"The Prevention of On-Line Financial Fraud"

Dr Russell G. Smith

Research Analyst

Australian Institute of Criminology

INTRODUCTION

This paper examines the risks associated with conducting commercial transactions through the use of electronic technologies and how best to prevent funds from being illegally misappropriated in the world of electronic commerce. It will not, however, deal with the many other problems which arise out of on-line commerce such as those relating to misleading and deceptive practices which create particular concerns for consumer protection agencies. Instead, it focuses on the ways of preventing illegality which arises out of the use of electronic payment systems.

The extent to which individuals are using the Internet for business transactions is increasing enormously. The market is potentially great with approximately 171.25 million people estimated to be using the Internet worldwide in May 1999 (NUA Internet Surveys 1999a). In terms of commercial usage, Forrester Research has estimated that global business-to-business on-line commerce could amount to US$327 billion by the year 2002. Although the rate of increase in on-line commerce has slowed somewhat recently, it will still represent an important part of economic life in the years to come.

Surveys of Internet usage have shown that most transactions which take place on-line involve small-value purchases such as books, CDs, wine, computers, and information technology products. The potential exists, however, for anything to be purchased electronically and we have recently seen the establishment of a number of on-line auction houses which deal in much higher-value goods (e.g. ‘eBay’ http://pages.ebay.com/index.html). A large proportion of Internet users also arrange travel and holidays electronically. Jupiter Communications (1999) has, for example, estimated that the on-line travel market will be worth US$16.6 billion by 2003.

The Internet is, arguably, at the moment an expansive advertising medium in which information as well as goods and services are made available to users throughout the world. Most business transactions take place by purchasers identifying goods and services which they require by inspecting Internet sites. They are then able to pay for the product chosen using conventional forms of payment, such as money orders or cheques which may be sent by post to the merchant before the product is despatched or the service provided.

Alternatively, purchasers may pay for a product or service by transferring funds electronically. This can be done by disclosing one’s bank account (usually a credit card account) details and authorising the merchant to debit the specified account to the value of the sum in question. In this way one could, for example, sitting in Malta, purchase a book from an antiquarian bookshop in London, or subscribe to an adult Internet site emanating from Sydney.

More recent payment systems have been developed which make use of telephone accounts to permit merchants to obtain access to a user’s funds, as well as forms of electronic cash in which value is held electronically on the computer’s hard drive and debited or credited as and when the need arises. New forms of stored value cards which have been designed to record monetary value, may also be used to

transfer funds from a bank's Automated Teller Machine to a personal computer, and thence to a merchant. These systems are obviously more efficient as transactions may be carried out and paid for instantaneously permitting such activities as on-line gambling to take place.

Each of these payment systems, however, creates security vulnerabilities and already we have seen instances of fraud being perpetrated on the Internet and funds being stolen electronically. A survey conducted by the National Consumers League estimated that over six million Internet users in the United States had been the victims of credit card fraud, representing seven per cent of on-line consumers in the United States (NUA Internet Surveys 1999b).

It needs to be understood, however, that the concept of transferring funds electronically is, conceptually, inaccurate. Bags of money do not travel in dematerialised form along telephone wires (see Mackenzie 1998: 22). What takes place is that a series of instructions are given to financial institutions to debit and credit accounts of customers and merchants. Systems are then put in place to ensure that these instructions are not altered without the authority of the senders and that other instructions are unable to be substituted unlawfully. Fraud prevention simply requires that the instructions given by customers, merchants, and financial institutions are unable to be tampered with.

INTERNET PAYMENT SYSTEMS AND THEIR VULNERABILITIES

The security risks associated with conducting on-line transactions may best be described by considering separately each of the three payment systems which are available: paper-based payment systems; direct debit electronic funds transfer systems; and systems which make use of electronic cash. Although some of these systems have yet to commence wide-scale operation, security flaws have already been identified by which offenders are able to steal funds electronically.

Paper-Based Payment Systems

Where goods and services are obtained through the Internet and paid for using paper-based instruments, such as postal orders or cheques, fraud may be perpetrated in the same ways as those which have operated in the past where these payment systems have been employed.

The vulnerabilities principally relate to individuals using accounts which have been opened through the use of false identification details, exceeding the credit balance held in cheque accounts, or counterfeiting or altering instruments themselves. Because there is pressure for transactions to be carried out quickly on the Internet, merchants may be less willing to wait for cheques to be cleared or for authentication checks to be carried out prior to authorising the dispatch of goods or the provision of services, thus leaving them open to fraud. Similarly, consumers may send off a cheque to a merchant they have no independent information about who may be located in a foreign country, receive payment, and default on the agreement.

Direct Debit Electronic Funds Transfer Systems

In addition to paper-based transactions, on-line payments could be made by way of direct debit, in which

value is transferred directly from the payer's account to the recipient's bank, or by way of credit transfer in which a payer advises his or her bank to debit his or her account with a sum which is electronically credited to another account. These are essentially 'card not present' transactions which operate the same way as any telephone or mail order transaction based on a credit card account.

In order for such transfers to take place, preliminary steps need to be taken by the parties involved which include the exchange of account details and the conduct of various identification checks. From the purchaser's point of view, an element of risk arises if funds are transferred before the goods arrive or the service is provided. From the merchant's point of view, it is necessary for funds to arrive before the goods are despatched or the service provided. Both purchasers and merchants may also incur bank and government fees in respect of such transactions which are higher in the case of Internet transactions where the risks are greater.

The principal safeguard against such fraud involves merchants taking adequate steps to authenticate the card details, the cardholder, and to ensure that adequate funds are held in the account to cover the purchase. Obtaining authorisation from the card issuer is the first step in fraud prevention and some banks are now offering real-time authorisation for transactions above the specified floor limits. Merchants should also require customers to sign receipts for any goods delivered, although this is impractical with some on-line transactions such as the purchase of software which can be downloaded immediately.

Home Banking

The Internet is also being used for Home Banking in which various transactions may be carried out from a personal computer in the customer's home which is connected to the bank via telephone wires and a modem. Home banking services include obtaining general information such as locations of branches and ATMs, interest and exchange rates; conducting various transaction services such as obtaining account balances and details of past transactions, transferring funds between accounts, using electronic chequebooks to pay bills; and other services including ordering statements, and chequebooks, reporting lost or stolen cards, notifying changes of address, stopping payment of cheques, obtaining loans, investment information or share dealing brokerage, and seeking share portfolio management services.

In each of these systems protection against fraud is obtained through the use of PIN authentication, transaction codes, and encryption of data in much the same way as an ATM system operates. The possibility exists, however, that passwords, PINs and cryptographic keys could be compromised. To limit the financial consequences of this, banks issue a PIN for home banking which is different from the customer's ordinary ATM PIN.

Both telephone and computer home banking are now being offered in a number of countries and already police have been called upon to investigate allegations of fraud. One case in Australia, for example, involved two individuals who claimed that they could illegally obtain access into Advance Bank's Internet banking system. The two individuals concerned offered to solve flaws which allegedly existed in the bank's security system in return for a payment of A$2 million, thus amounting to a form of extortion. No prosecution occurred, however (Da Silva 1996).

Secure EFT Systems

Various systems are being developed to enable customers, banks, and merchants to communicate securely with each other. A number of electronic funds transfer systems already operate throughout the world as substitutes for paper-based cheque transactions and these could well be adapted for Internet use. The United Kingdom GIRO system, for example, has benefits in preventing cheque fraud because the payment order is directed to the banker directly rather than through the payee. In the GIRO system, the person wishing to make a payment, the payer, instructs his or her bank concerning the details of the payment and the funds are electronically transferred from the payer's account to the payee's account.

These systems create a security risk if procedures are not in place to verify the availability of funds which are to be transferred or if account access controls are not in place. There is also the possibility of information being manipulated as it passes over the network in unencrypted form.

In order to secure electronic funds transfers, data are generally encrypted using algorithms which encode messages. These are then decoded using electronic keys known to the sender and the recipient. The major security risk associated with such a system lies in the possibility of the encryption keys being ascertained, in which case data within the system could be revealed or manipulated. Most of the large scale electronic funds transfer frauds which have been committed in the past have involved the interception or alteration of electronic data messages transmitted from the computers of financial institutions (see Meijboom 1988). In many cases offenders have worked within financial institutions themselves and been privy to the operation of the security systems in question (see, for example, the cases of *Stanley Mark Rifkin* (Rawitch 1979 and Sullivan 1987); *R v Thompson* [1984] 1 WLR 962; *Director of Public Prosecutions v Murdoch* [1993] 1 VR 406 and the 1994 *Citibank case* (R. v *Governor of Brixton Prison; Ex parte Levin* [1996] 3 WLR 657; Holland 1995; and Kennedy 1996)).

In order to enhance the security of credit card transactions on the Internet, various companies have designed systems to ensure that the identity of the contracting parties is able to be authenticated and that merchants are able to ascertain if the customer has adequate funds with which to conduct the transaction. Microsoft and Visa, for example, are developing a payment protocol called 'SET' (Secure Electronic Transactions) which uses public key encryption to protect data from being compromised. Digital signatures are also used to authenticate each of the parties involved. Credit card details are encrypted prior to transmission with the decryption keys being separately protected. Merchants receive payment by passing to their bank an encrypted message which originates with the card holder permitting funds to be transferred from the credit card account to the merchant's account (Visa International 1997).

The main security risks associated with these systems relate to the possibility that private encryption keys could be stolen or used without authorisation by people who have obtained them illegitimately. The easiest way to do this would be to submit false identification evidence to Certification Authorities when obtaining a public-private key pair. Alternatively, if a private key were held on a smartcard it might be possible to obtain access to the key simply by breaking the access control device on the card which could simply be a password. Thus it could be possible for someone to make use of another person's private key to order goods or services from the Internet and be unable to be traced.

Card-Based Systems

Clearly, it would greatly facilitate Internet commerce if a user were able to insert a plastic card into an EFTPOS Terminal attached to a personal computer and to conduct transactions directly between a merchant and a financial institution. This would, however, require that every personal computer be included in the computer network which links all financial institutions worldwide.

Even if this were financially possible, plastic card payment systems have their own vulnerabilities to fraud through counterfeiting, alteration and theft of cards (Smith 1997), not to mention the logistical and security problems associated with having every financial institution's secure network provided to every Internet user.

Others are considering the use of smart cards with the capacity to store value and transfer this to merchants via the Internet.

Smart card payments systems may take a variety of forms. The system which most closely resembles the early forms of stored value cards involves a scheme operator which administers a central pool of funds. When a card holder transfers value to the card, the funds are actually transferred to a pool controlled by the scheme operator. A merchant who is paid from the card takes evidence of the receipt to the scheme operator, which pays the relevant amount from the pool. Other proposals, such as those operated by MasterCard and Visa International, envisage a number of brands of cards being accepted. In such schemes there is no central pool of funds, but rather each card issuer is responsible for reimbursing merchants which accept their cards.

In the United Kingdom, the Mondex system developed by the National Westminster and Midland Banks does not involve scheme operators. Funds are loaded onto the card which can then be used without reference to any other person. Funds are transferred from one card to another as well as to merchants but because funds loaded onto the card do not exist anywhere other than on the card, there is no audit trail of transactions or reconciliation of payments. This means that forgery could occur without trace and the scheme could be used for money laundering, or dispersing the proceeds of criminal activities. The Mondex card can be recharged from a mobile telephone link and can be used in EFTPOS terminals. In the United States, a modified version of the Mondex system is being trialed which will enable banks to trace card use. It will also be possible for money held on cards to be downloaded into computers, thus enabling Internet purchases to be paid for electronically from the card (Hansell 1996).

The main security risk associated with smart cards lies in the way in which data are encrypted. Levy (1994), for example, describes the potential for fraud using Mondex smart cards in England as being related to the card's code encryption system. The encryption used on smartcards is able to be broken if certain types of errors can be created on the card, such as through the use of ionising or microwave radiation. Bellcore, a United States computer and communications security company, and others have identified a number of design flaws in computer chip cards which may permit data to be leaked or information contained in the card to be tampered with (Bellcore 1996; Spinks 1996; Denning 1999).

Electronic Cash

Various systems are also being developed which will permit transactions to be carried out securely on the Internet through the use of electronic cash, or value tokens which are recorded digitally on computers.

The Digicash system, for example, which is based in the Netherlands

(http://digicash.com:80/home.html), uses a form of electronic money known as ‘E-cash’. Before purchases can be made, both the merchant and the customer need to establish banking arrangements and Internet links with the bank issuing the E-cash. The customer first requests a transfer of funds from his or her bank account into the E-cash system. This is similar to withdrawing cash from an ATM. The E-cash system then generates and validates E-cash coins which the customer is able to use on the Internet. The coins are data streams digitally signed by the issuing bank using its private key. The customer is then able to send E-cash to any merchant who will accept this form of payment using the software provided by the E-cash service provider. The customer encrypts the message and endorses the coins using the merchant’s public key. The merchant then decrypts the message with its private key and verifies the validity of the coin using the issuing bank’s public key. The merchant is then able to turn E-cash into real funds by presenting the E-cash to the issuing bank with a request for an equivalent amount of real funds to be credited to the merchant’s bank account.

An alternative approach is being used by an Australian company ‘Cybank’

(http://www.cybank.net/index.html). Cybank has patented a scheme in which value is created online through the use of telephone accounts. By selecting a cash amount on the Cybank Internet site, the software dials a pay service number and the sum requested is debited to the customer’s telephone account. The customer is then able to use the credit to purchase goods and services over the Internet (Bowes 1996; Carter 1996).

FRAUD PREVENTION ON THE INTERNET

Preventing on-line fraud will involve the use of both conventional as well as novel technological approaches. The essential elements of each are as follows.

Risk Awareness and User Education

One of the most effective strategies used to control crime is education of the public as to the nature of the security risks which they face, and how they may best protect themselves. As most on-line payment systems will require the use of a PIN or password in order for users to gain access to Personal Computers or plastic cards, protection of access codes will be the primary crime prevention strategy available. Users are best placed to protect themselves by taking basic security precautions to ensure that cards are not stolen. This includes not leaving them in public places and ensuring that they are reclaimed after use. Consumers are also advised not to compromise their security by disclosing access codes, keeping them with cards, or writing them on cards. Studies reveal, nonetheless, that between twenty and seventy per cent of people write their PIN on the card or on a piece of paper carried with the card (Sullivan 1987).

In the United Kingdom, one particularly effective plastic card fraud prevention strategy called ‘Cardwatch’ involved a high profile publicity and education campaign by the Association for Payment Clearing Service including posters, leaflets, and television and radio coverage to raise public awareness of the problem and to encourage card holders to take more care of their cards. It resulted in a forty-one per cent reduction in card fraud overall between 1991 and 1994, while losses occurring at retail points of sale were reduced by forty-nine per cent during the same period. Losses from cards lost or stolen in the post were reduced by sixty-two per cent between 1991 and 1994 (Webb 1996). Had these fraud

prevention initiatives not been introduced, it has been estimated that losses in Britain would have been 350 per cent higher than those recorded in 1996 (see Levi and Handley 1998).

When funds transfer systems become fully operational on the Internet, there will also be a need for users to be educated as to ways in which they may protect themselves from fraud and deception. The Internet, itself, may prove to be the most effective mechanism for transmitting such information.

Institutional Practices

Institutions involved in maintaining the infrastructure of the Internet as well as financial institutions are able to adopt a wide variety of self-help strategies which may reduce the risk of funds transfer fraud on the Internet.

First, and most importantly, is the need for organisations to be confident that the staff they are employing are reliable and trustworthy, as Internet fraud often involves confederates with inside knowledge of an institution's security and computer procedures. Personnel should also be regularly monitored in terms of their risk of behaving fraudulently, particularly long-term employees who have acquired considerable knowledge of an organisation's security procedures. Caution is also needed when organisational disputes develop.

A case heard before the New South Wales District Court on 27 March 1998, for example, concerned an unsuccessful applicant for a position with an Internet Service Provider (ISP). When he was refused the job he took revenge by illegally obtaining access to the company's database of credit card holders and publishing details relating to 1,225 cardholders on the Internet as a demonstration of the security weaknesses of the company. As a result, the business lost more than $A2 million and was forced to close its ISP activities (R. v *Stevens* unreported decision of the New South Wales District Court, 27 March 1998).

Financial institutions may be able to assist on-line merchants by notifying them of incidents of fraud as soon as they occur in order that they may be able to avoid repeat victimisation or that others may be able to avoid victimisation. In the United Kingdom, for example, a National Hot Card File was created by which details of lost and stolen cards were able to be quickly transmitted to retail outlets. A similar notification system could be established for on-line merchants.

Systems may also need to be created by which on-line merchants are able to obtain immediate authorisation from financial institutions before transactions are accepted. It may even be necessary for all on-line transactions to be authorised before they are accepted.

Frauds in which merchants are involved constitute a large problem for financial institutions as merchants or their employees are ideally placed to permit access to computer networks and to alter transaction details. Financial institutions may need to make use of artificial neural networks in order to isolate fraudulent claiming patterns by merchants and maintain databases of merchants who have engaged in illegal conduct on the Internet in the past. Already, organisations are providing certification services to enable users to identify illegal or unsafe Internet sites. One example is the United States Better Business Bureau which approves safe Web sites for Internet commerce (http://www.bbbonline.com).

Technological Solutions

A wide range of technological solutions have been devised in order to reduce the security risks associated with conducting on-line business.

Hardware Security

In order to provide a safe system for electronic commerce, computer hardware needs to be adequately secured. This extends from computer terminals used in homes, businesses, and public kiosks through servers operated by ISPs, to the hardware maintained by merchants and financial institutions. The extent of the security precautions used will be determined by the risks present. Terminals located in Internet kiosks may need only basic access controls such as through the use of passwords or smartcard tokens, whilst servers maintained by banks might need to be shielded against electro-magnetic radiation (EMR) scanning.

The threat of EMR scanning should not be taken lightly. Although the risk is remote, the possibility exists. In one case in England, for example, a computer eavesdropper scanned electronic transaction information transmitted by a bank. Despite the fact that the information was encrypted, the code was defeated and the individual successfully obtained £350,000 by blackmailing the bank and several customers by threatening to reveal certain information to the Inland Revenue (Nicholson 1989).

If payment systems are used which make use of digital signatures and encrypted data transmissions, then the need to protect computer cables from interception would not arise as any data would not travel in clear text. At present, however, a good deal of sensitive information travels across networks in unencrypted form making it vulnerable to interception and subsequent disclosure. The adequacy of encryption as a security measure depends, of course, upon the strength of the encryption system used and the determination of the attacker.

Card Security

Plastic cards may be used in conjunction with on-line transactions in a variety of ways. Primarily they will be used to store access devices such as cryptographic keys or other user authentication devices. They may also be used to store value in Mondex-type smart card systems.

The most sophisticated security features should be built into plastic cards in order to prevent counterfeiting, alteration or unauthorised access to the data which they hold. Newton (1995) describes various crime prevention strategies which have been used to prevent plastic card counterfeiting including the use of security printing, micro-printing, holograms, embossed characters, tamper-evident signature panels, magnetic stripes with improved card validation technologies, and indent printing. Smart cards, of course, are much more difficult to copy than ordinary magnetic stripe cards.

Unfortunately, all of these card security features have been overcome by organised criminals including computer chip circuitry in smart cards. On-line payment systems which do not rely upon plastic cards will, presumably, be much more secure and it may also be possible for these to operate in conjunction with biometric user identification systems.

Value Restrictions

As an alternative to target hardening, it has been suggested that the risk of large-scale fraud and money laundering using Internet-based funds transfer systems could be restricted by placing limits on the size of transactions.

Mackrell (1996), for example, has suggested that stored value cards should have a modest limit placed on the maximum value that can be stored on them, especially if they are to be used for card-to-card transfers. There could also be a limit on the life of the cards which would restrict their usefulness for hoarding and money laundering. Self-expiring cards have also been developed which automatically deteriorate after a certain period of time. In the case of on-line commerce, electronic restrictions could be placed on the value of transactions in order to avoid the possibility of large scale fraud, although this may be seen as an unwarranted intrusion into freedom of electronic commerce.

Password Protection

Passwords used as a means of restricting access to computer technologies are popular at present and frequently misused and abused. It is possible to guess passwords, particularly if little or no thought has been given to their selection, or to use various forms of social engineering to trick users into revealing their passwords for subsequent improper use.

The use of brute computing force has also been used to break passwords. Password cracking programs are available by which computers are able systematically to search entire dictionaries in search of a password. Even if passwords are encrypted so as to prevent them from direct exposure, encryption keys have been broken through the use of massive computing resources. Denning (1998: 40) reports, for example, that in 1994 a 129 digit RSA key was broken through combining the power of 1,600 computers linked through the Internet globally working for eight months at the rate of one million instructions per second. If additional information or cracks within the system are known, it is possible to break encryption keys even more quickly, which has also been documented.

There are various ways of enhancing access security through the use of passwords (see Alexander 1995). Appropriate education of users is an initial first step in which information is given concerning ways of ensuring that passwords are not disclosed, guessed, or otherwise compromised by the user in question. Systems should be used which change passwords regularly, or which deny access after a specified number of consecutive tries using invalid passwords. Terminals should have automatic shutdown facilities when they have not been used for specified periods, such as five minutes. Single use passwords, where the password changes with every successive login according to an agreed protocol known to the user and system operator, could also be used. The SecureID card, for example, generates a new password every sixty seconds which is a function of the time and a secret 64-bit seed that it unique to the card (Denning 1998: 44).

Challenge-response protocols may also be used as a means of carrying out user authentication. The server generates a random number which is sent to the card. In a public key system, the card digitally signs the number and returns it to the server. The server then validates the digital signature. Alternatively, call-back devices may be used. After the user dials into a computer through a modem and

gives his or her identity, the system disconnects the user and then telephones the user on a number previously registered with the server. After the user is verified, the transaction can then proceed (see, for example, NetCrusader 1998). Such a system is, however, able to be overcome through the use of call-forwarding arrangements (Denning 1998: 45).

Another user authentication system makes use of space geodetic methods to authenticate the physical locations of users, network nodes, and documents. One company, CyberLocator, involves the use of a location signature sensor which uses signals transmitted by satellite to provide a location on earth at any given time. Users are thus able to be located at the time they attempt to gain access to the system, which provides a safeguard against individuals pretending to be legitimate users who are located in a different physical location (Denning 1998: 45).

Biometrics

One way in which problems of password and token security may be overcome, is for users to identify themselves biometrically. Already there are a wide variety of such systems being used which make use of an individual's unique physical properties. Common biometric identifiers today include fingerprints, voice patterns, typing patterns, retinal images, facial or hand geometry, and even the identification of a person's subcutaneous vein structures or body odours (Johnson 1996). The body odour system called 'Scentinel' was developed by the British firm Bloodhouse Sensors and requires that you pass your hand under a sensor which records your unique smell and compares it with one registered in the database (Alexander 1995). It ignores extraneous smells such as perfume.

Fingerprint identification systems are now being used in retail stores and for access to ATMs (Anonymous 1996), whilst in California, a company 'Identix', has developed a system which has fingerprint recognition sensors on mobile telephones, computer keyboards, and plastic cards (Young 1999). The Bank of Texas has also recently introduced iris recognition systems for its ATM network.

The costs and volume of data required to be stored online to enable comparison for any potential user may, however, be prohibitive and there is always the possibility that computer security systems could be compromised by reproducing data streams which correspond with the biometric characteristics in question. An additional problem is that users must be required to provide samples of their personal characteristic and that the security of these samples could be compromised. Recognition systems are also, at present although not presumably in the future, costly and sometimes slow to use.

Digital Signature Security

The use of public key encryption systems also have their security risks. Public key systems require that cryptographic key pairs be issued to individuals who are able to establish their identity to an appropriate degree of assurance by supplying multiple and independent sources of identification such as those required when accounts are opened with a financial institution. Primary documentation (such as a passport, birth certificate etc) along with matching secondary documentation (such as a bank statement, car registration papers etc) would be required in order to satisfy the degree of documentary evidence of identity required.

This, however, may prove to be one of the system's weakest points in terms of security. Already systems which require the identification of individuals when they open accounts with financial institutions have been circumvented by offenders producing documents which have been forged or altered through the use of computerised desk-top publishing equipment.

Birth certificates are particularly susceptible, as they can be fraudulently obtained in some jurisdictions with little difficulty by tendering scant details to the issuing authority. Birth certificates often do not entail cross-referencing, such as address, nor are they amended when the subject is deceased. Fraudulently obtained birth certificates may then be used to obtain other false documentation, such as passports and drivers' licences. Many primary documents are now protected through the use of various security devices, such as holograms, micro-printing and void pantographs (which reveal the word 'void' when photocopied). Digitally-produced passports are also now being made with enhanced levels of security. Most of these, as well as other security devices, have all been compromised, however. Unless staff who inspect such documents are fully trained in recognising false or altered documents, it is possible to open various accounts in a variety of false names and make use of all of the banking facilities available, including loan facilities, until such time as the fraud is discovered or the false identity made known.

An example of the weaknesses of this manner of establishing one's identity arose recently in Victoria, Australia where an offender opened forty-two separate bank accounts throughout the Melbourne metropolitan region making use of false identification documents. Each account made use of a different false identity created by the offender using desk-top publishing equipment. Forty-one false birth certificates were produced along with forty-one false student identification cards, some containing photographs. Eventually, a driver's licence was obtained by relying on the false documents already produced. Along with the false bank accounts, the offender was able to register a business name, and make withdrawals from cheque accounts totalling tens of thousands of dollars. Health care refunds were also obtained and various retailers defrauded (Morton 1998).

There are various solutions to the problem of counterfeit identification documentation fraud. First, and perhaps most importantly, is the need to validate identification documents with the issuing source. Staff presented with a birth certificate should, for example, check if the details correspond with those held in the central office of Births Deaths and Marriages. An electricity account tendered as an identification document should be validated by checking with the electricity company concerned. This may not always solve the problem, however, as telephone answering services can be manipulated to support the creation of false employment or identity details.

Secondly, staff involved in validating documents need to be instructed as to the security features which are present on original documents, what original documents look like, and how forged documents appear.

Thirdly, modern security features should be incorporated on all primary identification documents and even secondary documents if at all possible. Among these new technologies are security printing, in which colour-coded particles are embedded into the medium, 'tracer fibre' which can be woven into textile labels, and hidden holographic images which can be read with a hand-held laser viewer or machine reader, thus permitting verification of a product's origin and authenticity. Similarly, technologies have already been developed which make counterfeiting extremely difficult.

In any system which entails the identification of individuals to whom cryptographic keys are to be issued, these primary fraud prevention procedures would need to be included.

Once questions of identification have been resolved, issues would arise in relation to the manner in which keys or hardware tokens are given to users. Standards would also need to be complied with for the storage and use of keys, perhaps by requiring keys to be used off-line or with the use of a smartcard which is able to process transactions.

The problem remains, however, that private key data or tokens themselves must be communicated to users. The financial world has already experienced considerable problems in transferring possession of plastic payment cards to users and similar problems could arise with respect to cryptographic keys which are stored on smartcards. Adequate security precautions would need to be used to ensure that tokens are passed securely to users from the issuing authority.

Another area of risk concerns the generation of cryptographic keys. It may be possible for the individual who generates a public and private key pair to retain a copy of the private key for later illegal use. Legislation may need to be enacted which will hold the key generator liable for subsequent losses which arise out of the compromise of a key issued by that generator. Cryptographic keys would be kept on the hard drive of a computer with the cryptographic service activated by a smartcard inserted into the PC. Smartcards may also be used to sign a digital signature and to authenticate the identity of a user.

In addition to the risks associated with compromising access mechanisms such as PINs, passwords, and biometric devices, the possibility exists that smartcard tokens themselves may be altered or counterfeited. Already this has taken place in relation to smartcards used for small value commercial transactions. Where keys are stored on personal computers or servers, their security may be compromised in which case appropriate risk management measures need to be taken.

Fraud Detection Software (Neural Networks)

If one is unable to prevent on-line fraud from taking place entirely, then at least it may be possible to identify the presence of fraudulent transactions quickly in order to reduce the extent of any losses which are suffered or the occurrence of repeat victimisation.

A number of organisations are now providing software for use in the prevention of electronic funds transfer fraud. Software has been devised to analyse user spending patterns in order to alert individuals to the presence of unauthorised transactions and also merchant deposit monitoring techniques to detect claiming patterns of corrupt merchants. Nestor Inc., for example, provides software called PRISM (Proactive Fraud Risk Management) which is used to detect credit card fraud such as lost cards, stolen cards, counterfeit cards, fraudulent applications, cards never received, mail order, phone order and catalogue sales and merchant fraud. It is designed for use by credit card issuers, credit card processors, credit card acquirers, Merchant Banks, and anyone who has over 500,000 card holder accounts. The cost is between A$300,000 and A$1,500,000 depending on system requirements and configuration (see Nestor Inc. 1996). Similar types of systems could be adapted to monitor on-line transactions. The success of such an approach depends, however, upon the extent to which the software cannot be interfered with or modified.

Legislative Measures and Codes of Practice

Conducting a secure system for electronic commerce may require various laws to be examined in order to ensure that fraud may effectively be investigated and prosecuted. A range of different approaches have been taken to law reform internationally in order to accommodate on-line commerce with some parliaments enacting highly specific reforms to define ‘documents’, ‘writing’, and ‘signatures’ as well as to specify the rules which govern the attribution of communications.

In Australia, a more generalised approach is being adopted with the enactment of broad, technology-neutral provisions which would constitute a basis for more specific legal changes which could be introduced subsequently (Australia, Attorney-General’s Department 1998).

As an alternative to the use of legislative regulatory controls, the banking and credit industries have relied on the use of codes of conduct to prevent fraud and to resolve disputes between institutions and customers. Codes have the dual function of acting as a form of education and publicity for both institutions and customers, as well as providing a statement of recommended practice which may be relied upon to resolve individual disputes.

Codes of conduct are, however, only going to be an appropriate regulatory mechanism where financial institutions or system operators are involved. If electronic money or stored value cards are used on the Internet, then only the consumer and the merchant may be involved. This may require existing codes of conduct to be re-written.

It may now be appropriate for an Internet Commercial Code of Conduct to be established in order to deal with the allocation of risk and determination of liability involved in Internet-based transactions. Issues which could be dealt with in the Code could include: guidelines on users’ obligations in maintaining computer hardware in a secure environment; principles to be observed for obtaining, storing, and using encryption keys securely; principles to be observed for storing key tokens securely and for preventing unauthorised access to tokens; obligations to be complied with regarding security and privacy of data; and principles to be observed in determining liability and the allocation of loss arising out of the use of the use of the Internet.

CONCLUSIONS

This paper has described a wide variety of ways in which funds may be stolen through exploiting security flaws in electronic funds transfer systems used in conjunction with on-line commerce. The range of electronic systems used to conduct commercial transactions is increasing rapidly and considerable effort is being directed at ensuring the security of digital transmissions which represent monetary value. The opportunities for fraud are, however, substantial.

The solution to electronic funds transfer crime on the Internet will ultimately involve the adoption of a range of strategies both technological and strategic in which close cooperation will exist between all those involved in providing and using systems. This includes telecommunications carriers and service providers, financial institutions, retail merchants, and individual users.

One area of particular importance relates to the need for strategies to be used which will enable the emergence of weaknesses in systems to be quickly identified. Once recognised, there should be a prompt

response to the problem. In ensuring that particular weak points in security systems are identified and weaknesses solved, it is likely that technology will provide the most effective response.

Probably the greatest source of risk in conducting on-line business lies in the area of user authentication. False identity fraud has been a continuing problem in commerce for decades now and it is likely that it will continue in adapted forms on the Internet. If passwords continue to be used to restrict access to computers then they should be protected by the various security devices I have mentioned. Biometric identifiers will, presumably, become much more widely accepted as Internet commerce develops.

In planning for the future, it will be necessary to ensure that the weak points in security protocols are not overlooked. As in other areas of fraud control, the weak points in on-line commerce will invariably arise out of human factors rather than technological considerations.

-

References

Alexander, M. 1995, *The Underground Guide to Computer Security*, Addison-Wesley Longman Inc., New York. http://www.securitymanagement.com/library/000273.htm

Anonymous 1996, "Fingerscan's $2.5m Deal", *Security Australia*, vol. 16, no. 10, p. 2.

Australia, Attorney-General's Department 1998, *Electronic Commerce: Building the Legal Framework*, Report of the Electronic Commerce Expert Group to the Attorney-General, Australian Government Publishing Service, Canberra.

Bellcore 1996, "New Crypto-Attack Weakens Seeming Strength in Smart Cards, Secure ID Cards, or Vale Cards", Internet http://www.infowar.com/sample/infosec4.html-ssi

Bowes, C, 1996, "Digital Dollars", *Bulletin*, 20 August: 50.

Carter, S, 1996, "Online 'Bank' Cashes in on Cyber Commerce", *The Australian*, 30 July, Computers, p. 49.

Da Silva, W. 1996, " 'Hackers' May Evade Charges", *The Age (Melbourne)*, 11 June: C1.

Denning, D. 1998, 'Cyberspace Attacks and Countermeasures', in Denning, D. E. and Denning, P. J. *Internet Besieged: Countering Cyberspace Scofflaws*, ACM Press, New York, pp. 29-55.

Denning, D. E. 1999, *Information Warfare and Security*, ACM Press, Reading, Massachusetts.

Hansell, S. 1996, "AT&T and Wells Fargo Investing in an Electronic Cash Card", *New York Times*, 19 July, p. C2.

Holland, K. 1995, "Bank Fraud, The Old-Fashioned Way", *Business Week*, 4 September, p. 88.

Johnson, E. 1996, "Body of Evidence: How Biometric Technology Could Help in the Fight Against Crime", *Crime Prevention News*, December, pp. 17-19.

Jupiter Communications 1999, ‘Travel Suppliers Missing Online Market Potential’, http://www.jup.com/jupiter/press/releases/1999/0512a.html

Kennedy, D. 1996, "Russian Pleads Guilty to Stealing from Citibank Accounts", http://catless.ncl.ac.uk/Risks/17.61.html#subj

Levi, M. and Handley, J. 1998, *The Prevention of Plastic and Cheque Fraud Revisited*, Home Office Research Study No. 182, Home Office, London.

Levy, S. 1994, "E-Money (That’s What I Want)", *Wired*, December, pp. 174-9, 213.

Mackenzie, R. 1998, "Virtual Money, Vanishing Law: Dematerialisation in Electronic Funds Transfer, Financial Wrongs and Doctrinal Makeshifts in English Legal Structures", *Journal of Money Laundering Control*, vol. 2, no. 1, pp. 22-32.

Mackrell, N. 1996, "Economic Consequences of Money Laundering", in Graycar, A. and Grabosky, P. (eds.), *Money Laundering in the 21st Century: Risks and Countermeasures*, pp. 29-35, Australian Institute of Criminology, Canberra.

Meijboom, A. P. 1988, "Problems Related to the Use of EFT and Teleshopping Systems by the Consumer", in Poullet, Y. and Vandenberghe, G. P. V. *Telebanking, Teleshopping and the Law*, Kluwer Law and Taxation Publishers, Deventer, pp. 23-32.

Morton, G. 1998. Personal communication, Detective Sergeant Gavin Morton, Victoria Police, Major Fraud Group, 22 January 1998.

Nestor Inc. 1996, "Proactive Fraud Risk Management: Neural Network Based Credit Card Fraud Detection from Nestor Inc." Internet http://www.nestor.com/rmd.htm

NetCrusader 1998, ‘NetCrusader Product Family: Security Solutions for the Enterprise’, http://www.gradient.com/Products/NetCrusader/netc_frt.htm

Newton, J. 1995, *Organised Plastic Counterfeiting*, HMSO, London.

Nicholson, E., ‘Hacking away at liberty’, *Times (London)*, 18 April 1989.

NUA Internet Surveys 1999a, ‘Internet Usage’, http://www.nua.ie/surveys/how_many_online/index.html

NUA Internet Surveys 1999b, ‘National Consumers League: Seven Percent of US Users Hit by Credit Card Fraud’, http://www.nua.ie/surveys/?f=VS&art_id=905354917&rel=true

Rawitch, R. 1979, "Expected Bank Plot to Fail", *Los Angeles Times*, 23 February, pp. 1, 27.

Smith, R. G. 1997, "Plastic Card Fraud", in *Trends and Issues in Crime and Criminal Justice*, No. 71, Australian Institute of Criminology, Canberra.

Spinks, P. 1996, "Tests Show Up Smart Card Flaws", *The Age (Melbourne)*, 6 December.

Sullivan, C. 1987, Unauthorised Automatic Teller Machine Transactions: Consequences for Customers of Financial Institutions", *Australian Business Law Review*, vol. 15, no. 3, pp. 187-214.

Visa International 1997, "SET Draft Reference Implementation",

http://www.visa.com/cgi-bin/vee/sf/set/intro.html?2+0.

Webb, B. 1996, "Preventing Plastic Card Fraud in the UK", *Security Journal*, vol. 7, pp. 23-5.

Young, S. 1999, ‘Thumbs Up for Fingerprint-Based Ids’, *The Age (Melbourne)*, IT p. 4.