

**Australian Society of Certified Practising Accountants
CPA Congress 2000**

**CPAs—Leading With Vision and Commitment
Sub-Theme—Integrity
25 October 2000
Sydney Hilton Hotel**

**Session T39—Electronic Fraud
4.10 to 5.10pm**

**Dr Russell G. Smith
Senior Research Analyst
Australian Institute of Criminology**

INTRODUCTION

The convergence of computing and communications technologies has changed dramatically the nature of our lives, at least for those of us who live in developed countries. We are able to do our shopping and banking from home, work and be paid electronically, and engage in leisure activities using computers. Government benefits are also able to be processed electronically and a wide range of services delivered on-line. 'Digitisation', or the process of reducing information to electronic streams of '0s and 1s' that are stored on computers, has enabled people to communicate more effectively and at lower cost than in the past. It has also meant that geographical boundaries are able to be crossed more easily. This has enhanced the process of globalisation of economic and social life enormously.

These same technologies that have provided so many benefits have, however, created enormous opportunities for economic offenders. Fraudsters are able to communicate with each other in secret, disguise their identities in order to avoid detection, and manipulate electronic payment systems to obtain funds illegally. They are also able to target a wide range of potential victims throughout the world, all from the comfort of their home or office. The risk of fraud is one of the principal barriers to electronic commerce systems becoming widely accepted in the community.

Australians, in particular, are avid users of new technologies. The Internet usage surveys carried out by the Australian Bureau of Statistics (1998, 1999, 2000), for example, have found an increase of forty-two per cent in the number of adults in Australia who had gained access to the Internet between November 1998 and February 2000—4.2 million adults (31 per cent of the adult population) to 6 million adults (43 per cent of the adult population).

The surveys also found a 113 per cent increase in the number of adults who had used the Internet to purchase or order goods or services for their own private use between November 1998 and February 2000—(286,000 or 2.6 per cent of adults in the twelve months to November 1998 to 740,000 adults (5 per cent of Australian adults) in the 12 months to February 2000 (a 2.4 per cent increase in the percentage of the adult population).

However, the percentage of Internet shoppers who paid for goods and services by disclosing their credit card details on-line, dropped by 6.5 per cent—from 80.5 per cent in November 1998 to 74

per cent in February 2000. This reduction is perhaps indicative of the concern which exists in the community regarding the security of on-line payment mechanisms. It also raises the important question of 'integrity' of electronic business systems—the sub-theme of today's papers at this Congress.

Although some may be reluctant to use the new technologies through fear of being victimised, the expansion of electronic and mobile commerce cannot be halted, particularly for business and government activities. Forrester Research, for example, has estimated that global business-to-business electronic commerce will be worth \$2.7 trillion by 2004 while the Gartner Group puts this figure closer to \$7 trillion. (*San Jose Mercury News* cited by O'Brien 2000).

At present, books / magazines and computer software / equipment are the most common types of products purchased on-line. The potential exists, however, for anything to be purchased electronically and recently a number of higher-value transactions have been conducted electronically with purchasers buying holidays, cars, and even houses on-line. We have also seen the establishment of a number of on-line auction houses and the use of the Internet for on-line share trading and gambling, each of which entail larger sums of money. The potential losses due to on-line fraud could, therefore, be substantial.

THE EXTENT OF ELECTRONIC FRAUD

As electronic commerce continues to expand in terms of the range of products and services which offered for sale on-line, and as the number of users continues to increase, so the opportunities for dishonesty and fraud have also increased.

A worldwide clean-up operation, involving the Office of Fair Trading in Britain and its counterparts in twenty-two other countries, identified 1,159 potential 'get rich quick' schemes being advertised on Internet sites (Office of Fair Trading 1998).

In the United States, over 18,600 complaints were registered on the Federal Trade Commission's fraud database 'Consumer Sentinel' in 1999, more than double the number in 1998—when 8,000 were registered (United States, Department of Justice 2000). In a telephone survey of 1,006 on-line consumers conducted for the National Consumers League in the United States between April and May 1999, twenty-four per cent said they had purchased goods and services on-line. Seven per cent, which represents six million people, however, said that they had experienced fraud or unauthorised use of credit card or personal information on-line (Louis Harris and Associates Inc 1999). Another commentator has estimated that as much as ten per cent of on-line commerce may involve consumer fraud (Rothchild 1999, p. 897, n. 11).

In 1999, a survey was conducted at the University of Utah of Internet trading which was coordinated by Consumers International and funded by the European Union. Representatives of those groups bought more than 150 items from Web sites based in seventeen countries, and then tried to return them. It was found that eight percent of the items ordered never arrived; many Web sites did not give clear information about delivery charges; a minority disclosed whether the laws of the seller's country or the buyer's country would apply in the event of a dispute, and only fifty-three percent had a return policy. In addition, only about thirteen percent of the sites promised not to sell customers' personal data to a third party and only thirty-two percent

provided information on how to complain if there was a problem with a transaction (Clousing 1999).

THE MECHANICS OF ELECTRONIC FRAUD

Commercial transactions can be carried out in a wide variety of ways electronically and each of the various payment systems involved has been targeted by fraudsters. In addition, misrepresentation concerning one's identity often lies at the heart of electronic fraud.

Fraud Involving Paper-Based Payment Systems

Where goods and services are obtained on-line and paid for using paper-based instruments, such as money 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 electronic transactions to be carried out quickly, 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.

Fraud Involving Direct Debit 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.

The principal safeguard against such fraud involves merchants taking adequate steps to authenticate the account details provided by the purchaser and to ensure that adequate funds are held in the account to cover the purchase. Obtaining authorisation from a financial institution is the first step in fraud prevention and some banks are now offering real-time authorisation for transactions above the specified floor limits.

Fraud Involving Electronic Funds Transfer 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 (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. Account information is 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 customer permitting funds to be transferred from the customer's 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 Registration 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.

Fraud Involving Card-Based Systems

Clearly, it would greatly facilitate electronic 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. 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 (Spinks 1996; Denning 1999).

Fraud Involving 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, uses a form of electronic money known as 'E-cash' (E-cash 2000). 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.

Identity-Related Fraud

The advent of on-line commerce has also created new forms of illegality which are less likely to occur in traditional marketplaces. Many consumers, for example, now have great difficulty in identifying those with whom they do business. Some merchants may intentionally disguise their identity through the use of remailing facilities in order later to defraud customers and avoid detection (see Rothchild 1999, p. 927). Others may simply be neglectful in providing accurate and verifiable information.

The technology of the Internet makes it relatively simple for users to disguise their identities. Electronic mail and Internet addresses may be manipulated by including details which are misleading or the source of a message may be made anonymous or changed so that it appears to be coming from another user. Similarly, there is no way of knowing the commercial affiliations of those on the Internet. Referees for businesses or products might, in fact, be individuals employed specifically to indicate their approval of the venture or product in question.

Businesses might also choose legitimate-sounding names in order to improve their credibility or include domain names which are misleading. There has recently developed a practice in the United States and Canada of some businesses adopting domain names containing the names of Australian cities in order to improve their marketability and credibility, despite the fact that they have no connection at all with Australia.

In one case investigated by the ACCC (1997b), an Internet trader used the same domain name as another trader (the original bearer of the name), but with a <.com> suffix, as opposed to the <.net> suffix of the original site. The confusion created as to the identity of the actual proprietor of the site allowed consumers to be misled or deceived. The <.com> site did, however, include an inconspicuous notice stating that the site should not be confused with the <.net> site of the same name, although this could easily have been overlooked by those visiting the site.

TYPES OF ELECTRONIC FRAUD

There are three main types of business and consumer fraud that can take place electronically which correspond with traditional misleading and deceptive business practices: pretending to sell something you don't have whilst taking the money in advance (advance fee schemes); supplying

goods or services which are of a lower quality than the goods or services paid for, or failing to supply the goods and services sought at all (non-delivery and defective products and services); and persuading customers to buy something they do not really want through oppressive marketing techniques (unsolicited and unwanted goods and services).

Advance Fee Schemes

The gist of so-called 'advance fee schemes' is to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit in return for providing some modest payment in advance. The characteristics of this type of fraudulent scheme usually entail enlisting the services of the prospective victim to assist in an activity of questionable legality, thus providing some assurance that the victim would be unlikely to report the matter to the police, once defrauded. Thus, the offender is able to carry out the scheme repeatedly, sometimes in respect of the same victim, whilst police are faced with difficulties in finding witnesses and securing evidence.

Examples of on-line advance fee schemes include pyramid schemes that have the primary purpose of enlisting individuals to earn money through recruiting other persons such as through the use of E:mail chain letters and electronic mailing lists. One recent example investigated by the ACCC involved the Canadian Global Interactive Investments Club which advertised the fact that offshore banks would issue low-interest Visa cards via the Internet with the promise of no credit checks or income verification. The scheme was actually an international pyramid scheme, in which applicants were encouraged to recruit others in return for \$25 each (ACCC 1997b).

The Internet is also being used as a medium for Ponzi investment schemes and a variety of fraudulent business opportunity schemes as well as schemes that make use of on-line auctions. One of the most recent areas of concern relates to on-line securities fraud. A number of problems have already arisen with misleading information being given to investors and sharemarkets being manipulated via E:mail and the Internet.

Non-Delivery and Defective Products and Services

On-line fraud may also involve the merchant failing to deliver the goods when and where requested, or at all. This problem is exacerbated in global commercial transactions where long-distance delivery of goods is involved, sometimes entailing customs clearance and the payment of importation taxes. Alternatively, defective goods may be delivered or the wrong ones supplied, in which case consumers need to arrange for return and the refund of the price paid and any expenses involved. Many of these problems arise out of the fact that the goods are unable to be physically examined on-line in the first place.

Problems are also created by reason of the immediacy of some transactions in which goods or services are obtained at exactly the same time as payment is authorised (e.g. the purchase of software downloaded after providing a credit card number). In such cases, the traditional methods of stopping payment on a cheque or withdrawing authorisation for a credit card purchase are unavailable.

As consumers continue to increase their use of the Internet so the number of complaints about Internet Service Providers has also increased. The ACCC, for example, has investigated

allegations of overbilling, inadequate detail when billing, failure to supply technical support and other services as represented, failure to connect consumers to the Internet as agreed, not honouring requests to disconnect, the need to have a credit card to obtain services, attempts to avoid consumers' legal rights, and misrepresentations about the speed of Internet access and the experience of the Service Provider (ACCC 1999).

The Internet is now being used to advertise cable television decryption kits which enable consumers to obtain cable television without paying contract fees. Not only do such kits seldom work but they also require consumers to break the law by stealing cable services.

In the digital age, it has also become possible to purchase a variety of digitised products by downloading them electronically. The Internet provides a comprehensive advertising medium for these products, often with on-line samples being provided free of charge. Once payment has been transmitted to the merchant, the purchaser is able to download the complete product along with appropriate licences for its use. If, however, the software has been illegally copied, or if it is defective in some way, the consumer is often disappointed having paid for a product which cannot legally be used.

One area of on-line commerce that has developed prolifically is that which concerns the provision of pornographic images and sexual services. Some of these involve misleading and deceptive conduct. One example involved a company which advertised 'free' erotic photographs on the Internet. In order to see the images, the user was required to download software which, once installed, took control of the user's modem, cut off the local Internet Service Provider, and dialled a number in the former Soviet Republic of Moldova in Eastern Europe. The line remained open until the computer was turned off resulting in the user incurring large international telephone charges which were shared between the fraudster and the Moldovian telecommunications company. The fraud was detected through regular surveillance of customers' telephone accounts and the FTC was able to obtain an order requiring the defendants to place US\$1 million in an escrow account pending resolution of the case (*Federal Trade Commission v Audiotex Connection Inc* E.D.N.Y. Filed 13 February 1997).

Other on-line unlawful practices have included the advertising and sale of loan schemes, credit-repair kits, health and medicinal products such as cures for cancer and HIV, and educational qualifications from on-line universities, some of which fail to provide recognised, or indeed, any, valid qualifications, or occasionally fail to deliver any educational programs at all.

Unsolicited and Unwanted Goods and Services

Traditionally, there were few controls on advertising conducted by mail and direct marketers inflicted a barrage of advertising material on unsuspecting, and often unwilling, recipients. The electronic equivalent, known as 'spam', entails the same idea carried out through the use of E:mail. Its future equivalents may be even more invasive with self-opening attachments which could carry viruses into the recipient's computer hard drive causing damage and loss.

Bait advertising that involves the offer of a product or service for sale at an enticingly low price in order to sell some other more expensive product or service, or advertising a bargain which does not exist in order to attract customers to do business with the merchant is also able to be conducted electronically, as is inertia selling or sending unordered goods to consumers and

billing them in the hope that they will accept the goods and pay the bill without question. Various statutes now make such practices illegal which would, arguably, apply where electronic goods or services are provided to on-line consumers without their request. One could imagine software being provided as a self-opening attachment to an E:mail message which would then be billed. Similarly, requiring payment for access to Internet sites could amount to a form of inertia selling of the service in question.

DEALING WITH ELECTRONIC FRAUD

There are three generally-recognised ways of dealing with electronic fraud: hard regulation involving the use of the law; soft regulation using codes of practice; and strategies based on fraud prevention.

Hard Regulation

The regulation of advertising and marketing is a relatively new phenomenon which was gradually introduced as the twentieth century progressed. Consumer advocacy groups, which emerged in the 1970s, tended to demand strict legal prohibition of unethical practices (the so-called hard regulation approach) whilst those within the business community felt that self-regulation through the use of codes of practice was just as effective (soft regulation). With the introduction of new communications media, which included the telephone, radio, television and later the Internet, the debate as to the appropriate form which regulation should take has continued unabated.

Civil Action

Most of the advertising content which appears on the Internet is, legally, in the nature of an invitation to treat, or mere puffery. Only if interested consumers respond by disclosing their personal details, which may include a name, address and credit card account numbers, will a formal offer to purchase be transmitted which, if accepted and supported by consideration, will give rise to a legally binding agreement (*Carlill v Carbolic Smoke Ball Co* [1892] 2 QB 484—see Davies 1997).

Those who display misleading or deceptive advertisements on the Internet will generally only be held liable if the objectionable content forms part of the terms of the agreement. This may then give rise to a right to rescind the contract or sue for damages. In this sense, the use of the Internet raises legal issues which are substantively the same as those which arise out of paper-based advertisements and contracts. There are, however, particular evidentiary and forensic difficulties associated with establishing what transpired between the parties to an electronic transaction.

Consumer Protection

In Australia, one of the first consumer protection statutes to be enacted was the *Book Purchasers Protection Act 1899* (NSW) which sought to regulate the conduct of itinerant merchants who engaged in door-to-door sales. Since then, more restrictive legislative regimes have been devised to control marketing and advertising practices. These laws now help to ensure that consumers are not coerced into buying products which they do not want and are not otherwise deceived by

sellers. Statutory cooling-off periods, for example, are an example of a legislative means of empowering consumers who are subjected to high-pressure sales techniques in their homes (see Goldring, Maher, McKeough, and Pearson, G. 1998, pp. 270-306).

Both federal and state consumer protection laws apply to transactions in which Australian citizens or corporations are involved (see Goldring *et al.* 1998). The *Trade Practices Act 1974* (Cth) has provisions concerning consumer protection in Part V which proscribe various unfair practices and specify product safety standards and the operation of conditions and warranties in contracts.

The *Trade Practices Act 1974* (Cth) is, however, generally silent as to whether its provisions apply to conduct carried out electronically, although the breadth of its controls would, arguably, apply to all on-line activities carried out between corporations and consumers. Most of the consumer protection provisions of the Act specifically apply to conduct which 'involves the use of postal, telegraphic or telephonic services' (s. 6(3)) which would seem to exclude the Internet and E:mail which are not specifically 'telephonic'. This question has yet to be judicially determined in Australia although the ACCC takes the view that advertising on the Internet comes within the provisions of the *Trade Practices Act 1974* (Cth) (ACCC 1997a).

Although Australia's consumer protection laws would apply to contracts for the purchase of goods and services entered into with merchants who have advertised on the Internet, the imposition of liability may be difficult and costly where overseas corporations are involved. Most laws apply only to transactions carried out between Australian citizens and corporations within Australia. The cost, inconvenience, and logistics of cross-border legal proceedings make the imposition of liability on manufacturers, distributors, and merchants outside Australia unviable for most consumers.

Criminal Action

Finally, where property has been obtained by deception, or where false documents have been used to perpetrate a fraud, it may be possible to take criminal action. Criminal prosecution and punishment aims to deter those who perpetrate offences from re-offending and also to deter others in the community from acting illegally. It is difficult to quantify the precise extent to which the law deters crime, although well-publicised severe sentences clearly act as a deterrent to some extent.

In addition to conventional judicial punishments such as fines and imprisonment, there are a variety of other consequences which may follow the detection of fraudulent on-line conduct. These include adverse publicity, professional disciplinary sanctions, civil action, injunctive orders and, most recently, various forms of community conferencing. The confiscation of an offender's assets also represents an effective means of deterrence.

There are, however, a number of legal problems associated with proving deception carried out electronically. These are gradually being addressed by bodies such as the Model Criminal Code Officers Committee (2000) which in its latest Discussion Paper on computer crimes and jurisdiction has addressed many of the problems that arise in prosecuting crimes of dishonesty committed electronically. There remain, however, various forensic difficulties associated with

gathering evidence from computers in a number of different jurisdictions that often make proceedings both difficult and costly.

Soft Regulation

In view of the practical difficulties associated with relying upon legislative regulatory approaches to control misleading and deceptive on-line conduct, a number of industry groups have established self-regulatory groups which have devised their own standards and codes of practice. These were originally created to deal with non-electronic forms of advertising and marketing, but are now being extended to deal with conduct in the digital world.

Content Regulation

One of the primary strategies which seeks to prevent misleading and deceptive material from being disseminated electronically relates to the regulation of on-line content. This can be done through the use of screening software or through measures which require Internet Service Providers to monitor the material being publicised on their networks. Recent proposals have also entailed an element of hard regulation through the criminalisation of content deemed to be unsuitable which has been publicly disseminated.

Although the use of screening software has been widely advocated to control access to obscene and objectionable materials, its use in the control of misleading and deceptive advertising may be more difficult. Often the deception would not be discernible from an image or description of the product in question, and it might be impossible to differentiate between a legitimate advertisement and one which contains some misleading content, merely on the basis of the words or images used.

Instead, various industry groups have developed guidelines for Internet Service providers to follow when regulating the content of material which appears on their networks. The Internet Industry Association, for example, recognises that the Internet should provide a means to enable control of access to content while acknowledging it is impractical to filter all Internet content. Accordingly, the Association endorses methods by which content can be recognised and possibly excluded by content filter technologies as the most practical means of empowering responsible adults to control access to the Internet to determine appropriate controls on content.

As with the regulation of sexually explicit, racist, or other illegal content, questions of freedom of speech and the practicality of regulating content are the major areas of concern in adopting content regulatory approaches.

Certification and Endorsement Services

As an alternative to the use of prohibitory schemes which seek to identify objectionable content and to prevent users from gaining access to it, a number of certification and endorsement services have been established which provide users with information as to the reliability and acceptability of on-line material. Users are then free to decide whether or not they wish to make use of the material in question.

The Platform for Internet Content Selection (2000), for example, is a voluntary content rating system which helps users identify material which complies with specified standards. Although this has primarily been used to deal with obscene and objectionable content, it could be adapted to deal with misleading and deceptive content as well.

In the United States, the Council of Better Business Bureaus carries out a certification service in which Internet business sites are given a form of approval. Sites which display the authorised and encrypted seal of approval agree to abide by the Council's truth-in-advertising standards and to adopt its dispute resolution procedures. Members of approved Internet Associations are able to display the fact of their membership and consumers are able to check to see if organisations do, in fact, have membership.

The WebTrust program, which was developed by the American Institute of Certified Professional Accountants (2000), certifies Internet sites which demonstrate sound online business practices after having undergone an extensive auditing procedure. The audit, which varies in cost depending upon the complexity of the business and the site, includes checking the site's security measures, privacy practices and transaction-processing systems. The service is available from any WebTrust-licensed CPA or accounting company. Since the AICPA began the WebTrust program, some 1,500 CPAs and seventy-five accounting companies have been qualified as able to perform WebTrust audits (Tweney 1998). To date, only a small number of sites have successfully undergone the audit process, permitting them to display the WebTrust seal on their site. Like other third-party certification programs, WebTrust depends for its success upon widespread acceptance by on-line merchants and users, which, hopefully, will be achieved in time.

Certification and endorsement services have two primary benefits. First, consumers are able to rely upon the fact of a merchant being certified in order to have some measure of confidence in the trustworthiness of that merchant and in the availability of redress mechanisms if problems arise. Secondly, financial institutions involved in providing payment facilities could be encouraged to deal only with certified merchants who have agreed to comply with a code of conduct which meets certain minimum standards. This would provide a powerful industry-based inducement for merchants to undergo certification and to act responsibly and in conformity with established codes of practice.

One of the main problems with endorsement and certification, is the proliferation of services and the determination of appropriate standards. Already, some twenty so-called 'Webseals' are in circulation in Australia with the government providing a comparative table which sets out their various attributes (Department of Communications, Information Technology and the Arts 2000b). Determining acceptable standards and publicising these will represent a major challenge for the future.

Preventive Strategies

In addition to the use of both hard and soft-regulatory approaches, much can be achieved by way of fraud prevention strategies. These may extend from the creation of guidelines and policies on fraud control to the use of computer-based security techniques.

Management of Fraud Control

Adopting fraud control policies within organisations is one of the principal ways of preventing fraud, in both electronic as well as non-electronic environments. Establishing principles on, for example, the ethical use of information technologies and how to respond to instances of fraud are essential in conducting a business of any kind, whether or not it makes use of electronic commerce.

Of particular importance is the need to develop specific policies on computer security along with appropriate guidelines on reporting computer misuse and abuse. Policies need to deal with specific on-line behaviour of employees such as security of user authentication systems (e.g. passwords), access to and use of the computers for private purposes, personal use of electronic mail, downloading software, and the use of copyright material. Principles also need to be established to ensure that those who report illegal conduct are not disadvantaged by their conduct.

Personnel Monitoring

One of the most important areas in which technology-based fraud can be curtailed lies in ensuring that trustworthy and reliable staff are employed, particularly in senior positions of responsibility. The administration of modern technologically-based security systems involves a wide range of personnel from those engaged in the manufacture of security devices to those who maintain sensitive information concerning passwords and account records. Each has the ability to make use of confidential information or facilities to commit fraud or, what is more likely to occur, to collude with people outside the organisation to perpetrate an offence. Preventing such activities requires an application of effective risk management procedures which extend from pre-employment screening of staff to regular monitoring of the workplace. Long-term employees who have acquired considerable knowledge of an organisation's security procedures should be particularly monitored, as it is they who have the greatest knowledge of the opportunities for fraud which exist and the influence to carry them out.

Computer Usage Monitoring

Employees' use of computers and their on-line activities can be monitored through the use of software which logs usage and allows managers to know, for example, whether staff have been using the Internet for non-work-related activities. Ideally, agreed procedures and rules should be established which enable staff to know precisely the extent to which computers are able to be used for private activities, if at all. If staff are permitted to make use of computers for private purposes, then procedures should be in place to protect privacy and confidentiality of communications, subject, of course, to employees obeying the law.

Where certain on-line activities have been prohibited, it is possible to monitor the activities of staff, sometimes covertly such as through video surveillance or checking electronic mail and files transmitted through servers. Filtering software may also be used to prevent staff from engaging in certain behaviours. 'Surfwatch', for example, can be customised to deny employees access to specified content. When the employee requests a site, the software matches the user's ID with the content allowable for the assigned category, then either loads the requested page, or advises the user that the request has been denied. The software also logs denied requests for later inspection by management.

The use of computer software to monitor business activities also provides an effective means of detecting fraud and deterring individuals from acting illegally.

Personal Identification

Authentication of one's identity is crucial in preventing electronic fraud. At present, most authentication procedures involve the use of passwords or PINs. Ensuring that these are used carefully and are not able to be compromised represents a fundamental fraud control measure. In addition to user education, a variety of innovative ideas have been developed to protect passwords and to enhance user authentication (see Alexander 1995).

Systems are available which change passwords regularly, or which deny access after a specified number of consecutive tries using invalid passwords. Terminals have been devised with automatic shutdown facilities which operate when they have not been used for specified periods. Single use passwords, where the password changes with every successive login according to an agreed protocol known to the user and system operator, are also available. Challenge-response protocols and call-back systems have also been devised as a means of carrying out user authentication. Finally, space geodetic methods have been devised to authenticate the physical locations of users.

In the future, many user authentication systems will make use of so-called biometric identifiers which make use of an individual's unique physical characteristics. Common examples 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). Although such systems achieve much higher levels of security than those which rely upon passwords, they are expensive to introduce and raise potential problems in terms of privacy and confidentiality of the personal data stored on networks. It is also difficult to revoke biometric identifiers.

User authentication is also necessary when public key infrastructures are used. Public key systems are one way of helping to ensure that both consumers and merchants are confident of the identity of the person with whom they are dealing. Such technologies would not, however, prevent individuals from illegally obtaining access to private cryptographic keys by stealing tokens which hold keys or by presenting fabricated documentation in order to obtain key pairs fraudulently (see Office of Government Information Technology 1998). They do, however, represent a much more secure way on conducting on-line transactions than simply by trusting material that is displayed on the Internet and hoping that it will be secure

Information Services

Preventive action may also take the form of regular surveillance of the Internet by regulators in order to locate objectionable and illegal practices, providing educational material warning users of dangerous schemes and the use of authentication technologies to permit individuals to know with certainty with whom they are dealing in the on-line world.

Most regulatory agencies throughout the world provide information in paper form and electronically through Websites which alert consumers to misleading and deceptive practices.

One of the most comprehensive booklets directed at Australian consumers is *The Little Black Book of Scams* published by the Ministerial Council on Consumer Affairs (1999). In electronic form, the ACCC's Website gives advice on pyramid selling schemes, business opportunity schemes, and phoney prizes and lotteries. Examples of popular deceptive practices are listed along with the legal penalties which apply to those who run or participate in such activities. In addition, and in order to enhance consumer confidence in the Internet, the Australian government has produced a series of fact sheets which provide information to consumers about the risks of shopping on-line, and certain other issues such as paying tax and duty and privacy issues (Department of Communications, Information Technology and the Arts 2000a).

The ACCC (1997b) has also raised the idea of using information intermediaries to provide information about on-line merchants and the procedures involved in conducting business on-line, similar to the kinds of information which insurance or mortgage brokers provide. Several private enterprises, including the Australian Consumers Association, have set up an independent advice service on loans and mortgages offered on-line by financial institutions whilst various consumer subscription services publish independently conducted evaluations of products offered on-line. Consumer groups generally provide a good source of trusted information on how to avoid fraud. Groups, such as the Australian Consumers Association, conduct their own testing of products and services and publicise the results through subscriber based magazines such as *Choice* (Australia). Although consumer organisations already provide consumer information by various means, including the Internet, perhaps the role of consumer groups in providing information services could be increased.

CONCLUSIONS

Although some may question their effectiveness, on-line activities are already subject to a variety of laws and other regulatory controls. Those who engage in misleading and deceptive practices invariably infringe local laws in the jurisdiction in which they reside or the jurisdiction in which their material is read; or sometimes both. This often provides sufficient jurisdictional basis for the commencement of legal proceedings. The last thirty years has seen continual improvements in consumer protection legislation and dispute resolution procedures and many on-line activities fall within the scope of these initiatives.

Unfortunately, the remedies which are available to those who have been deceived electronically are often practically unavailable as they would require offenders to be extradited from other places or victims to take cross-border legal proceedings. Such action is invariably beyond the means of most individuals and costs far in excess of the amount lost in most consumer frauds.

Legal enforcement proceedings can, however, sometimes be taken on behalf of groups of consumers who have suffered loss in the form of class actions against large corporations. Although these are sometimes slow and costly, victims are empowered through the weight of numbers and compensation is occasionally able to be obtained.

The perpetrators of many on-line scams, however, are often not large corporations. They are able to close-down their operations quickly and easily, move assets to secure locations and use digital technologies to conceal their identities and disguise evidence. In such cases there is little likelihood of success whether civil or criminal proceedings are taken.

Consumers who transact business on-line need to be made aware of the risks they face and informed about the nature of misleading and deceptive practices which are present. Already there are substantial amounts of information of this nature available. The challenge lies in ensuring that consumers are made aware of its existence. In this regard, certification and notification systems, which permit consumers to identify readily businesses which have been found to be trustworthy, seem to provide the best option. Technology needs to be developed, however, to ensure that certification services are, themselves, unable to be manipulated. There could, for example, develop a trade in fraudulently acquired certificates of propriety which illegitimate businesses could attach to their Website. Fraud relating to the process of certification might also develop in the future as might the use of 'phoenix businesses' which re-establish themselves immediately they have been closed down because of improper practices.

Achieving integrity in electronic commerce will, therefore, become of the great challenges for the future. Professional advisers, such as CPAs, will have an important role to play in both informing their clients of the risks and countermeasures that are present as well as in administering some services, such as the WebTrust program. If there is one positive outcome associated with electronic fraud, it is that there will be abundant new opportunities for work for those involved in the computer security and fraud prevention industries.

REFERENCES

- Alexander, M. 1995, *The Underground Guide to Computer Security*, Addison-Wesley Longman Inc., New York.
- American Institute of Certified Professional Accountants 2000, 'WebTrust', <http://www.aicpa.org/webtrust/index.htm> (visited 21 July 2000).
- Australian Bureau of Statistics 1998, *Household Use of Information Technology, Australia 1998*, (Cat. No. 8146.0), Australian Bureau of Statistics, Canberra.
- Australian Bureau of Statistics 1999, *Household Use of Information Technology, Australia 1999*, (Cat. No. 8146.0), Australian Bureau of Statistics, Canberra.
- Australian Bureau of Statistics 2000, *Use of the Internet by Householders, Australia*, (Cat. No. 8147.0), Australian Bureau of Statistics, Canberra.
- Australian Competition and Consumer Commission 1997a, *Advertising and Selling*, ACCC, Sydney.
- Australian Competition and Consumer Commission 1997b, *The Global Enforcement Challenge: The Enforcement of Consumer Protection Laws in a Global Marketplace - Discussion Paper*, ACCC, Sydney.
- Australian Competition and Consumer Commission 1999, 'Internet Service Providers' <http://www.accc.gov.au/docs/catalog.htm> (visited: 30 April 1999).
- Clausing, J. 1999, 'FTC Holds Meeting on International E-Commerce', *New York Times*, June 8.
- Cook, V. 1999, 'Trust Me, I'm a Computer', *Communications Newsletter*, September, pp. 14-15.
- Davies, L. 1997, 'Contract Formation on the Internet: Shattering a Few Myths', in Edwards, and Waelde, C. (eds.), *Law and the Internet: Regulating Cyberspace*, pp. 97-120, Hart Publishing, Oxford.
- Denning, D. E. 1999, *Information Warfare and Security*, ACM Press, Reading, Massachusetts.
- Department of Communications, Information Technology and the Arts 2000a, 'Shopping on the Internet: Facts for Consumers', <http://www.dcita.gov.au/shoponline> (visited 21 July 2000).
- Department of Communications, Information Technology and the Arts 2000b, 'Website Seals of Approval: A Comparative Examination', http://www.dcita.gov.au/nsapi-graphics/?MIval=dca_dispdoc&pathid=%2fshoponline%2fsealtable%2html (visited 21 July 2000).
- E-cash 2000, 'E-cash Technologies Inc Home Page', <http://digicash.com/> (visited 21 July 2000).
- Goldring, J., Maher, L. W., McKeough, J., and Pearson, G. 1998, *Consumer Protection Law*, 5th ed., Federation Press, Sydney.

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.

Kennedy, D. 1996, 'Russian Pleads Guilty to Stealing from Citibank Accounts', <http://catless.ncl.ac.uk/Risks/17.61.html#subj> (visited 2 May 2000).

Louis Harris and Associates Inc 1999, *Consumers and the 21st Century: A Survey Conducted for the National Consumers League*, Louis Harris and Associates Inc, New York.

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

Ministerial Council on Consumer Affairs 1999, *The Little Black Book of Scams*, Department of Treasury, Canberra.

Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000, *Damage and Computer Offences: Discussion Paper, Chapter 4*, Commonwealth Attorney-General's Department, Canberra.

O'Brien, Chris 2000, 'The Next Revolution?', *The Age (Melbourne)*, I.T.(2), 27 June, p. 1.

Office of Fair Trading 1998, 'Internet Scams Deleted, Sweep Identifies 'Get Rich Quick' Schemes', *Fair Trading Magazine*, Spring, Office of Fair Trading, London.

Office of Government Information Technology 1998, *Gatekeeper: A Strategy for Public Key Technology Use in the Government*, Australian Government Publishing Service, Canberra.

Platform for Internet Content Selection 2000, 'Platform for Internet Content Selection Home Page', <http://www.w3.org/PICS/> (visited 21 July 2000).

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

Rothchild, J. 1999, 'Protecting the Digital Consumer: The Limits of Cyberspace Utopianism', *Indiana Law Journal*, vol. 74, pp. 893-989.

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.

Tweney, D. 1998, 'Sex Scam Points Out Lack of Safeguards in Online Business', <http://cnn.com/TECH/computing/9903/11/net.schemes.ap/> (visited 15 March 1999).

United States, Department of Justice 2000, *Internet Fraud: Appendix B*, Report of the Criminal Division's Computer Crime and Intellectual Property Section <http://www.cybercrime.gov/append.htm> (visited 5 July 2000).

Visa International 1997, 'SET Draft Reference Implementation', <http://www.visa.com/> (visited 2 May 2000).