high level of technological sophistication;
- relatively rapid time frame for execution;
- potential for large scale effect;
- often no direct contact with the victim; and
- little fault on part of victims;

The level of technological sophistication involved in such fraud presents several challenges to law enforcement agencies. Most of these challenges devolve to budgetary issues. Firstly a high level of training and practical experience is required to investigate sophisticated crime. Once individuals have such training, however, they become very attractive to private industry and are often headhunted for very large salaries. Law enforcement is also challenged by the methods by which they may legally obtain electronic evidence. In digital fraud investigations, time is often going to be of the essence, yet procedures under several acts put in place a vast paper trail to be meticulously observed. The benefit to the public of checks is to ensure that privacy as a rule is respected and that listening devices and the interception of telecommunications does not become mainstream. Competing considerations such as this present a particularly difficult hurdle to legislative change.

Digital fraud also has potential to reach more victims than conventional means of fraud. This is partly linked to the final two points. In contrast to traditional fraud schemes to which require some gullibility, greed or culpability on the part of the victims, victims of digital age fraud are less likely to have made contact with the fraudulent individual let alone been actively deceived. This presents problems in terms of prevention and enforcement. Because the victim might never have any personal contact with the perpetrator education is a vastly less potent weapon. For example, in relation to credit card cloning it can only raise consumer awareness and it is unlikely to alter behaviour significantly. In relation to enforcement, the main problems relate to resources both financial and of human expertise. The challenge, therefore, rests largely with technological means of prevention and enforcement. This is inevitable given that every instance of digital fraud involves a computer somewhere recording a transaction, be it a credit card transaction, e-cash or a mobile phone call.

Another cause for significant concern in relation to scale is to what use the proceeds are being put. Digital fraud is likely to be a means to an end rather than an end in itself. For example, the links between drugs, money laundering and credit-card fraud are well established. In the United States, digital phone fraud was found to be being perpetrated by a group from the middle east who were using it to fund arms deals.

The response to problems such as lack of law enforcement budget and the nature of such fraud is to rely on technology to make the system (be it telephone, credit card or other) more secure. Although it would be true to say that it is possible to make systems much more secure, there are many competing considerations. These can roughly be grouped into considerations relating to the system's efficiency and effectiveness. Efficiency considerations relate to matters such as the speed at which a system will run in the presence of security measures that provide the ability to trace transactions via an audit trail. Effectiveness considerations relate to more intangible but equally important matters such as the right to privacy and ease of use. These desirable criteria often clash. For example, a system that has significant levels of monitoring may have undesirable privacy implications for users. The challenge for regulators in relation to fraud policing and prevention is to ensure high levels of protection against fraud while not compromising the benefits of technology, including accessibility, openness and ease of use.

2. The changing nature of fraud: the example of digital phone fraud

Digital phone fraud is an important issue for digital crime (analogue mobile phones will be phased out by the year 2001). Digital phone fraud has the potential to be a most prevalent form of fraud, and yet remain difficult to adequately investigate. This paper concentrates on the technological aspects of digital phone fraud rather than physical theft, for example, of a handset, although the encryption considerations are similar.

2.1 SIM cloning

The GSM¹ relies on special cryptographic codes to authenticate customers and bill them appropriately. This is done via small smartcard called a SIM (or Subscriber Identification Module) registered with the network operator (e.g. Telstra) which stores a secret key (a

¹ <http://www.gsmworld.org>

unique identifier) which can be used to authenticate the customer and enable calls to be billed to that number. As each handset also has a unique identifier it is possible to key the SIM to the handset such that they will not operate in another phone. This is not currently done. When making a phone call, the SIM “proves” the knowledge of the secret key to the service provider. The main security problem, however, is that knowledge of the key and how to program it into a blank SIM is sufficient to create a cloned phone that can then make calls billed to the owner of the real phone. The numbers for SIMs are generated in a special way and contain check digits so that cloning is not simply a matter of entering a random number onto a blank SIM.

Interacting repeatedly with the SIM using known cracking techniques available on the World Wide Web can reveal the SIM’s key. Once the key is compromised, it is possible to make fraudulent calls, which will be billed, to the victim. Cracking one SIM does not break the algorithm for the entire system per se, but once the information as to the construction parameters of that algorithm are released, it makes further cracking less difficult. The interrogation can also involve interception of the transmissions between the network and a SIM.

2.2 What are the cloned phones being used for?

Unlike most manufacturing age frauds where obtaining the goods or services by deceit was an end in itself, cloned phones (like cloned credit cards) are often used to mask other activity. Cloning a phone can be the virtual equivalent of driving a stolen getaway car in a bank robbery in terms of the anonymity offered. Illicit uses of cloned mobile phones have extended from hacking to terrorism. A clever cloner will not use the same configuration all the time. Shifting through various cloned SIM numbers may leave the actual owner of the phone wondering whether they placed a call or thinking that their phone company’s billing system had hiccupped again.

3. Balancing considerations: security versus accessibility

Security

Difficult political constraints face regulators in relation to setting adequate standards in relation to digital fraud. Digital fraud is a phenomenon as global as the telecommunications and computer systems on which it preys. Many of the problems associated with SIM card and mobile phone security are intimately related to the international debate concerning encryption standards:

One of the most attractive features of GSM is that it is a very secure network. All communications, both speech and data, are encrypted to prevent eavesdropping. In fact, in the early stages of its development it was found that the encryption algorithm was too powerful for certain technology export regulators. This could have had serious implications for the global spread of GSM by limiting the number of countries to which it could be sold. Fortunately, the MoU[memorandum of

understanding] reacted promptly to this threat. Alternative algorithms were developed that enabled the free dissemination of the technology worldwide.²

This means that the protection afforded to mobile phones worldwide was *deliberately decreased* as a result of intervention of the US government – particularly in response to the opposition of the FBI and the National Security Agency to strong encryption. The opposition derived from the problem that the FBI and NSA were concerned about being able to conduct successful "wiretaps" on cellular phone conversations. As a result of these concerns, the algorithm that protects GSM communications is markedly less strong than it might have been. The encryption cracked in so little time by the University of California ISAAC group was the "alternative algorithm". GSM have recognised, however, that the standards should be improved – they established a Security Accreditation Scheme in July 1998, to establish uniform security standards. This involves voluntary participation in "external audit" of security standards.³ They also run a Fraud Forum, which has an Asia-Pacific sub-group operating out of Singapore. The Forum conducts research into the "legal implications of fraud management", and seeks "to clarify all the legal, regulatory and data protection issues relevant to managing fraud".⁴ The difficulty that confronts the Forum is the constant change in the technology and the increasing sophistication of both users and criminals.

Australian standards for mobile phones are identical to the agreed-upon Global System Mobile (GSM) standards other than in relation to emergency dialing and acceptable radiation output levels.⁵ These standards will soon be replaced by the Universal Mobile Telecommunication System (UMTS), or third generation protocols which are supposed to be in place by the end of this year. The transition was foreseen as "a smooth and continuous process, rather than the introduction of a completely new system that would rapidly take over from GSM".⁶ It currently appears that GSM are attempting to redress the problem of encryption via the proposed third generation protocols:

Security for third generation systems must be greater in scope and more sophisticated than for existing systems, in which the majority of security features are aimed solely at counteracting threats to the air interface.⁷

Again, the problem as perceived by industry professionals is that the algorithm used to encrypt will not reflect the state of the art (elliptic curve encryption rather than RSA) due to the US's import restrictions in that area. Secrecy in the development of standards results in poorer testing and in weaker security. The result is a deliberate technological lag. Ironically, this lag enables fraud perpetrators to gain simple advantage over intelligence agencies' wiretaps by using cloned phones, yet legitimate users remain at risk of being defrauded.

Accessibility

Global political considerations will prevent the best technological defences from being adopted as a standard for digital phones. The implication of this is that other methods must be devised

² <http://www.gsmworld.com/history/page15.htm>

³ <http://www.gsmworld.org/news/comm3.htm>

⁴ <http://www.gsmworld.org/assoc/page26.htm>

⁵ <http://www.austel.gov.au/standards/brief.htm>

⁶ <http://www.etsi.org/brochures/stateart/dupuis.htm>

⁷ UMTS Security Objectives, Sect. 1

to mitigate the incidence of fraud. One simple principle is that fraud prevention and detection mechanisms should not preclude or bias classes of users from adopting the technology.

The two main elements of accessibility relate to ease of use and privacy. In relation to ease of use, pin numbers, passwords and similar restrictions are almost certainly more often abused than used correctly. Pin numbers are typically based on birthdays, anniversaries or easy to recall number sequences (such as 2468). Passwords are often the names of relatives or pets. A typical reason for such laxity is that people have neither the time nor the inclination to remember a series of 'useless' numbers and require something to prompt their memory. In relation to ease of use, such identification devices can be alienating. SIMs do, however, have the potential to contain biometric data which could be used to provide an extra level of security. The difficulty with adoption here is not so much technical as historical and cultural. Biometric data is very sensitive data indeed and many people are genuinely disturbed by the thought of its use and potential abuse.

To date, the most widely used method to detect digital phone fraud is traffic analysis. Notable variances in calling patterns may indicate fraud. The time and location of the previous call may also indicate by physical impossibility the presence of a clone. At best, however, this would provide evidence for the individual being wrongly billed. To act on the suspicions raised in this data can be prejudicial if not handled correctly – people do change their call patterns and an investigation based solely on traffic may cause invasion of their privacy to their detriment.

5. Conclusions

Digital fraud presents yet another increasing layer of complexity for law enforcement agencies. Education is slightly less effective in relation to digital fraud, on the grounds that the victim does not need to be the weak link in the chain. Technological measures do not represent a panacea, in that they are heavily constrained by global political considerations such as the US's ban on encryption export. In this context, competing considerations of security and accessibility provide a considerable challenge for policy-makers into the next century.