Controlling Fraud on the Internet: A CAPA Perspective

Controlling Fraud on the Internet: A CAPA Perspective

A Report for the Confederation of Asian and Pacific Accountants

Russell G. Smith and Gregor Urbas

Confederation of Asian and Pacific Accountants

Australian Institute of Criminology Research and Public Policy Series No. 39

ISSN 1326-6004

National Library of Australia Cataloguing-in-Publication entry

Smith, Russell G.
Controlling fraud on the Internet : a CAPA perspective : a report for the Confederation of Asian and Pacific Accountants

Bibliography
ISBN 0 642 24242 9.

1. Internet fraud – Pacific Area. 2. Internet fraud – Pacific Area – Prevention. 3. Internet – Security measures – Pacific Area. 4. Internet – Law and legislation – Pacific Area. I. Urbas, Gregor. II. Australian Institute of Criminology. III. Confederation of Asian and Pacific Accountants. IV. Title. (Series : Research and public policy series ; no. 39).

364.168

Published by:

Confederation of Asian and Pacific Accountants
Level 3, Dewan Akuntan
2 Jalan Tun Sambanthan 3
50470 Kuala Lumpur
Malaysia
http://www.capa.com.au

Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Tel: 02 6260 9221
Fax: 02 9260 9201
email: aicpress@aic.gov.au
http://www.aic.gov.au

The Confederation of Aisan and Pacific Accountants (CAPA) represents national accountancy organisations in the Asia-Pacific region. The mission of CAPA is to provide leadership in the development, enhancement and coordination of the accountancy profession in the Asia-Pacific region to enable the profession to provide services of consistently high quality in the public interest.

The Australian Institute of Criminology (AIC) is Australia's national centre for the analysis and dissemination of criminological data and information.

Dr Russell G. Smith is Deputy Director of Research at the Australian Institute of Criminology.
Dr Gregor Urbas is a Research Analyst at the Australian Institute of Criminology.

Printed by Panther Publishing and Printing, Canberra

Foreword

One of the great benefits which developments in computing and communications technologies have brought is the enhanced ability of people to communicate with each other internationally. Information can be exchanged both quickly and cheaply using online services and business transactions have been greatly facilitated in many ways through the use of digital technologies. Although still predominantly English-language based, the Internet now has users located throughout the globe communicating in many languages. Developing nations, in particular, are seeing dramatic growth in their use of online services.

The Asia-Pacific region, in particular, is experiencing enormous growth in all forms of online services and both business and government are now making extensive use of the Internet for the dissemination of information as well as for electronic service delivery and online transactions. The large population of the Asia-Pacific region has, accordingly, proved to be a great inducement to the development of electronic commerce and the region is likely to become the greatest user of these technologies in the world in the near future.

Along with these developments, however, is the concern that misuse of online technologies for financial gain may grow at a correspondingly rapid rate. Already, Internet-related fraud has become a considerable problem in the United States and the European Union, and it is likely that those within the Asia-Pacific region will also be subjected to acts of fraud and economic crime facilitated through the use of Internet-based technologies. Given the global reach of the Internet and the rapid expansion of electronic commerce, it is inevitable that countries in the Asia-Pacific region will be affected by Internet fraud in the years to come.

It is trite to say that crime in the twenty-first century knows no borders, and it can be predicted that the Asia-Pacific region will be subjected to online victimisation in direct proportion to its usage of digital technologies. It is timely, therefore, for those in the region to understand the nature of the risks they face and to make use of the latest fraud prevention strategies that are

available. Not every risk can be avoided, but with a sound knowledge base, and effective use of appropriate technologies, the level of harm might be minimised.

Some of the key challenges in responding to electronic crime lie in establishing partnerships between agencies and organisations and in sharing information widely across nations. In this regard, key stakeholders need to coordinate the efforts of those in individual countries in order to ensure that initiatives are not duplicated and achievements not overlooked. In the Asia-Pacific region, the Confederation of Asian and Pacific Accountants (CAPA) is an extensive network of accounting professionals with the ability to coordinate efforts at fraud reduction among the business community and to mobilise governments to adopt uniform and effective measures to deal with economic crime. CAPA is, therefore, ideally placed to mobilise the fight against Internet fraud in the region.

CAPA was established in 1957 and represents 31 national accountancy organisations in 21 countries with a total membership of almost 700,000 accounting professionals. CAPA is by far the largest regional accountancy organisation, with its geographical area spanning half the globe. The current members of CAPA are Australia, Bangladesh, Canada, China, Fiji, France, Hong Kong, India, Japan, Korea, Malaysia, Mongolia, Nepal, New Zealand, Pakistan, Philippines, Samoa, Solomon Islands, Sri Lanka, Thailand and the United Kingdom.

On 28 and 29 April 2000, the 54th CAPA Executive Committee meeting held in Macau identified crime relating to electronic commerce and Internet-related fraud as problems of increasing concern in the Asia-Pacific region. In order to assess the scale of the problem and the range of possible solutions, in November 2000, CAPA commissioned the Australian Institute of Criminology (AIC), Australia's national centre for the analysis and dissemination of criminological data and information, to undertake a study on behalf of CAPA of Internet-related fraud as it affects business and government organisations in the Asia-Pacific region. The AIC works regularly with a range of international bodies including the United Nations Office for Drug Control and Crime Prevention on topics such as the Global Program Against Trafficking in Human Beings focusing on the Asia-Pacific region, and the Council for Security Cooperation also in the Asia-Pacific area.

In order to limit the scope of the study, the AIC was asked to examine the problem in those countries with current representation as members of CAPA. Other countries in the region are likely to experience Internet-related fraud to a similar extent as current CAPA member countries, and the results of this study should have relevance to those throughout the region. The current analysis will, however, focus on the experience in the 21 current member countries. In the case of non-regional members, such as the United Kingdom, Canada and France, their experience of Internet-related fraud will only be examined in so far as it concerns their business and government activities within the region.

The study also principally examines the fraud risks associated with electronic commerce on the Internet in business and government contexts, rather than consumer transactions. Although the problem of Internet fraud perpetrated against consumers remains a problem globally, this report focuses on the less well documented problem of fraud involving business and government electronic transactions which, as yet, has not been subjected to rigorous study. As such, this report identifies some of the key areas of risk and reviews the various strategies that are being suggested to control the problem in the Asia-Pacific region.

The current report provides a sound basis for CAPA to undertake further initiatives to control fraud on the Internet. The problem is not one that is amenable to simple or quick solutions. There are, however, many ways in which accounting professionals in the region can assist those in business and government to avoid some of the risks which new technologies of electronic commerce have created. This report provides an agenda for CAPA to take action that should help to make electronic commerce a safer and more efficient way in which to conduct business in the future.

Ranel T. Wijesinha
President
Confederation of Asian and Pacific Accountants

9 October 2001

Preface

Within the next few years, the Asia-Pacific region will have the largest number of Internet users of any region globally. Electronic commerce is also predicted to expand considerably, with massive increases in the number of business transactions in the region expected to be carried out electronically by 2003. Throughout the region considerable resources are being devoted to enhancing the technological infrastructure to facilitate on-line activities in both business and government contexts. Attention is also being directed to preventing any crime that might be associated with the use of these new business models.

This innovative report is the first systematic look at the problem of Internet fraud as it affects business and government in the Asia-Pacific region. Risks of electronic crime clearly know no boundaries, and as new technologies are taken up by countries within the region, so will opportunities arise for individuals—both within the region and beyond—to act dishonestly for personal gain.

After reviewing the nature and extent of the problem of on-line fraud, an extensive range of responses is considered—business and government policy responses; responses by investigatory agencies within the public and private sectors; legal and procedural reforms; and a wide variety of fraud prevention initiatives. A detailed agenda for controlling Internet fraud is set out to assist those within the region to take appropriate and effective measures to minimise the risks of economic crime that the Internet has created.

The Confederation of Asian and Pacific Accountants is to be congratulated for embarking upon this important research initiative. Its extensive network of accounting professionals throughout the region will help to ensure that the crime control measures outlined in this report will be taken up throughout the region without delay.

Adam Graycar
Director
Australian Institute of Criminology

9 October 2001

Contents

Foreword v

Preface ix

Executive Summary 1

Chapter 1: Introduction 12

1.1 Defining Internet Fraud 12

1.2 The Mechanics of Internet Fraud 13

1.3 Sources of Information 17

1.4 Aims of the Study 18

Chapter 2: Technological Infrastructure 19

2.1 Introduction 19

2.2 Telecommunications Carriers 22

2.3 Internet Service Providers 23

2.4 Internet / World Wide Web Traffic 24

2.5 Email Usage 27

2.6 Intranets / Virtual Private Networks 28

2.7 Internet Kiosks 28

2.8 Electronic Funds Transfers 29

2.9 Public Key Infrastructure 31

Chapter 3: Electronic Commerce in the Region 32

3.1 Electronic Commerce Activities 32

3.2 Projected Levels of Electronic Commerce 37

3.3 Significance for the Region 39

Chapter 4: The Nature and Extent of Internet Fraud 41

4.1 The Problem of Under-reporting 41

4.2 General Assessments of the Scale of the Problem 42

4.3 Specific Types of Internet Fraud 45

Chapter 5: Business and Government Policy Framework 64

5.1 Relevant Policy Developments 64

5.2 Fraud Control Policies 68

5.3 Codes of Practice 70

Chapter 6: Investigatory Framework **76**
6.1 Problems of Investigation and Policing 76
6.2 Trans-jurisdictional Problems 77
6.3 Regional Initiatives 78
6.4 Specialist Law Enforcement Agencies 80
6.5 Resources Devoted to Investigating Internet Fraud 83
6.6 Mutual Assistance 84
6.7 Forensic Computing and Accounting 84
6.8 Specialist Legal Expertise 85
Chapter 7: Legal Framework **86**
7.1 Legal Problems 86
7.2 Court Processes 87
7.3 Law Reforms Already Undertaken 88
7.4 How Laws Could be Improved 91
7.5 Criminal Proceedings Undertaken 93
Chapter 8: Fraud Prevention Initiatives **94**
8.1 Introduction 94
8.2 Regional Initiatives 94
8.3 Risk Management 96
8.4 Site Certification 97
8.5 Value Restrictions 98
8.6 Information Services 99
8.7 Educational Responses 101
8.8 Internet Sweeps 102
8.9 Technological Responses 103
Chapter 9: Conclusions **110**
9.1 Introduction 110
9.2 Theories of Internet Fraud 110
9.3 Risks and Remedies 111
9.4 Guidelines on Fraud Minimisation 114
9.5 The Future 114
9.6 Suggested Initiatives 115
References **118**
Appendix: Guidelines on Fraud Minimisation for Organisations Engaged in Electronic Commerce 135

Abbreviations

ACCC	Australian Competition and Consumer Commission
AIC	Australian Institute of Criminology
ASIC	Australian Securities and Investments Commission
ASP	application service provider
ATM	automatic teller machine
CAPA	Confederation of Asian and Pacific Accountants
EBT	electronic benefits transfer
EFTPOS	electronic funds transfer at point of sale
GDP	gross domestic product
GII	global information infrastructure
ISP	Internet service provider
LAN	local area network
MEPS	Malaysian Electronic Payment System
NII	national information infrastructure
OECD	Organisation for Economic Cooperation and Development
PIN	personal identification number
SET	secure electronic transactions
SWIFT	Society for Worldwide Interbank Financial Telecommunications

Executive Summary

Introduction

ES-1 This report provides a preliminary assessment of the problem of Internet fraud in a selection of Asia-Pacific countries. The countries included in the study were confined to the current membership of CAPA: Australia, Bangladesh, Canada, China, Fiji, France, Hong Kong, India, Japan, Korea, Malaysia, Mongolia, Nepal, New Zealand, Pakistan, Philippines, Samoa, Solomon Islands, Sri Lanka, Thailand and the United Kingdom.

ES-2 The aims of the study were to describe the nature and extent of Internet-related fraud as it affects business and government electronic commerce in the above countries; to assess the likely future trends in this type of fraud; to evaluate business and law enforcement strategies aimed at preventing this type of fraud; and to assess the extent to which current legal and business responses are adequate in dealing with the problem in the region.

ES-3 Internet fraud was defined as any act of dishonesty or deception carried out through the use of the Internet, or directed at the technologies that support the Internet. The study principally examined the fraud risks associated with electronic commerce on the Internet in business and government contexts, rather than consumer transactions. Examples include sending misleading and deceptive information to a business or government agency, manipulating electronic payment systems, misappropriating corporate information and intellectual property from the Internet, identity-related deception when using the Internet, and failing to honour commercial obligations entered into on the Internet.

ES-4 The study was confined to an examination and analysis of publicly available documentary sources of information. Although the bulk of material relied upon came from authoritative sources, some reports of criminal activities obtained from online sources could not independently be verified and should, accordingly, be treated with some caution.

Technological Infrastructure

ES-5 In order to assess the scale of the problem of Internet fraud in the region, and how it is likely to change in the future, evidence was gathered to document the development and size of the relevant technological infrastructure.

ES-6 Although the expansion of the infrastructure that supports the Internet is variable across the countries examined, it is clear that the Asia-Pacific region will have the largest number of users of the Internet of all regions globally in the near future. One estimate indicates that the region will have some 242 million Internet users by 2005.

ES-7 There is wide variation in the number of telecommunications carriers, Internet service providers (ISPs) and Internet hosts in the countries examined. Australia and Canada, for example, each has over 700 ISPs, while most Asian countries have less than 100 ISPs. Similarly, the number of Internet users varies considerably, with Australia, Canada, Hong Kong, Japan and Korea each having more than 3,000 per 10,000 of their populations online, while Bangladesh, India, Nepal and Sri Lanka have less than 100 users per 10,000 population.

ES-8 Although fixed-line services will continue to expand, the use of mobile communications and satellite connections is likely to take on greater importance in the region than elsewhere, in view of the under-developed land-based infrastructure in some countries.

Electronic Commerce in the Region

ES-9 Although consumer use of the Internet for commercial purposes has been surveyed quite extensively—and found to be expanding considerably—there are few studies of business and government use of the Internet for commercial purposes, other than in some of the larger economies in the region. There is a need for more extensive research to be undertaken of the manner in which the Internet is being used by all levels of business and government throughout the region. Only then will the full nature and extent of the risks associated with the use of the Internet be capable of quantification.

ES-10 On the basis of the information available, it appears that many businesses and government agencies are using the Internet for commercial activities at present throughout the region, although few actually conduct financial transactions online. Some sectors of the economy—particularly financial

services—engage in electronic commerce to a large extent. Smaller and less developed countries are only beginning to engage in electronic commerce for business and government purposes, although plans are being developed to increase usage once secure technologies have been established.

ES-11 It has been estimated that one quarter of all business purchases within the Asia-Pacific region will be made online by 2003. The Gartner Group has estimated that the business-to-business market in the Asia-Pacific region will be worth US$910 billion by 2004 and that by 2005, the Asia-Pacific region will account for 28 per cent of worldwide business-to-business commerce.

ES-12 Many government agencies throughout the region are beginning to make use of electronic service delivery, although regionally most still use the Internet for the provision of information at present, with only some agencies in the larger economies actually engaging in commercial transactions online.

ES-13 Given the global reach of the Internet and the rapid expansion of electronic commerce, it is inevitable that countries in the Asia-Pacific region will be affected by Internet fraud. The likely risks for the region will closely follow business and government usage patterns. Particular risks may be present for those countries with low levels of technological expertise and those which are unable to provide adequate funding for fraud prevention initiatives.

The Nature and Extent of Internet Fraud

ES-14 As in other areas of fraud and white-collar crime, Internet fraud is infrequently reported to authorities for investigation. Official statistics also do not generally isolate the specific means by which fraud is perpetrated, making them of little use in quantifying the scale of the problem. These problems exist in the Asia-Pacific region to a similar extent as in other regions globally.

ES-15 The principal sources of information concerning Internet fraud are business victimisation surveys and anecdotal accounts of successful criminal prosecutions that are reported publicly. The incidents of Internet fraud that are disclosed publicly represent only a small proportion of the total number of incidents that occur. There is a need for more systematic data to be collected on the nature and extent of Internet fraud and for more intensive surveys of the problem to be conducted.

ES-16 General estimates of consumer-based Internet fraud indicate that between five and 10 per cent of online transactions may involve fraud. There are no

comparable estimates for fraud involving business and government transactions conducted electronically, although it is likely that similar fraud rates would be present in these areas.

ES-17 Victimisation surveys have, however, found high rates of concern about online security and fraud risks amongst consumers, businesses and government agencies, which are continuing to retard the development of electronic commerce globally.

ES-18 Ten types of Internet fraud were examined in this study. They relate to: fraudulent online business practices; online funds transfer fraud; securities and investment fraud; identity-related fraud; procurement fraud; outsourcing risks; public sector fraud; theft of services / non-provision of services; information piracy; page jacking; digital extortion; and consumer fraud. Examples of fraudulent activities have been documented for each of these types of fraud in the Asia-Pacific region. Areas of particular concern for the region are securities and investment fraud, information piracy, and consumer fraud. Although some offenders operate from within the region, occasionally they may be based in other countries of the world and act in collaboration with individuals within the target country. There is also some evidence of organised groups becoming involved in Internet fraud and in laundering the proceeds of illegal activities internationally.

ES-19 In the absence of more systematic data collection by police agencies and regulators, the precise scale of the problem cannot be documented. Consumer victimisation surveys have found that fraudulent activities occur globally, and the same is likely to be the case for business and government Internet fraud within the region.

Business and Government Policy Framework

ES-20 Individual countries within the region have begun building policies for the expansion of information technology and the use of electronic commerce. These began in the context of consumer transactions, but are gradually extending to government and business activities. Most governments have policies and dedicated departments with an interest in the expansion of electronic commerce, although actual levels of implementation of such policies vary considerably throughout the region.

ES-21 One characteristic of the region that distinguishes it from some other developed countries is the attempt by some governments within the region to control access to the Internet and to regulate online content. To date,

however, such controls have largely dealt with content deemed to be objectionable in terms of its sexual subject matter or potential for subversive or anti-governmental action. Little attention has been given to the regulation of content that is misleading, deceptive, dishonest or fraudulent—other than in the context of consumer protection advice. The regulation of fraudulent material is an area that government and business policy should address throughout the region.

ES-22 Both business and government organisations are beginning to create fraud control policies that address the risks associated with Internet use. These, however, tend to be focused on national interests. In developing Internet fraud control policies, both public and private sector organisations should seek to harmonise their initiatives in order to deal with an essentially global problem.

ES-23 A range of codes of practice and best practice guidelines are beginning to emerge within the region to address Internet usage and the practices of those who provide online services and content. There is a need for uniform guidelines to be established that set out desirable online practices with a view to minimising the risks of fraud relating to electronic commerce. To date, most codes and guidelines have focused on consumer-oriented issues, leaving business and government organisations without guidance. CAPA may have a role to play in coordinating the development of appropriate best practice guidelines in this area.

Investigatory Framework

ES-24 Law enforcement and private sector investigatory agencies throughout the region face similar problems in addressing Internet fraud. Funding may not be adequate to enable trained staff to be employed and retained, and appropriate technology may be unable to be purchased for use in the public sector. In addition, the resources of the private sector may be inadequate to deal with the complexity and size of some matters. Other problems of mutual assistance, extradition of suspects, sophistication of forensic procedures, and length of court trials all have an impact on dealing with matters of this nature.

ES-25 The particular problems of anonymity and pseudonymity of persons accused of Internet fraud create further difficulties for investigators where individuals repudiate transactions or otherwise deny involvement in the alleged activities.

ES-26 A number of initiatives have begun to emerge in the region in recent times to address the problems of investigating cybercrime—and Internet fraud in particular. Various fora have been established to share information amongst public and private sector bodies, and a number of specially trained, dedicated units have been established to conduct complex investigations in this area. There is a need for more advanced countries to make such expertise available to less developed nations and to share strategic information throughout the region. This is beginning to occur on a global scale.

ES-27 Private sector investigatory organisations are also beginning to be established throughout the region to assist in the investigation and prevention of Internet fraud and cybercrime. Forensic accountants and legal practices with specialist expertise now operate within the region—although sometimes their services are beyond the geographical reach and financial means of those in smaller nations. There is, however, a continuing need for more highly trained legal and accounting professionals to provide services in this area throughout the Asia-Pacific region.

Legal Framework

ES-28 A variety of legal problems arise in prosecuting Internet fraud. These relate to the multiplicity of rules that exist in the various jurisdictions and the fact that many of the rules are complex, unclear and contradictory. A range of different approaches has been taken to law reform throughout the region in order to accommodate electronic transactions, with some parliaments enacting highly specific reforms to define words such as ‘documents’, ‘writing’ and ‘signatures’, as well as to specify the rules which govern the attribution of communications.

ES-29 Many advances have been made in the reform and amendment of laws relevant to Internet fraud and cybercrime in recent years, and there is an awareness of the need for laws to be technology-neutral as well as uniform across nations. The creation of international conventions and treaties has helped in this regard—although not all countries in the region have been involved in this process of reform.

ES-30 Resources are also needed to ensure that courts are adequately equipped in terms of digital technologies to deal with complex cases involving Internet fraud, and also that legal personnel and members of the judiciary have appropriate levels of training.

ES-31 Although some countries within the region have updated their laws to deal with computer-related crime, there is a need for a detailed stocktake to be undertaken of the amendments that have been made, and those that are still required. Only then will the process of harmonisation internationally be able to progress. Although individual countries will differ with respect to their perception of the seriousness of various forms of Internet-related crime and the extent to which individual activities should be proscribed, there remains a need to have uniform procedural and evidentiary laws to deal with crimes of this nature.

ES-32 There is also a need for judicial cases involving all forms of Internet-related crime to be kept on a register so that emerging trends can be identified across nations.

Fraud Prevention Initiatives

ES-33 The solutions to Internet fraud involve a wide range of strategies which extend from traditional crime control measures to novel technology-based means of preventing illegal conduct from being carried out electronically. Fraud prevention in the Internet age requires the use and adaptation of traditional measures (such as the use of appropriate fraud control policies and the provision of information) as well as the use of novel technological approaches (such as the use of effective means to authenticate users of computers and to track how they are using computers). Fraudulent conduct may also be deterred through the use of prosecution and punishment, although in the Internet age this is often difficult and costly to achieve.

ES-34 Throughout the region efforts are being made to address the various issues that arise in preventing Internet fraud. Improved user authentication procedures are being introduced, including those that utilise biometric technologies, which will help to solve the intractable problem of identity-related fraud. In addition, both public sector and private sector organisations are establishing effective fraud control and risk management strategies. It is essential for these to be in place prior to the introduction of electronic commerce on a wide scale in order to avoid fraud risks before they arise.

ES-35 The use of web site certification and endorsement services could provide an effective means of improving levels of trust in electronic commerce throughout the region. Services such as WebTrust could be implemented much more extensively throughout the region, and CAPA could have role to play in achieving this.

ES-36 Much remains to be done in the area of education of the users of electronic commerce—be they consumers, businesses or public sector agencies—as the most effective response to Internet fraud is to be fully informed of the risks and knowledgeable about how to avoid them. Abundant sources of information exist in the realm of consumer Internet commerce, although few in-roads have been made into business and government arenas of electronic commerce.

ES-37 There is also an established and continually expanding industry that provides electronic security measures associated with electronic commerce. Some products are clearly better suited to the risks of Internet fraud than others and the challenge lies in choosing appropriate measures tailored to suit individual needs. CAPA could assist by certifying products proved to be reliable. The nature of this market is such, however, that there are likely to be numerous equally effective solutions to the problems associated with electronic commerce. It remains to be seen which will capture the global market of the future. In the short-term, businesses and government agencies need to be made aware of products that are inappropriate, unreliable, overly expensive, or unsuited to their needs. CAPA could assist in providing information of this nature.

Conclusions

ES-38 The continuing expansion of electronic commerce in business and government will create many new opportunities for those intent on gaining a financial advantage improperly by deception. Although the motivations and rationalisations for acting illegally will remain much the same, the rapid introduction of new business models may create risks of fraud that can be utilised by individuals with the appropriate levels of expertise. Failing to maintain appropriate guardianship of the Internet may also make fraud easier to commit and more difficult to detect.

ES-39 The challenge facing those who would seek to minimise Internet fraud is to seek a balance which would allow a tolerable degree of illegality in return for creative exploitation of the technology. Even at this early stage in the development of electronic commerce, it may be useful for individuals, interest groups and governments to articulate their preferences and let these serve as signals to the market. Markets may then be able to provide appropriate responses which governments are unwilling or unable to achieve. Internet fraud is bound to increase as the new century unfolds. By

making effective use of traditional crime control measures coupled with some sophisticated technological solutions, it may, however, be able to be kept within manageable limits.

Suggested Initiatives

ES-40 The following measures may help both to prevent and to control Internet fraud in the future, as well as to facilitate the ongoing monitoring of the nature and scope of the problem. Some of these initiatives could be introduced with little difficulty and expense, while others may require substantial resources to be expended. As many of the issues are common throughout the region, it would be appropriate for uniform measures to be taken with respect to each of the following matters.

Guidelines

ES-41 Countries within the region should aim to establish guidelines, similar to the OECD's best practice recommendations with respect to business-to-consumer electronic commerce, for business and government electronic transactions. In this regard, CAPA could play an important role by promulgating a set of guidelines designed to minimise victimisation in business and government contexts. Appended to this report are draft *Guidelines on Fraud Minimisation for Organisations Engaged in Electronic Commerce* which could be used as the basis for assisting businesses and government agencies in preventing and controlling Internet fraud in the region.

Law and Policy Stocktake

ES-42 A stocktake could be undertaken of the specific policies and laws throughout the region that seek to address the problem of Internet fraud in business and government contexts. Any gaps in policy and legal frameworks could then be identified and appropriate uniform solutions adopted.

Police Incident Database

ES-43 Uniform practices should be implemented within national law enforcement and regulatory agencies to identify and to record all cases involving Internet fraud. A database could then be created that would permit a regional assessment to be undertaken of the precise extent of the problem, and how agencies and courts have responded.

Sentencing Database

ES-44 Justice departments throughout the region should establish a sentencing database of Internet fraud cases in order to assist judicial decision-makers in arriving at consistent decisions and to publicise cases that have been successfully prosecuted. This would help to enhance general deterrent effects of the judicial process throughout the region.

Regional Internet Fraud Desk

ES-45 A confidential electronic database could be created throughout the region in which individuals could report cases of business and government Internet fraud to the police. A Regional Internet Fraud Desk could be used as a vehicle to collect and to collate reports and to share information between law enforcement bodies. Certain unrestricted information from the database could be provided publicly to publicise new areas of risk.

Certification Services Stocktake

ES-46 A stocktake could be undertaken of existing certification and authorisation services available throughout the region that provide information on the trustworthiness of businesses and agencies that engage in electronic commerce.

Skilled Professionals Register

ES-47 A register could be created listing individuals and organisations with appropriate qualifications and expertise in dealing with Internet fraud. Included could be forensic accountants, lawyers, investigators, prosecutors, policy officers, and those skilled in fraud prevention activities.

Resource Assessment

ES-48 On the basis of the information gathered using the above techniques, an assessment could then be made of the level of resources required by agencies to deal with Internet fraud.

Legal and Law Enforcement Partnerships

ES-49 Because of the borderless nature of the Internet, partnerships should be created and extended throughout the region and with other nations to encourage the enactment of uniform laws that adequately address Internet fraud and to provide mutual assistance in the conduct of investigations.

Educational Programs

ES-50 Efforts could also be taken to educate those involved in using the technologies of electronic commerce as to their ethical and legal obligations designed to prevent dishonest and fraudulent activities from taking place. Such educational initiatives could be provided in schools and tertiary educational institutions, as well as by business and professional bodies such as CAPA.

1 Introduction

1.1 Defining Internet Fraud

For the purposes of this study, Internet-related fraud will be taken to mean any act of dishonesty or deception carried out through the use of the Internet, or directed at the technologies that support the Internet. This, of course, could include a range of activities not immediately recognisable as Internet fraud, such as the misappropriation of funds from accounts in which critical access information is obtained from electronic mail (email) or the Internet or the theft of sensitive information from electronic databases created using online sources. Generally, the present study will examine the problem in its broadest conception, including all acts of dishonesty that have some connection to Internet-based technologies.

Although consumer-related Internet fraud is of concern in the region, the present research looks at the problem in business and government sectors (so-called business-to-business and government-to-business activities). Business-to-consumer and person-to-person transactions are generally excluded, although they clearly have some degree of relevance to business and government activities as well. Throughout this report, the expressions B2B, B2G, B2C and P2P will generally be avoided as their definition and scope is often unclear and their use can be confusing. Addressing so-called B2G issues should include not only communications sent from business entities to government agencies, but also communications sent from government agencies to businesses (which sometimes raise problems distinct from the former category of communications). In addition, describing businesses as the source of communications also neglects the distinction between corporate entities, registered unincorporated associations, partnerships and other business models.

A related definitional problem, of course, concerns the legal entity responsible for the conduct in question. To date, most investigations of Internet-related crime have focused upon individual human perpetrators. The future may, however, see an expanding role for corporate criminal responsibility, particularly where intellectual property infringements have taken place or where corporate espionage has been engaged in electronically.

A wide range of conduct is included within the scope of Internet fraud. Examples are sending misleading and deceptive information to a business or government agency, manipulating electronic payment systems, misappropriating corporate information and intellectual property from the Internet, identity-related deception when using the Internet, failing to honour commercial obligations entered into on the Internet, and using misleading domain names with intent to defraud. Also included are acts of dishonesty that make use of online business communications, business and government bulletin boards, electronic mail and the World Wide Web.

As such, there is a close relationship between Internet fraud and fraud relating to electronic commerce activities of business and government organisations. Electronic commerce—or using computing and communications technologies to trade in goods and services—makes use of a range of technologies. These include electronic mail, facsimile transfers, and a variety of web-based systems for the sharing and exchange of information. Acts of dishonesty, deception and misrepresentation relating to any of these technologies are included within the scope of the present study. For convenience, these various aspects of fraud that involve electronic commerce shall collectively be referred to as Internet fraud.

1.2 The Mechanics of Internet Fraud

Internet fraud can occur by offenders transmitting misleading and deceptive information online, by failing to honour contractual agreements entered into electronically, or through the misappropriation of funds transmitted electronically. Theft of funds does not, however, involve stealing ‘digital bags of money’ as they pass along telephone wires, but simply entails the manipulation of instructions provided by users to debit or credit specified accounts (see Grabosky, Smith and Dempsey 2001, chapter 2). Fraud prevention simply requires that the instructions given by the parties to a transaction, be they consumers, merchants or financial institutions, cannot be tampered with.

Various payment systems have been developed for use in connection with Internet transactions. Some make use of telephone accounts that allow vendors to obtain access to purchasers’ funds, while others make use 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. Newer forms of stored-value cards (usually involving computer chip technology) have been

designed to record monetary value, may also be used to transfer funds from a bank's ATM to a personal computer and thence to a business. These systems are obviously more efficient since transactions may be carried out and paid for instantaneously.

Goods and services purchased online may be paid for using a variety of payment systems. The simplest mechanism involves payment by cash or money order once an agreement has been reached electronically. In addition to paper-based transactions, online 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.

Internet fraud has been greatly facilitated by offenders obtaining credit card account numbers from online services, such as Credit Master and Credit Wizard, that generate large volumes of credit card numbers which can then be used to pay for goods or services ordered online. The sole purpose of these credit-card generator programs is to aid in finding particular credit card numbers that the program's user is not authorised to use but that online merchants will, nonetheless, accept. By generating a large enough group of card numbers that merchants will accept, participants in an online fraud scheme can make substantial fraudulent purchases of goods or services, or cause fraudulent billings for nonexistent goods or services, at the expense of the credit card company or the customers to whom the valid credit card numbers have been assigned (United States, Department of Justice 1999).

Alternatively, credit card account numbers and other personal information can be misappropriated from databases maintained by organisations in both the public and private sectors. Some recent cases have involved the removal of tens of thousands of credit card details from commercial enterprises. In the largest known case, a hacker stole 485,000 credit card numbers from an electronic commerce web site and secretly stored the information on an American government agency's web site (*The Australian*, 21 March 2000). In another case, Creditcards.com was hacked, and 55,000 card numbers were retained until the offender received a payment of US$100,000 which he

claimed from the victim company. When the extortion attempt failed, the hacker posted the card numbers on the Internet. The company has since created a web site at which merchants and customers can check for fraudulent transactions (Berinato 2000).

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. 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 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 can be authenticated and that merchants can 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 cardholder permitting funds to be transferred from the credit card account to the merchant’s account. The SET Protocol has undergone various revisions in recent years and its latest form, known as the 3-D Secure Protocol, is being implemented globally, including, in 2001, in the Asia-Pacific region (Visa International 2001).

Others are considering the use of smart cards with the capacity to store value and transfer this to merchants via the Internet. Smart card payment 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 cardholder 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 that accept their cards.

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. In these systems before purchases can be made, both the merchant and the customer need to establish banking arrangements and Internet links with the bank issuing the tokens. The customer first requests a transfer of funds from his or her bank account into the electronic systems. This is similar to withdrawing cash from an ATM. The system then generates and validates 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 electronic cash to any merchant who will accept this form of payment using the software provided by the 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 the electronic cash into real funds by presenting the electronic cash to the issuing bank with a request for an equivalent amount of real funds to be credited to the merchant's bank account.

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 or PIN. 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 untraceable.

1.3 Sources of Information

The present report is in the nature of a scoping study of the issues that arise in controlling fraud associated with Internet usage and electronic commerce in business and government contexts in the Asia-Pacific region. Information has been collected from a range of sources including currently available legal, technological, and commerce-based prevention and control strategies. Some specific surveys of the fraud risks associated with electronic commerce, such as that conducted by KPMG (2001) were also relied upon. In addition, searches were conducted of newspaper reports of fraud incidents, relevant legislation and judicial decisions, and other policy documents. The Internet itself was also used to obtain recent information regarding developments in electronic commerce usage and technological fraud prevention solutions in the Asia-Pacific region.

Although contact was made by electronic mail with a number of stakeholders in the region, including members of CAPA, it was impossible to obtain much information by direct approaches being made to individuals in the public and private sectors. As such, the present scoping study relies primarily upon documentary sources of information and the results of previously published surveys. Of greatest value were published government, business and academic books, reports and professional journal articles from the region.

Some caution needs to be exercised when relying on some of the materials obtained from online sources, particularly media reports, as the accuracy of data and other information are often unable to be verified from independent sources. In addition, the present study relied solely upon English-language sources which, of course, reduced the depth of information used.

Finally, care is needed in interpreting some of the published survey results as many involved consumer fraud-related incidents rather than crimes arising out of business and government online transactions which have only recently become of interest. Although the present study seeks to focus upon business and government transactions, these are generally still in their

infancy in most countries in the region, and, accordingly, few instances of fraud have emerged to date. The nature of the risks can, however, be described, and the likely impact of Internet fraud for the region in the future can be predicted.

1.4 Aims of the Study

The aims of the study are:

- to describe the nature and extent of Internet-related fraud as it affects business and government electronic commerce in the Asia-Pacific region (being restricted to countries that are currently members of CAPA);
- to assess the likely future trends of this type of fraud;
- to evaluate business and law enforcement strategies aimed at preventing this type of fraud; and
- to assess the extent to which current legal and business responses are adequate to deal with the problem in the region.

This report reviews existing information on the nature and incidence of the problem, and examines both existing mechanisms being used to address it and strategies likely to be effective in controlling Internet-related fraud in the future. The findings should enable members of CAPA in individual nations throughout the region to design appropriate responses to prevent and to deal with the problem and will support the goal of harmonisation of laws and business approaches throughout the region. The report should also provide an indication of the likely course which Internet-related fraud will take in the immediate future in the Asia-Pacific region.

2 Technological Infrastructure

2.1 Introduction

As with most forms of crime, as opportunities for illegal conduct arise, so the number of crimes perpetrated increases. In the case of Internet-related crime, the opportunities created by the greatly expanding use of the Internet are substantial. Opportunities for Internet fraud increase with the number of participants engaged in electronic commerce. Moreover, increased distribution of transactions across jurisdictions, networks and Internet sites reduces the potential for systematic fraud prevention and response measures.

In the Asia-Pacific region, information technology industries are developing rapidly and although individual countries have varying policies on access to and use of technologies such as the Internet, use of the Internet is expanding quickly. Recent research predicts that by 2003, the Asia-Pacific region will have more Internet users than either the United States or Western Europe (Dataquest 2001; see also IDC 1999).

In India, for example, substantial investments have been made in information technologies which have been estimated at the equivalent of US$2.2 billion, much of it in the software industry and training sector. Approximately 0.7 to 0.8 per cent of GDP is invested in information technology (Amarnathan 2000, pp. 66–7). Since 1998, many licences have been issued to private Internet service providers (ISPs) in India but, despite these efforts, 75 per cent of the country's connections are made through cybercafés with the expansion of the Internet being blocked by the poor condition of the country's telecommunications infrastructure (Reporters Sans Frontières 2001).

There are few Internet users in Sri Lanka, and the Internet hardly exists in rural areas. About a hundred cybercafés have opened in the larger cities, where Internet users give preference to email, especially for communicating with the large expatriate community (Reporters Sans Frontières 2001).

In Pakistan, in November 2000, the government claimed to have spent the equivalent of more than 90 million Euros on Internet infrastructure which

was said to have reduced the cost of connecting to the Internet by 55 per cent. Three hundred cities and towns are already connected. In July 2000, the daily newspaper *Dawn* revealed that the Pakistan Telecommunication Corporation Limited (PTCL), a public company with a monopoly on service, was setting up two Internet connection nodes (National Access Points) that ISPs were required to use. As a result, this public company would be able to permanently block access to pornographic sites and telephone calls made through the Internet (Reporters Sans Frontières 2001). The Government's Information Technology policy aims to provide nearly 100 cities in Pakistan with Internet access by 2002 (BBC Online Network 2000).

As in other Asian countries, much of the interest in the Internet in Bangladesh has been driven by middle class youth, particularly students (Nando Times 1997).

In China, at 30 June 2001, the government agency, China Internet Network Information Centre, estimated that there were 26.5 million regular users of the Internet, which represented an increase of almost 10 million over the preceding year. In 1995, there were only 15,000 Internet users, making the increase since then dramatic. Despite this increase in usage, the government maintains strict control on content; some 2,000 illegal Internet cafés were closed in 2001 after the government examined more than 58,000 Internet cafés. China also blocks various foreign and domestic web sites that are considered to be contrary to the interests of the government, including the *New York Times Online* (Schauble 2001).

In Malaysia, the general public began using the Internet in 1996, through an offer from Telekom Malaysia (TMB), the governmental telecommunications company that still remains the market leader. Until recently, this market was open only to Malaysian ISPs, but has recently opened to foreigners, with the Japanese company NTT offering Internet access. All providers must, however, obtain a licence from the Communication and Multimedia Commission (Reporters Sans Frontières 2001). It has been noted that many Malaysian Internet users use more than one ISP, making the compilation of accurate usage statistics difficult (IDC 2001).

The consolidation of 55 financial institutions in Malaysia into 10 anchor banking groups is proceeding prior to the deregulation of the banking sector in 2007. Local banks are seeking to interface their post-merger systems into the Malaysian Electronic Payment System (MEPS) which supports a SET payment gateway, an E-purse smart card, a multi-function payment card

and an inter-bank giro. By contrast, foreign banks were the first to establish online services as early as 1992 and 1993, while Malaysian banks only started to move online in 2000, following approval by Bank Negara in January 2000 (*New Straits Times*, 22 May 2001).

Only three of the 10 anchor banks, Malayan Banking, Southern Bank and Hong Leong Bank, offer online services, but Bumiputra-Commerce Bank and Affin Bank are preparing to go online. Bank Negara has issued guidelines whereby banks have to establish informational web sites before transaction-enabling these sites. From 1 June 2000, local banks could establish transactional web sites, whereas locally incorporated foreign banks could set up communicative web sites from 1 January 2001, but cannot transaction-enable these sites until 1 January 2002, and must link to Bank Negara's site.

In mid-2000, it was estimated that some eight per cent of the Philippine adult population was online (CyberAtlas 2000). According to one report, the Catholic Church was active in providing Internet connections to provincial areas through the church-run ISP, CBCPNet (Silicon Valley News 2001).

The Korean information technology market is also large and has been estimated to be worth US$194 billion a year. The Korean Software Industry Association estimates that more than a third of Korean homes have broadband access (Sinclair 2001). In South Korea, the Internet is experiencing a period of spectacular growth with the number of users increasing from three million to sixteen million in less than two years. The 2001 figure has been estimated at 22.3 million, making the Korean Internet market the world's fourth largest, behind the United States, Japan and Germany (Nielsen NetRatings 2001). Thirty-five per cent of South Korean Internet users buy online at least once every three months (Yankee Group 2001). Nearly nine per cent of the population has traded shares online (Korea Times 2001). The government has also created 'Cyber Korea 21', an investment plan of the equivalent of more than nine billion Euros, to increase connectivity and to improve infrastructure (Reporters Sans Frontières 2001).

In Thailand, Internet access is free. This has led to the rapid development of hosts, but has meant that the government controls ISPs. The telecommunications industry is regulated by the Telephone Organisation of Thailand and the Communication Authority of Thailand, and Thai law specifies that the Communication Authority of Thailand must hold at least 32 per cent of the capital of each of the country's ISPs, all of which are

private. As part of the country's deregulation of the telecommunications sector, the obligation to sell company shares to the Communication Authority of Thailand is scheduled to be eliminated in 2001 and a new regulating agency, the National Commission of Communications, could be created (Reporters Sans Frontières 2001).

2.2 Telecommunications Carriers

There is considerable diversity in the extent to which populations in the Asia-Pacific region are serviced by telecommunications providers. For example, the World Bank estimated that in 1999 Australia had around 520 telephone mainlines per 1,000 inhabitants, while Bangladesh had three per 1,000 people (World Bank 2001). Also at the higher end of telecommunications provision were Canada (655), Hong Kong (576), Japan (558), New Zealand (496), Korea (438) and Malaysia (203); while less well-serviced were Thailand (86), Philippines (39), Mongolia (39), Sri Lanka (36), India (27), Pakistan (22), Nepal (11) and China (7).

However, the Internet is increasingly being linked to wireless access, particularly in the Asia-Pacific region, through the use of mobile telephone networks and emerging wireless technologies (CNN Interactive 2001). Wireless Internet transmission using desktop computers, solar panels and satellite dishes has been promoted in countries such as Cambodia and Indonesia, where many inhabitants are far removed from telephone lines and electrical grids (Chandrasekaran 2001; Arnold 2001).

In India, it has recently been observed that parts of the under-developed countryside now have more mobile phones per 100 people than do some of the larger cities (Rai 2001). This is critical for the development of electronic commerce, as approximately half of India's villages lack fixed-line telephone services, and those that are connected have outdated equipment and long waiting lists for service. Recently, problems of poor infrastructure have been met by the development of battery operated handheld computers that even translate messages into local languages and read the messages aloud to users. The 'Simputer', as it is known, should sell for around US$200 and become available in 2002. The Simputer, and its text-to-speech software, Encore, was developed by engineers at the Indian Institute of Sciences in Bangalore and is expected to overcome the problem of illiteracy in retarding computer usage in India (Millar 2001).

2.3 Internet Service Providers

Countries within the Asia-Pacific region vary considerably in terms of ownership and control of ISPs. In some cases, owner/operators are private companies, while in others (particularly where national telecommunications carriers have a monopoly over Internet service delivery), public ownership is the norm. The variation can be observed in the country extracts on the Reporters Sans Frontières web site.

A significant indicator of Internet penetration is the number of ISPs in each country, along with numbers of Internet hosts and individual users (Table 1).

Table 1: Internet usage by country

	Number of ISPs		Number of hosts (1,000s)		Hosts per 10,000 population		Number of users (1,000s)		Users per 10,000 population	
	1999	2000	1999	2000	1999	2000	1999	2000	1999	2000
Australia	709		1,090	1,615	576.63	843.52	6,000	6,700	3,172	3,497
Bangladesh	6		0.001	3.5	N/A	0.25	30.0	50.0	2.36	3.94
Canada	750		1,669	2,364	547.59	768.78	11,000	12,700	3,607	4,130
China	3	200	71	70	0.57	0.55	8,900	22,500	70.25	176.06
Fiji	2		359	555	4.45	6.82	7.5	N/A	93.02	N/A
Hong Kong	49		114	228	166.89	336.90	1,734	2,283	2,519	3,358
India	3	>80	23	35	0.23	0.35	2.0	5.0	20.04	49.39
Japan	357		2,636	4,640	208.41	365.66	18,300	47,080	1,446	3,709
Korea	11	80	283	397	60.99	84.10	6,823	19,040	1,467	4,025
Malaysia	11	5	59	68	27.03	29.34	1,500	3,500	687.13	1,504
Mongolia	N/A		0.050	0.171	0.19	0.64	3.0	30	11.45	112.70
Nepal	N/A		0.29	1.1	0.12	0.48	35.0	50	14.97	21.70
New Zealand	56		271	345	707.86	900.87	700	830	1,828	2,166
Pakistan	26	50	4.7	6.4	0.35	0.46	80.0	N/A	5.95	N/A
Philippines	93		12.3	19.4	1.66	2.54	500	2,000	67.16	261.44
Samoa	N/A		0.007	2,513	0.40	139.5	0.5	N/A	28.22	N/A
Solomon Islands	N/A		210	364	4.88	8.14	3.0	2.0	69.72	44.70
Sri Lanka	4	10	1.2	2.1	0.65	1.14	65.0	121.5	34.87	64.21
Thailand	13	17	40.1	63.4	6.60	10.47	800	1,200	131.46	197.96

Sources: CIA 2000 (1999 ISP figures), Reporters Sans Frontières 2001 (2000 ISP figures), ITU 2001 (other figures).

These statistics indicate that in some countries, Internet usage has more than doubled in the year from 1999 to 2000. It can be expected that 2001 figures for individual countries will in some cases show a similar increase. For example, a study conducted by Bangkok University indicates that the number of Internet users in Thailand will reach 4.6 million during 2001 (CyberAtlas 2001c). It should be noted, however, that estimates and predictions of Internet usage over recent years have diverged considerably among leading sources such as ACNielsen (2001), CyberAtlas (2001a), NUA (2001) and ITU (2001).

As might be expected, Internet usage largely follows the pattern of personal computer ownership and usage within populations (Table 2).

Table 2: Personal computer use by country

	Number of PCs (1,000s)		PCs per 100 population	
	1999	2000	1999	2000
Australia	8,900	8,900	47.06	46.46
Bangladesh	130	N/A	0.10	N/A
Canada	11,000	12,000	36.08	39.02
China	15,500	20,600	1.22	1.61
Fiji	40	N/A	4.96	N/A
Hong Kong	2,000	2,360	29.05	34.72
India	3,300	4,600	0.33	0.45
Japan	36,300	40,000	28.69	31.52
Korea	8,500	9,000	18.29	19.03
Malaysia	1,500	2,440	6.87	10.49
Mongolia	17	24	0.65	0.92
Nepal	60	N/A	0.26	N/A
New Zealand	1,250	1,380	32.65	36.02
Pakistan	580	N/A	0.43	N/A
Philippines	1,260	1,480	1.69	1.93
Samoa	1	N/A	0.56	N/A
Solomon Islands	18	N/A	4.18	N/A
Sri Lanka	105	N/A	0.56	N/A
Thailand	1,382	1,471	2.27	2.43

Source: ITU (2001)

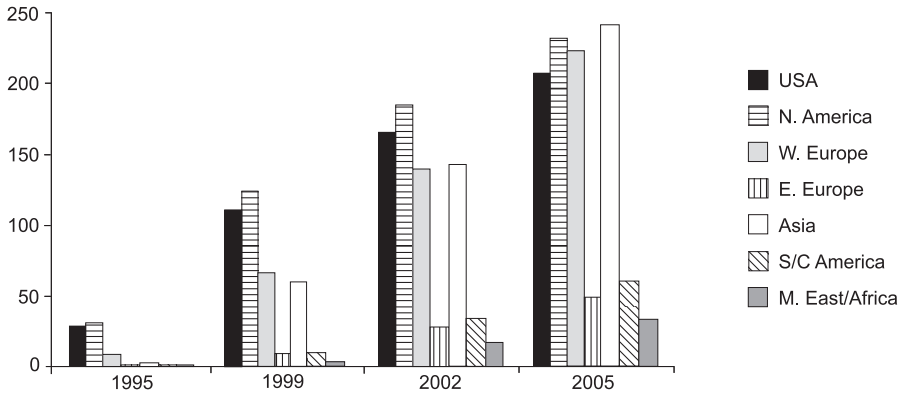
2.4 Internet/World Wide Web Traffic

While Internet development was largely based in the United States in the 1980s and early 1990s, the phenomenon is now truly global. The market research and consultancy service eTForecasts predicts that there will be over 1 billion Internet users in the world by the year 2005. Of six regions considered alongside the United States, it is predicted that the Asia-Pacific region will become the largest Internet usage region with 242 million Internet users in 2005 (Figure 1).

According to eTForecasts, Asia will see especially strong growth. Japan has until now followed the United States in terms of Internet usage in recent years, but it is forecast that China will become second to the United States in number of Internet users by 2005 (Table 3).

Similar trends are evident in the numbers of computers in use in different countries (Figure 2). From 2003, it is forecast that the Asia-Pacific region will have more computers in use than North America.

Figure 1: Internet use by region 1995–2005



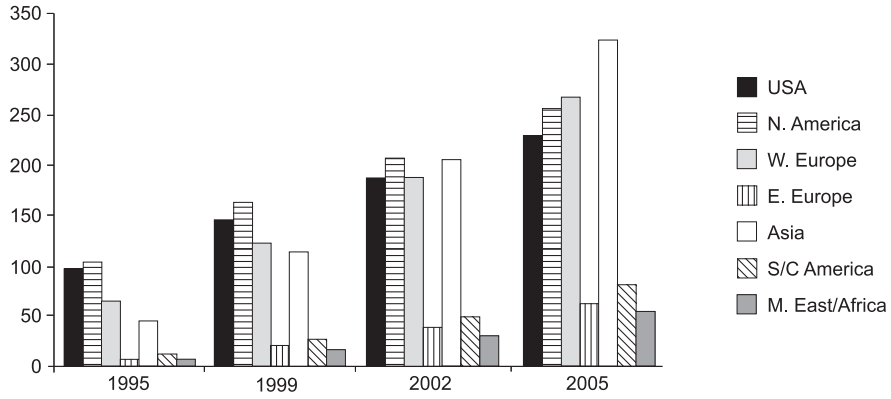
Source: eTForecasts (2001a)

Table 3: Top 15 countries' Internet users

Internet users (#M)	Year-end 2000	Share %
1. United States	135.7	36.2
2. Japan	26.9	7.18
3. Germany	19.1	5.10
4. United Kingdom	17.9	4.77
5. China	15.8	4.20
6. Canada	15.2	4.05
7. South Korea	13.8	3.68
8. Italy	11.6	3.08
9. Brazil	10.6	2.84
10. France	9.0	2.39
11. Australia	8.1	2.16
12. Russia	6.6	1.77
13. Taiwan	6.5	1.73

Source: eTForecasts (2001a)

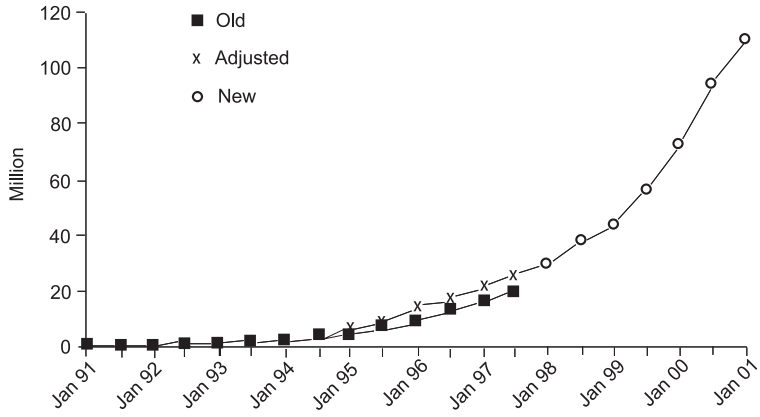
Figure 2: Computer use by region 1995–2005



Source: eTForecasts (2001b)

Another way of measuring the expansion of Internet activity is by reference to the number of individual Internet hosts identifiable by domain name. The Internet Survey Consortium has been running an Internet Domain Survey twice a year since 1987 (Figure 3).

Figure 3: Internet software consortium host count graph 1991–2001



Source: Internet Software Consortium 2001 (http://www.isc.org/)

This survey is a combination of two slightly different techniques. The pre-1998 (old) survey counted the number of domain names on the Internet that had IP addresses assigned to them. From 1998 onwards, the (new) survey counts the number of IP addresses that have been assigned a domain name. Notwithstanding this slight shift in methodology, the ISC survey clearly indicates a rapid expansion in the number of Internet hosts, with the figure for January 2001 standing at 109,574,429 (ISC 2001).

In Australia, Internet usage surveys carried out by the Australian Bureau of Statistics (1998, 1999, 2000), have found an increase of 52 per cent in the number of adults who had gained access to the Internet between November 1998 and May 2000—4.2 million adults (31 per cent of the adult population) to 6.4 million adults (46 per cent of the adult population).

The surveys also found a 180 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 May 2000—(286,000 or 2.6 per cent of adults in the 12 months to November 1998 to 802,000 adults (six per cent of Australian adults) in the 12 months to May 2000 (a 2.4 per cent increase in the percentage of the adult population). The percentage of Internet shoppers

who paid for goods and services by disclosing their credit card details online stayed much the same, increasing by only 0.5 per cent—from 80.5 per cent in November 1998 to 81 per cent in May 2000.

Books / magazines and computer software / equipment were the most common (27 per cent and 19 per cent respectively) types of goods or services purchased from the Internet for private use in the 12 months to November 1999 by adults in Australia. The potential exists, however, for anything to be purchased electronically and over the last year a number of higher-value transactions have been conducted electronically with purchasers buying holidays, cars and even houses online. We have also seen the establishment of a number of online auction houses and the use of the Internet for online share trading and gambling, each of which entail larger sums of money.

In China, a survey conducted by Iamasia found that five per cent of Internet users had made an online purchase in the preceding 12 months, while 15 per cent of users in Hong Kong had purchased from the Internet (Legard 2000).

Another survey of Internet users in Hong Kong conducted by ACNielsen found that the number of online consumers more than doubled from 50,000 to 110,000 during the 12 months preceding March 1999. The survey sampled 2,000 people in Hong Kong between the ages of 15 and 54. On average, online shoppers spent HK$700 online with 33 per cent spending less than HK$250, and 21 per cent spending more than HK$1,000 on their most recent purchase. Local electronic commerce in Hong Kong was thus estimated to be worth HK$76 million in 1999. One online shop developed by the local store Wing On received more than 10,000 hits per week. In 1998, 22 per cent of Internet users expressed concern that their personal information could be obtained illegally from the Internet while in 1999, 43 per cent of users expressed similar concerns (Lemon 1999).

2.5 Email Usage

Possibly the most socially revolutionary aspect of the development of the World Wide Web has been the phenomenal growth of email as a medium of personal and business communication. With it have come new opportunities for fraud, as well as avenues for other forms of cybercrime, such as malicious spamming, hacking, the spread of computer viruses, cyberstalking, cyberlibel and so on (Grabosky and Smith 1998).

Many of those who use the Internet, particularly in countries where web site content is strictly controlled, do so principally to send and receive email. In China, for example, email is the main reason why people use the Internet, although one recent survey has found a decline in email usage (Schauble 2001).

Given the efficiency of email as a means of mass communication, it is perhaps not surprising that fraudsters have seen its potential for misuse. Notable examples of email misuse for financial gain include the practice of sending out thousands or even millions of unsolicited email messages suggesting that identified shares will rapidly rise (or fall) in value, thus manipulating the stock price (see below).

2.6 Intranets/Virtual Private Networks

Throughout the region, both businesses and government agencies make considerable use of intranets and virtual private networks. These provide a secure and efficient means of communication between employees of large organisations as well as restricted groups of users who have been included in the network. Where fraud occurs in connection with an intranet, it is clearly easier to locate the offender than where a wide area network is involved. This is because the potential pool of offenders is somewhat limited (unless an act of hacking by an outsider has occurred).

India, in 2000, had approximately 30 large networks such as the large government networks ERNET, NICNET, RABMN, 1-NET, SIRNET, HV-NWET, BANK-NET, and various dedicated networks in other public and private sector domains. A number of private networks have also been established, mainly using 'sat.com'. Internet gateway access is provided only by the government-owned VSNL (Videsh Sanchar Nigam Ltd) although other ISPs are being established in India (Amarnathan 2000, p. 69).

2.7 Internet Kiosks

Internet kiosks / cafés are becoming an increasingly common feature of urban environments, particularly in many Asian countries where home and business personal computers are less prevalent than in more developed countries (Asia Internet Report 2001):

> *For travellers in Asia, Internet cafés serve as lifelines to family and friends. Access to information on flights, hotels and special attractions*

> *empower both business travellers and backpackers, giving them information and guidance that only fine hotels could provide just a few years ago.*

A new Tokyo Internet café operated by Yahoo! is described as follows (Japan Internet Report 2001):

> *It's a two-storey place with five sections: two with computers and two without, plus a stand-alone Starbucks from which you can order drinks and snacks that can be enjoyed anywhere in the facility. No charge for computer use, though users must register and pay if they damage the equipment.*
>
> *All of the machines have flat displays, and many are laptops with wireless LAN connections, making for a spacious feel and the ability to move about … The 30 PCs available boast connection speeds up to 100Mbps, no doubt making for some fiery surfing.*

In China, one of the world's largest Internet cafés, Fei Yu (literally 'fly in the universe') that covers a large part of the block opposite the main entrance to Beida University, was raided by more than a hundred police officers in December 2000. Fifty computers whose users had visited pornographic web sites were seized and their owner was fined 30,000 Yuan (approximately 3,800 Euros). On 16 March 2000, Beijing city hall announced a directive authorising the closing of cybercafés which did not verify the sites visited by their customers. In Shanghai, in June 1999 and February 2000, the government closed 420 unlicensed cybercafés (Reporters Sans Frontières 2001). More recently, some 2,000 Internet cafes were closed by the Chinese government following a sweep of more than 58,000 establishments (Schauble 2001).

2.8 Electronic Funds Transfers

Although only indirectly relevant to Internet fraud, the provision of means to transfer funds electronically between customers and financial institutions creates considerable opportunities for crime. Electronic funds transfers take place in a wide range of contexts that extend from personal online home banking, through to international funds transfers using wholesale banking facilities such as SWIFT. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a Belgian cooperative that connects over 5,000 financial institutions in over 80 countries. All SWIFT messages are

passed first to a regional 'condenser' and then by satellite to the central 'switch' in Brussels where they are stored (if required) and re-routed to their destination. They are received again by a regional centre and then forwarded to the destination bank. Messages must contain prescribed information and be in a prescribed format.

As an example of the extent of various types of payment transactions, Tables 4 and 5 illustrate the different methods of payment that are available in Australia and the changes that have occurred in the number of transactions using each since 1994. Electronic forms of payment are increasing and displacing cheques which were virtually the only form of non-cash payment in the early 1980s. Though there are still considerably more cheque transactions than other forms, and more money is transacted by cheque. Together, debit and credit cards are now more often used than cheques in Australia (Reserve Bank of Australia 2000).

Table 4: Number of payment transactions, Australia, 1994–2000

	1994	1995	1996	1997	1998	1999	2000
Cheques*	3.7	3.9	3.9	3.7	3.7	3.2	3.1
Direct entry credits*	1.6	1.9	1.7	1.8	1.9	2.1	2.3
Direct entry debits*	0.3	0.4	0.4	0.4	0.6	0.8	0.9
ATM withdrawals**	40.7	38.8	41.6	39.2	42.9	41.9	48.4
EFTPOS**	20.7	29.1	35.5	39.2	44.5	48.6	52.0
Credit cards**	19.9	22.6	24.6	25.9	32.8	42.9	57.7

* millions of items per day

** millions of items per month

Source: Reserve Bank of Australia (2000)

Table 5: Value of payment transactions, Australia, 1994–2000

	1994	1995	1996	1997	1998	1999	2000
Cheques*	24.8	23. 4	24.3	24.9	14.6	12.3	13.9
Direct entry credits*	1.9	2.6	4.2	3.4	3.6	5.3	7.1
Direct entry debits*	1.3	1.2	1.6	1.6	2.4	4.0	3.9
ATM withdrawals**	4.4	4.9	5.6	5.4	6.2	6.8	7.3
EFTPOS**	1.1	1.5	1.9	2.1	2.4	2.8	3.1
Credit cards**	1.8	2.0	2.3	2.5	3.6	4.3	6.4

* A$ billions per day

** A$ billions per month

Source: Reserve Bank of Australia (2000)

Although other payment mechanisms are becoming more prevalent, cash is still the most widely used form of payment in retail settings. According to the Reserve Bank of Australia, its use 'appears to be just as widespread in the late 1990s as it was in the 1980s' (Reserve Bank of Australia 2000, p. 11).

Electronic payment transactions that make use of PIN authentication are governed in many countries by detailed codes of conduct that specify who is liable for loss in certain circumstances, and how payment systems should be used. In terms of electronic funds transfers, the statistics complied by the Australian Securities and Investments Commission (2000) on the operation of the Electronic Funds Transfer Code of Conduct in Australia show that there has been an increase from 42 to 64 complaints made under the Code per million transactions between 1998–99 and 1999–2000. In 1999–2000 there were 106,719 complaints out of 1,655,362,481 electronic transactions. In percentage terms, this represents a very small number indeed. It seems, therefore, on the whole, that electronic funds transfer systems operate in a secure and efficient manner.

2.9 Public Key Infrastructure

A number of countries in the region are starting to make use of public key systems in connection with electronic commerce transactions in government and business contexts.

In Australia, in accordance with the Federal Government's policy on electronic commerce, *Project Gatekeeper*, digital certificates have been issued by various agencies that permit secure electronic communications to be conducted between businesses and government agencies. Digital certificates linked with encoded Australian Business Numbers (which are required for taxation purposes) are being used by the Australian Taxation Office and the Australian Securities and Investments Commission to permit lodgment of taxation returns and other company documents electronically. The Health Insurance Commission, which provides funding for publicly-funded health and medical services in Australia, has issued its own digital certificates to permit secure electronic communications between health service providers and itself over the Internet. In the private sector, two companies, Baltimore Certificates Pty Ltd and eSign, an Australian subsidiary of VeriSign, have been accredited to issue digital certificates to businesses which wish to transact business online with government agencies (Cant 2001).

3 Electronic Commerce in the Region

3.1 Electronic Commerce Activities

An indication of the extent to which organisations within the region have taken up electronic commerce is provided in KPMG's Global eFraud Survey (2001). In 2000, a survey was sent to more than 14,000 senior executives in large public and private companies in 12 countries. In the Asia-Pacific Region responses were obtained from 92 companies in Australia, 24 in Hong Kong and 33 in India. In total, 1,253 responses were received.

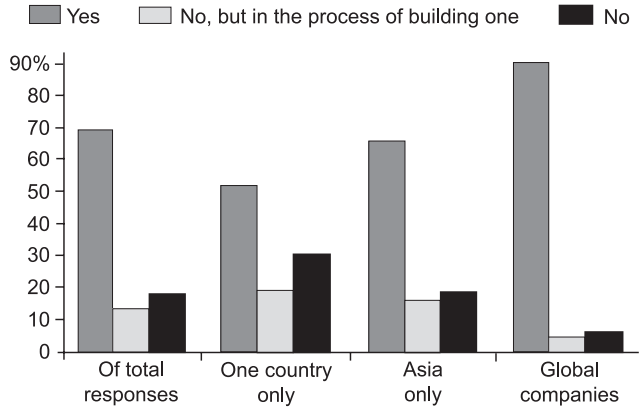
Overall, 86 per cent of respondents considered themselves somewhat to very knowledgeable about electronic commerce, although 20 per cent of respondents from Hong Kong considered themselves not very knowledgeable about electronic commerce. Some 62 per cent of respondents said that their company engaged in some form of electronic commerce with 63 per cent of these reporting having engaged in business-to-business transactions.

In another study of electronic financial transactions carried out in 2000, it was estimated that approximately 100 per cent of stockbrokers and 70 per cent of banks in the Asia-Pacific region will be converted to online transactions within three years, and that as much as 50 per cent of retail brokerage trade will be done over the Internet in the more advanced economies of Japan, Australia, Hong Kong, Singapore, South Korea and Taiwan in two years' time. It was further predicted that retail online banking will be the most profitable part of banks' businesses in countries like Japan, Australia and Singapore in less than three years, and that wireless Internet usage will take off faster in Asia than anywhere else in the world, due to the very high levels of mobile phone penetration (Bain 2000).

In November 2000, the *Far Eastern Economic Review* (FEER 2000), in association with Deloitte Consulting, conducted a survey among the Review's e-newsletter readership, with nearly 5,000 responses mostly from the Asian region.

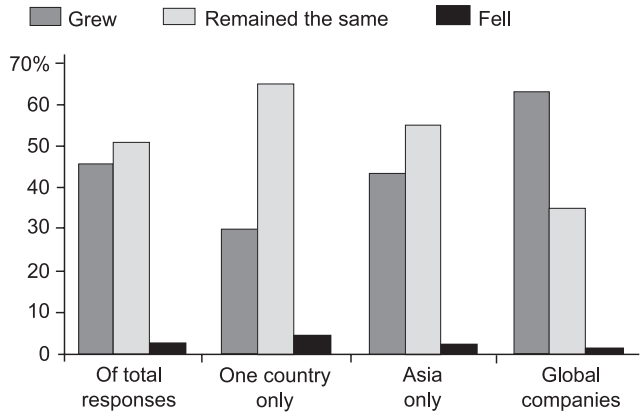
The survey produced information about the use of Internet trading by companies. The Asian region reflected the substantial growth globally of business activities conducted online (Figures 4 and 5).

Figure 4: Companies with web sites



Source: Far Eastern Economic Review/Deloitte Consulting (2000)

Figure 5: Companies' e-business development



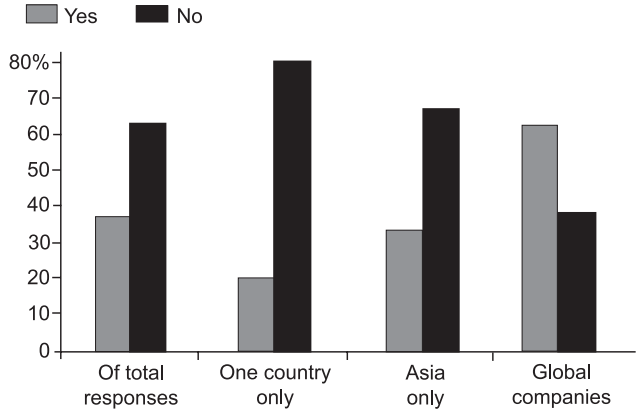
Source: Far Eastern Economic Review/Deloitte Consulting (2000)

The FEER–Deloitte survey did not further identify the types of company most likely to be trading online. However, the associated report notes (Burns 2000):

> *Small companies are often seen as more likely to use new technology to explore new markets. The reality seems to be that while the earliest pioneers are indeed mostly small firms, the vast majority of small and medium-sized businesses are not so nimble.*

One indicator of commitment to electronic commerce among larger companies is the employment of staff specifically dealing with Internet trading (Figure 6).

Figure 6: Companies with and e-business manager



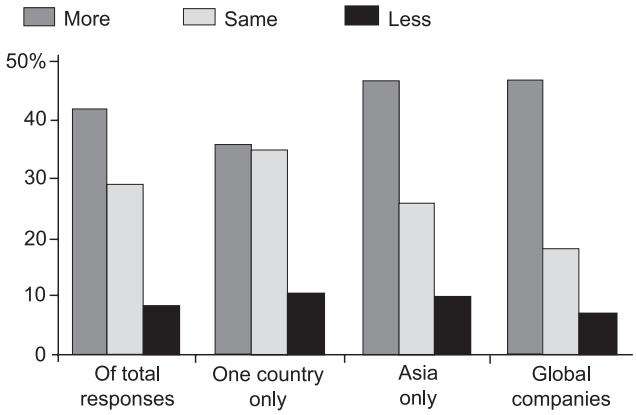
Source: Far Eastern Economic Review/Deloitte Consulting (2000)

In regard to the level of online spending by companies, the FEER-Deloitte survey revealed (Burns 2000):

> *About 20 per cent of respondents said their company didn't buy anything online last year. Of the companies that did buy online, nearly all said the total spending last year was below $100,000. This, and other data gathered, suggests that for most companies the supply chain remains off-line. Outside the United States, those that didn't buy anything over the Internet said they were particularly put off by the lack of an effective payment system.*
>
> *The results may not be revealing the whole picture, however. About half of our respondents admitted that they were out of the loop and didn't know how much their companies spent online. In addition, most said their companies' business-to-business spending was higher this year than in 1999.*

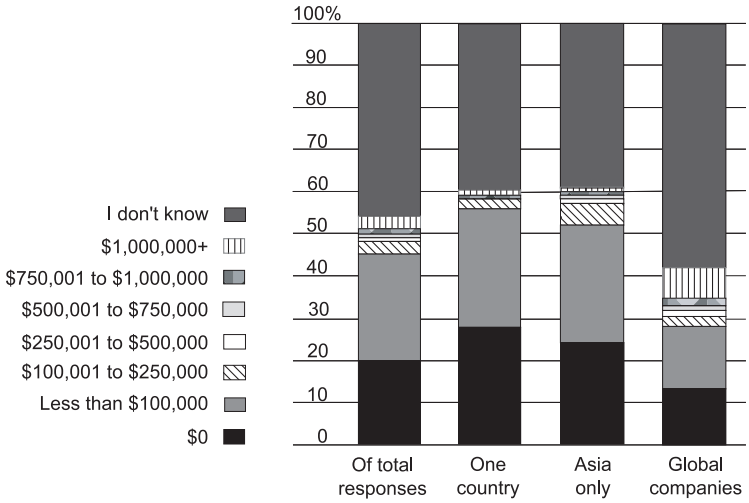
Most respondents in the Asian region reported an increase in online spending from 1999 to 2000 (Figure 7). Online purchasing by Asian companies was also comparable with global responses (Figure 8).

Figure 7: Companies' online spending levels



Source: Far Eastern Economic Review/Deloitte Consulting (2000)

Figure 8: Company online purchasing



Source: Far Eastern Economic Review/Deloitte Consulting (2000)

In regard to the type of online spending by companies, the FEER-Deloitte survey revealed (Burns 2000):

> *The most popular online business purchases were office supplies, office equipment and travel services. Some 20 to 25 per cent of companies have bought something in at least one of these categories. Big industry belies its reputation for inflexibility: 18 per cent of REVIEW readers that work for industrial companies said their firms buy raw materials online.*

Details are set out in Table 6.

Table 6: Items that companies purchase online

	Of total responses	One country only	% Asia only	Global companies
Office supplies (including stationery, beverages consumed daily)	26	21	25	23
Office equipment	25	25	22	20
Company travel-related services	21	17	18	18
Professional services	13	12	15	11
Components for manufactured products	7	6	6	8
Raw materials	5	3	5	6
Others	7	9	7	4

Source: Far Eastern Economic Review/Deloitte Consulting (2000)

Companies' reasons for online spending were described thus (Burns 2000):

> *The obvious goals of raising efficiency and cutting costs were popular, but surprisingly, not overwhelmingly so. We also found that larger companies were quite likely to have adopted online purchasing as part of a company-wide computerisation program in which they introduced automated inventory control, supply-chain management and similar systems.*

Details of businesses' reasons for online purchases are set out in Table 7.

Table 7: Businesses' reasons for online purchases

	Of total responses	One country only	% Asia only	Global companies
Higher efficiency, less paperwork and lower overhead	60	58	59	58
Lower cost	42	41	42	42
Part of automatic inventory control/ purchasing system	16	11	15	22
Part of linked supply chain/ production system	15	11	16	23
Others	18	21	11	19

Source: Far Eastern Economic Review/Deloitte Consulting (2000)

3.2 Projected Levels of Electronic Commerce

Electronic commerce has emerged as particularly important within the Asia-Pacific region, with one quarter of all business purchases predicted to be made online by 2003 (Boston Consulting Group 1999; Greenberg 2000). This translates into US$430 billion, approximately one quarter of the worldwide business commerce total, according to Boston Consulting Group (CyberAtlas 2001a).

The Gartner Group has estimated that the business-to-business market in the Asia-Pacific region will be worth US$910 billion by 2004. The most commonly traded products will be in the utilities sector. Chemicals, rubber and plastic will produce a combined trading value of US$100 billion for the region's business-to-business market, while US$18 billion will be contributed by textiles, apparel, shoes and leather. Gartner attributes this growth largely to the entrance of banks such as Siam Commercial Bank, Bank of Asia, and Krung Thai Bank into the market, providing the necessary financial infrastructures and payment mechanisms (Gartner Group 2001). Gartner Group's prediction is that by 2005, the Asia-Pacific region will account for 28 per cent of the worldwide business-to-business commerce total, with business-to-business Internet commerce transactions of US$2.4 trillion (CyberAtlas 2001a).

Individual countries have also identified business-to-business electronic commerce as a growth area. In Canada, for example, business-to-business electronic commerce is predicted to increase to Can$272 billion (US$181.3 billion) over the next five years (Forrester Research 2001). Small business online transactions reportedly increased by Can$540 million (US$356.4 million) to Can$1.3 billion (US$858 million) in the year to May 2001 (SES Research 2001).

The growth of the Internet in China has been spectacular, rising from under 1 million users in 1997 to 8.9 million by the end of 1999, and nearly 23 million by the end of 2000 (CNNIC 2001a). At 30 June 2001, China Internet Network Information Centre, estimates that there were 26.5 million regular users of the Internet (Schauble 2001), while a recent report from the *New York Times* puts the current number of Internet users in China at about 30 million (Smith 2001). Nearly 15.5 million Chinese Internet users had dial-in access, around 60 per cent using home access and around 44 per cent using office access (CyberAtlas 2001b).

While many of these users are individuals such as students and professionals, a significant proportion of Internet users are engaged in commerce, banking and other industries (CNNIC 2001b).

However, the development of electronic commerce is assessed as being still at an early stage, largely due to the absence of a consumer credit system to facilitate online trading:

> *Online stock trading is in its infancy because of regulations that bar brokers from discounting commissions. Even application service providers—companies that sell online software for accounting and other services—have yet to take hold.*
>
> *About half of the people with Internet access, meanwhile, log on through Internet cafés or other public venues, making them unlikely candidates for online economic activity*.

In India, electronic commerce levels are predicted to reach INR252 billion (US$5.3 billion) by 2005, up from INR4.5 billion (US$95.8 million) in 2000 (NUA Surveys, 23 May 2001). While Internet trading is a relatively new activity, with only a third of Indian Internet users having purchased goods online, there is reportedly strong interest in using the Internet for commercial dealings (Brandquiver / Yahoo 2001).

In Japan, it has been estimated that by 2003 the business-to-business electronic commerce market will be some 20 times greater than the business-to-consumer market and will involve around 11 per cent of all commercial transactions, compared to only one per cent of consumer transactions (Japan Economic Foundation 2000).

In New Zealand, over half (54 per cent) of businesses recently surveyed were found to have their own web sites, 28 per cent had web sites capable of taking orders, and eight per cent were capable of taking payments online. Further, 19.6 per cent of organisations reported involvement with business-to-business sales while 19.2 per cent were doing business-to-consumer sales (Clark et al. 2001).

In Australia, the National Office for the Information Economy's (NOIE) report on electronic commerce beyond 2000 suggests that electronic commerce initiatives in Australia could bring about a 2.7 per cent increase in the level of national output, and enhance consumption by about A$10 billion

within the next decade (NOIE 2000). It has also been predicted that electronic commerce will be worth A$1.6 trillion to the Asia / Pacific region by 2004 (Gosnell 2000).

However, NOIE estimated in late 1999 that electronic commerce activity will increase Australian gross domestic product by 2.7 per cent by the year 2007, with real wages expected to increase by 3.5 per cent as a result of improved efficiency and employment levels increasing by 0.5 per cent (NOIE 1999).

3.3 Significance for the Region

Given the global reach of the Internet and the rapid expansion of electronic commerce, it is inevitable that countries in the Asia-Pacific region will be affected by Internet fraud. The United States-based Internet Fraud Complaint Center reported in October 2000 that (IFCC 2001):

> *The IFCC has received complaints of victims from 103 different countries. The top 10 countries reporting Internet fraud include victims from the United States, Canada, Australia, United Kingdom, Singapore, Japan, Germany, Aruba, Uganda and Hong Kong. Other complaints received include victims from China, Malaysia, Armenia, Iceland, Saudi Arabia, Fiji, Pakistan, Wales, Ukraine, Tuvalu and Thailand, to name a few.*

It can be predicted that as electronic commerce continues to expand in the Asia-Pacific region, more instances of Internet fraud affecting business and government transactions will emerge.

KPMG's Nolan Norton Institute in Australia and New Zealand recently conducted a survey to determine the views of senior business and IT executives about electronic commerce usage, benefits, barriers and the likely future uptake of electronic commerce technologies.

> *Our findings indicate that the electronic commerce wave is beginning to break in the Asia-Pacific region. For those organisations brave enough to overcome the perceived and real challenges that this exciting new business tool offers, genuine gains in both profitability and productivity are already being achieved.*
>
> *E-commerce is here to stay and is considered a 'must do' by many organisations in the Australia/New Zealand region. Whether their adoption of this business tool proves to be profitable or not will depend largely on how they approach it.*

Despite many advances being made in electronic commerce adoption and implementation in the region, much of the activity remains in the talking stage. The expected benefits from the adoption of electronic commerce technologies and the actual benefits achieved have proved somewhat disappointing for many organisations. Much of the failure to live up to expectations is due to the perception that gains will be easy and that they will be achievable within an overly optimistic timeframe. This may also be due to inappropriate metrics being applied to measure the success of a venture.

Security is perceived as one of the main barriers to the adoption of electronic commerce technologies, though solutions are readily available. Surprisingly, environmental determinants have little influence on respondents' electronic commerce strategic intent.

KPMG's Nolan Norton Institute identified two groups from its survey results—those organisations that had achieved profit and / or productivity gains from electronic commerce implementation, and those that had not. These groups, classified as Leaders and Followers, displayed distinct sets of characteristics in terms of electronic commerce adoption, implementation and integration.

Generally, the future of electronic commerce in the region looks optimistic, with significant plans being made for increased activity and implementation in the region.

4 The Nature and Extent of Internet Fraud

4.1 The Problem of Under-reporting

In carrying out an assessment of the scope of Internet fraud arising out of electronic commerce, the problem of under-reporting of incidents needs to be appreciated. Often when organisations have been victimised through fraud, managers are reluctant to report the matter to the police or otherwise to seek official redress. This means that information concerning the nature of the incident usually never enters the public arena. KPMG (1999), for example, found in its survey of business fraud, that 33.3 per cent of organisations surveyed failed to report frauds to the police, many instead preferring to deal with the matter internally and or by dismissing the individual in question.

Some of the reasons given by the respondents to Deakin University's (1994) survey of fraud incidents in Australia for not reporting fraud to the police included a belief that the matter was not serious enough to warrant police attention, a fear of consumer backlash, bad publicity, inadequate proof, and a reluctance to devote time and resources to prosecuting the matter. Similar reasons for non-reporting of electronic commerce incidents were given by the respondents to KPMG's Global eFraud survey (2001) in addition to the key factor of the need to re-instate systems quickly so as to prevent loss of business. Reporting the matter to the authorities simply prevented the organisation in question from minimising its financial losses, and possibly leading to further losses being incurred in prosecuting the matter.

Businesses are reluctant to report fraud simply due to a fear of 'sending good money after bad' as experience may have shown that it will be impossible to recover losses successfully through legal avenues and that the time and resources which are required to report an incident officially and to assist in its prosecution simply do not justify the likely return on investment. Prosecution may entail countless interviews with the police, extensive analysis of financial records, and lengthy involvement in court hearings for staff.

The other disincentive to taking official action lies in the reluctance of organisations to publicise the fact of their victimisation through fear of losing business or damaging their commercial reputation in the marketplace. Government agencies might also believe that adverse publicity may result in a loss of confidence in voters, whilst financial institutions might believe that publicity of security weaknesses might result in acts of repeat victimisation taking place using the same techniques as those being investigated.

Each of these considerations means that the incidents of Internet fraud that are disclosed publicly represent a small proportion of the total number of incidents that occur. In reading the following estimates of loss, therefore, this problem of under-reporting and under-estimation of loss needs to be fully appreciated.

4.2 General Assessments of the Scale of the Problem

Most of the general estimates of the scale of the problem of Internet fraud come from business victimisation surveys conducted by the large consulting practices. Unfortunately, official police records are generally not compiled in such a way that specific types of criminal fraud can be isolated. Most police agencies, for example, simply record statistics on offences of 'dishonesty', making it impossible to know which were carried out using online technologies. Individual corporations rarely indicate the scale of their losses due to fraud, although in relation to card-based transactions, MasterCard International estimates that fraudulent transactions account for 0.08 per cent of its annual gross dollar volume of US$857 billion, of which six per cent takes place on the Internet (Kennedy 2001).

The business victimisation surveys have shown generally high rates of concern about the problem of computer-related crime, and Internet fraud in particular, over the last few years. Although often based on relatively small samples of respondents, they do give some indication of the scale of the problem, although, once again, some of the surveys fail to differentiate Internet-related fraud from other types of fraud and specific types of computer crime.

One of the most recent surveys was carried out by KPMG in 2001. In relation to the influence of security risks on electronic commerce, KPMG's Global eFraud survey (2001), found that 39 per cent of the 1,253 respondents said

that security and privacy issues prevented their company from implementing an electronic commerce system, with 50 per cent of respondents saying that cost was the main problem in establishing such a system. Seventy-nine per cent of respondents indicated that a security breach to their electronic commerce system would most likely result from a breach caused via the Internet or other external access. Risk of damage to the company's reputation was considered by 72 per cent of respondents to be the major damage that could be caused to their electronic commerce system.

In KPMG's Global eFraud survey (2001), only nine per cent of respondents indicated that a security breach had actually occurred within the preceding 12-month period, although 23 per cent of respondents from India reported having experienced a security breach of their electronic commerce systems, the highest percentage reported from any country surveyed. The types of security breaches reported included viruses, system crashes, web site defacement or alteration, and system resources being re-directed or misappropriated. In approximately one half of cases, the victim was unable to identify the perpetrator.

Amarnathan (2000, p. 69) also confirms that the bulk of Internet-related crime in India relates to major banking fraud and stock market manipulation, and software piracy, representing a greater problem than content-related matters such as the dissemination of offensive materials.

Concern about Internet fraud was also expressed by public and private sector representatives who attended a seminar entitled, 'Information Security: A National and International Imperative' organised by the Bagladesh Computer Council in Dhaka on 13 January 2001. The need for adequate security policies and measures to be used in order to prevent various forms of cybercrime was expressed by the Commerce Minister, Abdul Jalil and S. M. Kamal, Founder President of the Bangladesh Computer Council (Independent Bangladesh Staff Reporter 2001).

KPMG has also regularly conducted global fraud victimisation surveys. Although small in number, between 1997 and 1999 there was a 71 per cent increase in the percentage of respondents to KPMG's fraud surveys who reported computer-related fraud (7 to 12%). Total reported losses due to computer crime were over US$16 million in KPMG's (1999) survey, although these figures are likely to be under-estimates as many organisations were unaware of the extent to which their organisation was being defrauded through the use of computers and some did not define other forms of fraud

as computer-related (such as ATM fraud and false identification fraud carried out through the use of desk-top publishing equipment). In 1999, 36 per cent of KPMG's respondents who reported computer crime were either unaware of how much they had lost or were unwilling to disclose it.

Of the 84 Australian organisations surveyed by Ernst and Young (1998) in October 1997, 80 per cent believed that they were vulnerable to computer fraud, which was considerably higher than in other countries.

In November 1998, a survey was carried out of 350 large Australian organisations by the Victoria Police and Deloitte Touche Tohmatsu (1999). Thirty-three per cent of respondents reported unauthorised use of their computers within the preceding 12-month period and one quarter of these attacks were motivated by financial gain. More than one third of those who responded believed that computer theft would have an impact on their organisation over the next five years.

In March 2001, the Computer Security Institute and the FBI's Computer Intrusion Squad (2001) based in San Francisco released its sixth 'Computer Crime and Security' survey. This was a survey of over 500 computer security practitioners in corporations, government agencies, financial institutions, medical institutions and universities in the United States.

Eighty-five per cent of respondents (primarily large corporations and government agencies) detected computer security breaches within the preceding 12 months. Sixty-four per cent acknowledged financial losses due to computer breaches. Thirty-five per cent (186 respondents) were willing and / or able to quantify their financial losses. These 186 respondents reported US$377,828,700 in financial losses. In contrast, the losses from 249 respondents in the 2000 survey totalled only US$265,589,940. The average annual total losses sustained over the three years prior to 2000 was US$120,240,180.

As in previous years, the most serious financial losses occurred through theft of proprietary information (34 respondents reported US$151,230,100) and financial fraud (21 respondents reported US$92,935,500). For the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the rise in those citing their Internet connections as a frequent point of attack rose from 59 per cent in 2000 to 70 per cent in 2001. Thirty-six per cent of respondents reported the intrusions to law

enforcement; a significant increase from 2000, when only 25 per cent reported them. (In 1996, only 16 per cent acknowledged reporting intrusions to law enforcement.)

In terms of reported incidents relating to electronic commerce, the survey found that of the 47 per cent of respondents who conducted electronic commerce on their web sites, 23 per cent suffered unauthorised access or misuse within the preceding 12 months, while 27 per cent said that they did not know if there had been unauthorised access or misuse of their sites. Twenty-one per cent of those acknowledging attacks reported between two and five incidents while 58 per cent reported 10 or more incidents. Eight per cent of respondents reported financial fraud of their electronic commerce sites which had increased from only three per cent in the 2000 survey.

Although solely based on corporations in the United States, these figures give some indication of the likely risk levels that might occur in the Asia-Pacific region in the future when computer-usage rates equal those currently existing in the United States.

4.3 Specific Types of Internet Fraud

Internet fraud, as defined above, can be committed in a wide range of ways and target various entities. The following categories of conduct are indicative of the scope of the problem, although clearly other instances could also be included. Generally, they involve the Internet as the target or as the means of perpetrating economic crimes of deception. The following discussion examines the nature and extent of some of the principal types of business and government Internet fraud and provides some examples of incidents that have taken place in the Asia-Pacific region. A final section looks briefly at the scale of consumer Internet fraud by way of comparison.

4.3.1 Fraudulent Online Business Practices

Although Internet-based technologies can greatly enhance the speed and efficiency of business transactions, they also create new business risks. Often the speed with which online transactions take place facilitates acts of fraud as there may be no ‘cooling-off’ period during which the parties to transactions can reflect on the terms of a proposed agreement and obtain verifying evidence about the subject matter or identity of the other contracting party. Sometimes, necessary internal controls that are designed

to prevent fraud, may not operate in the case of Internet transactions, in which agreements may be struck and payments made instantaneously.

In addition, electronic transactions entail a loss of collateral information about those involved, such as key social and business cues that are used to establish trust in commercial transactions. These include appearance, facial expression, body language, voice, dress, and demeanour which may all not be apparent when one transacts business online. The absence of such cues greatly enhances the ability of fraudsters to disguise their true identities or to make use of other people's identities which is often an essential precursor to committing a crime. The development of effective user authentication technologies may provide a solution to this problem (see below).

A related risk concerns the theft of personal information from databases which can then be used to commit fraud. Organisations that engage in electronic transactions maintain extensive databases of personal information including names, addresses, bank account and credit card details, as well as detailed personal information relating to patterns of purchasing which can be used for marketing purposes. Where such information is not held securely, considerable opportunities arise for fraudsters, not only in misusing identities but also in being able to target victims more easily and extensively.

Electronic commerce may also involve parties located in different countries. While this simply replicates the traditional risks associated with international trade, in the case of online transactions it may be more difficult to identify and to locate the offending party, and even more difficult to mobilise law enforcement agencies to take action.

A further problem associated with conducting business transactions online relates to the use of encryption. Although useful in order to protect confidentiality of legitimate information, the use of encryption makes it difficult or, on occasions, impossible for law enforcement and other official agencies to read the communications in question. This has already occurred in the international investigation conducted into the 'W0nderland' group in which those involved in distributing child pornography used heavy encryption to prevent law enforcement officers from obtaining evidence (the number '0' in its name also prevented inadvertent users of the Internet from stumbling across the group when searching the Internet). In business contexts, there is a risk that individuals could encrypt important communications and then refuse to decrypt them unless a fee were paid.

Most frauds involving business transactions carried out on the Internet relate to misleading and deceptive practices which mirror similar activities conducted using traditional paper-based techniques. On the Internet, however, fraudsters now enjoy direct access to millions of prospective victims around the world, instantaneously, and at minimal cost. Examples include so-called advance fee schemes, such as pyramid and Ponzi schemes, the use of chain letters and bulk electronic mail, business opportunity schemes, and fraudulent online auctions, prizes and lotteries. Even the endemic West African advance fee letter scams are now being conducted electronically (Smith, Holmes, and Kaufmann 1999).

West African advance fee scams began with offenders working from Nigeria targeting victims across the globe, principally through the use of letters posted by mail (often with counterfeit postage stamps). Confederates and other fraudsters in other African countries, the United States, Britain, Canada, Hong Kong and Japan then began using the same techniques. The scale of these frauds increased considerably and created a global problem for law enforcement. Some prosecutions have taken place in West Africa, the United States and England although many offenders have evaded detection and punishment. The United States Secret Service estimated that since 1989, US$5 billion had been stolen from victims throughout the world, including Australia. Between August and November 1998, Australia Post, in Sydney alone, confiscated 4.5 tonnes of advance fee correspondence which had counterfeit postage, amounting to approximately 1.8 million items. The Internet and email have recently proved to be an effective way of disseminating advance fee letters as the true identity of the sender is easy to disguise and original supporting documentation unable to be checked for authenticity.

Other frauds carried out through the use of the Internet involve the non-delivery of goods and services or the delivery of defective products and services. Those which have become particularly prevalent in business contexts have involved computer products and services and financial services, while in the realm of consumer transactions health and medical products, and the provision of sexual services, have often been found to be dishonest (see below).

Finally, the Internet is being used for various forms of unsolicited or bait advertising and illegal inertia selling techniques which generally infringe local consumer protection legislation.

Although many of these scams seek to defraud consumers, they can just as easily target businesses and government agencies.

4.3.2 Online Funds Transfer Fraud

The Internet may also be used in connection with the commission of various forms of theft of funds electronically (see Grabosky, Smith and Dempsey 2001). Sometimes, security information such as passwords and account details can be obtained by gaining access to databases held by businesses or financial institutions. On other occasions, insiders may move funds electronically by sending instructions via electronic mail. When the use of electronic commerce becomes more widespread, abuses relating to the transfer of funds electronically can be expected to increase.

In one case, for example, two individuals who worked for a computer training company, Aptech, in India, allegedly sent electronic mail messages in the name of Microsoft and Videsh Sanchar Nigam (India's overseas telephone service provider) that contained an attachment which, when opened, sent messages back to the accused containing passwords and other data from the State Bank of India. Both were arrested and charged under India's *Information Technology Act 2000* with hacking which carries a maximum penalty of three years' imprisonment and 200,000 rupees fine (US$4,300)(Bloomberg News 2001).

Another example of funds transfer fraud was perpetrated against the government of a South Pacific Island nation (name withheld) and reported at the first meeting of the INTERPOL Asia Region Working Party on Information Technology Crime in 1997. In that case, some US$600 million had been fraudulently transferred out of government funds held by the Central Bank via computer on a Friday afternoon to overseas bank accounts. The transfer failed, however, owing to the offender having made a simple syntax error in the instructions, and he was able to be located having left the country in question (Berwick 2001).

In the Australian Capital Territory in 1998, a financial consultant to the Department of Finance and Administration allegedly transferred A$8.725 million electronically to private companies in which he held an interest, after logging-on to the Department's computer network using another person's name and password. The individual in question was charged with defrauding the Commonwealth of Australia. It was reported that $5.48 million had not been recovered by the police following an investigation (Campbell 1999).

In December 1999, two offenders in China were reportedly sentenced to death for using a computer to illegally transfer the equivalent of US$31,000 from a bank into their own accounts (Yeang 2001).

4.3.3 Securities and Investment Fraud

The Internet is now regularly being used for corporate activities that extend from offering and trading in securities to lodging official documents electronically with regulatory agencies. Already instances have begun to emerge of fraudulent conduct involving the sharemarket that have used the Internet to disseminate false information in order to attract investors, or to manipulate sharemarkets.

In 1998, for example, a worldwide clean-up operation, involving the Office of Fair Trading in Britain and its counterparts in 22 other countries, identified 1,159 potential 'get rich quick' schemes being advertised on Internet sites (Office of Fair Trading 1998).

Individuals in the Asia-Pacific region have been victimised in a range of schemes disseminated globally via the Internet. In November 1998, Philippine police raided a hotel near Subic Bay and arrested three men involved in a scam in which Filipino, Chinese and Bangladeshi workers were being sold worthless passport documents for sums of US$3,500 (Lintner 1998). The ostensible origin of the documents is the Dominion of Melchizedek, a fictitious country existing only in cyberspace, complete with a web site containing maps, history, legislation, news, a university, stock exchange, and list of government ministries, embassies and legations (Melchizedek 2001). The founders and operators of this global scam have been prosecuted in various jurisdictions including the United States (*Securities and Exchange Commission v. World Financial & Investment Co., Inc. and Victor M. Wilson*, US District Court, E.D.N.Y., No. 99-CIV-7608 (ILG); see further Quatloos 2001). In Fiji, for example, agents from the (non-existent) Dominion of Melchizedek, headed by convicted Californian fraudster David Korem (also known as Mark Pedley), sold fictitious stocks on the Internet in the name of the Fijian island Rotuma, located 600 km north of Suva. The scam organisers, one of whom was part Rotuman, had been trying to engineer the breakaway of Rotuma from Fiji for their own political reasons, although the activities were financially motivated (Daily Excelsior 2000).

The accessibility of online share trading facilities has posed unprecedented opportunities for sharemarket manipulation. The proliferation of day traders contributes to the volatility of share prices, particularly in those securities

which are thinly traded. Against this background, structuring transactions in a manner which will give the impression of momentum in the price of a share would appear to be readily achievable at the hands of an individual or investors acting in concert (Grabosky, Smith and Dempsey 2001).

Bulk email programs allow stock promoters to send personalised messages to thousands and even millions of Internet users simultaneously. In the Asia-Pacific region, a number of instances have been discovered of Western fraudsters based in the Philippines, Indonesia and Thailand using high-pressure marketing techniques to sell non-existent or over-priced financial products to investors world-wide. In one recent operation, 70 foreigners were arrested in Bangkok for using unsolicited telephone and email contact to promote share investments (Australian Securities and Investments Commission 2001b). Victims have been offered quick and tax-free profits from trading shares, currencies and other equities. In July 2001, a 26-year-old Australian, Adam Cameron McGlashan, was arrested in the Philippines and charged with selling bogus shares worth more than A$12 million from a call centre in Manila. Since the operation began in July 2000, it was alleged that the syndicate had taken more than US$6 million with between 30 and 40 per cent coming from Australian investors. The case is being investigated by the Philippines Securities and Exchange Commission (Baker 2001).

In another recent case, a 24-year-old man who lived in a Melbourne suburb, manipulated the share price of an American company by posting information on the Internet and sending email messages around the globe that contained false and misleading information about the company (Tomazin 2001; ASIC 2001a).

On 8 and 9 May 1999, the man posted messages on Internet bulletin boards in the United States and sent more than four million unsolicited email messages to recipients in the United States, Australia and other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US$0.33 to US$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than 10 times the previous month's average trading volume.

The offender had purchased 65,500 shares in the company through a stockbroking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the

transmission of the information and realised a profit of approximately A$17,000. The offender was prosecuted by the Australian Securities and Investments Commission (2001a) for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that 21 months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of $500 (*Australian Securities and Investments Commission* v *Steven George Hourmouzis*, County Court of Victoria, 30 October 2000, Stott J). In a separate prosecution, Wayne Loughnan, of Cawarral in central Queensland, who assisted Hourmouzis in the sharemarket manipulation, was sentenced to two years' imprisonment, wholly suspended, in the County Court of Victoria on 22 May 2001.

So-called 'spamming' of information relevant to the stock market can be indiscriminate—in September 1998, the Chairman of the Australian Securities and Investments Commission, himself, received an anonymous email message enthusiastically promoting a stock traded in the United States (Phillips 1999, p. 13).

The possibility of insider trading also exists in the digital world of sharetrading in much the same way as in the traditional sharemarket. Already instances have begun to emerge. In Australia, for example, beginning in 1999, a number of small speculative mining companies began to diversify into Internet-related activities, hoping to ride the wave of high technology on the Australian and United States stockmarkets. Regulatory authorities observed a surge in stock price and trading volume of these companies *prior to* the announcement of their proposed metamorphosis, and expressed concern about future potential for false and misleading statements in this area (Phillips 1999).

4.3.4 Identity-related Fraud

One of the most frequently used strategies to perpetrate fraud is the creation of false documents for misrepresenting one's identity. Once a convincing identity has been fraudulently established, it is then possible to steal money or otherwise to act illegally and then to evade detection, investigation and arrest (Smith 1999).

The technology of the Internet makes it relatively simple to disguise one's identity. 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 organisations might, in fact, be individuals employed specifically to indicate their approval of the organisation in question.

It is also possible to choose legitimate-sounding names in order to improve one's credibility or include domain names which are misleading (see Bachner and Jiang 2000). There has recently developed a practice in the United States and Canada, for example, of some organisations adopting domain names containing the names of Australian cities in order to improve their credibility, despite the fact that they have no connection at all with Australia.

An example of a recent identity theft case that made use of the Internet concerned 200 of America's richest people who were victimised by a 32 year-old New York chef, Abraham Abdallah. Abdallah was alleged to have used computers in a public library to obtain millions of dollars from the accounts of billionaires such as George Soros, Steven Spielberg, talk show host Oprah Winfrey, former presidential candidate Ross Perot, George Lucas and Ted Turner. Abdallah allegedly obtained information from credit reference companies by forwarding letters, purporting to be from major banks, requesting information. He used answering machines, courier drop-offs and email accounts to discover enough information to take over the electronic identity of his victims. He was only detected when he sent an email message to Merrill Lynch pretending to be billionaire Thomas Siebel, asking for US$10 million to be transferred to an Australian account. Merrill Lynch was concerned that the transfer would overdraw his account and contacted Siebel (Ringin 2000).

In Japan, the Internet was used by an offender to advertise the availability of bank accounts he had opened using false identities. In September 1999, Osaka police arrested a 31-year-old man, Teruhiko Ikeda, on suspicion of having used forged health insurance certificates to open bank accounts in false names. He allegedly sold the bank accounts through the Internet to enable his customers to use the accounts to perpetrate fraud and other crimes. In May 1998, Ikeda allegedly instructed his accomplice, Kyuzo Takehara, to open five accounts at a bank in Kyoto under a false identity by using forged health insurance certificates. Some 50 accounts at banks in

Tokyo and Kyoto were opened in a similar way and then sold on the Internet. Both Ikeda and Takehara were arrested for alleged forgery and use of private documents (Japan Times Online 1999).

4.3.5 Procurement Fraud

There are considerable savings to be had from organisations carrying out purchasing and procurement activities electronically. Tenders can be widely disseminated and documents dowloaded electronically, while contracts can be negotiated and settled more quickly and easily than in pre-electronic times. This should lead to higher levels of openness, trust and cooperation being established between those involved in the procurement process (Department of Public Works and Services, New South Wales 1999).

In Pakistan, for example, the Electronic Government Program aims to generate transparency and savings in procurement costs for the government through the introduction of a complete system of electronic procurement from supplier management and tendering to the award of contracts. A database of suppliers and the latest market prices of items purchased will be maintained. Each department in the government will have access to the system and a database of suppliers and item prices maintained, thus enabling them to select the supplier of choice and the price to generate a purchase order. The system will be linked directly with the government's finance and budget system to ensure that expenditure on government procurement is subject to audit (Pakistan Information Technology Commission 2001).

Electronic procurement, however, carries risks of fraud and abuse as internal controls may be removed when new electronic procurement systems are introduced. Government agencies are particularly vulnerable in view of the extensive procurement activities in which they engage, and the large sums of money involved. In one Australian case, for example, a sub-contractor to a local Council in New South Wales allegedly gained access to the Council's database of tendering information and was able to secure numerous contracts through the use of this information (Bell 2000, p. 31).

4.3.6 Outsourcing Risks

Various opportunities also exist for economic crimes to take place in connection with the outsourcing of services, particularly those relating to information technology and data management (Bell 2000). The use of

Application Service Providers (ASPs) who provide space for the storage of digital information belonging to other entities on a commercial basis, creates risks that the information may be used for fraudulent purposes or sold-on without authority. The outsourcing of information technology services generally also creates risks of fraud and corruption where contractors abuse the trust that they are given in managing confidential and sensitive data.

4.3.7 Public Sector Fraud

As government benefits programs continue to be administered electronically, the opportunities for fraud against public sector agencies will increase. In Australia, for example, Electronic Benefits Transfer (EBT) systems are being used for the delivery of social security benefits and, unfortunately, have been subject to abuse. The system operates on a national scale and assists in the electronic delivery of limited social security benefits in cases previously addressed using the traditional counter cheque. Plastic cards can be used to obtain cash from ATMs by authorised recipients.

In Australia a number of prosecutions have taken place in respect of internal fraud carried out by government employees fraudulently using the EBT computer system in December 1997 and January 1998. EBT cards were issued in fictitious names enabling the offenders to obtain cash at ATMs. In one case, the proceeds of the fraud were used to purchase heroin in the same street as the location of the ATM and within 10 minutes of the fraud occurring (Warton 1999).

Opportunities have also arisen for employees of public sector health benefit providers to manipulate the electronic claims processing systems. Risks relate to the possibility of electronic claim forms being counterfeited or manipulated electronically, digital signature keys being compromised, and electronic funds transfers being altered or diverted away from legitimate recipients (Smith 1999). In Australia in 1997, for example, two former employees of the Health Insurance Commission (which provides health and medical benefits to doctors and the public) were convicted of defrauding the government by creating false provider accounts and making illegal claims to the combined value of more than A$45,000 (Health Insurance Commission 1997).

Another Australian incident involved the Australian Taxation Office's web site, GST Assist (established following the introduction of Australia's new taxation system) being compromised. A student known variously as K2 and Kelly exposed a glaring security breach in the web site. Simply by typing in

a string of numbers, K2 was able to gain access to the records of more than 20,000 GST-registered providers, which contained their bank account details. He alerted more than 17,000 of the providers by sending their confidential details to them by email (Dancer 2000, p. 76).

Public sector employees may also use information technologies that have been provided to them for official purposes inappropriately for unauthorised purposes. Despite the most clear warnings being given to employees of the consequences of inappropriate use of the Internet in the workplace, cases continue to emerge of staff misusing the Internet in this way. In a number of widely-reported cases, employees have been disciplined or dismissed for using workplace computers inappropriately. In New Zealand, for example, four employees of the Department of Child, Youth and Family Services were dismissed for inappropriate use of the Internet which included gaining access to pornographic material (Anonymous 2000).

4.3.8 Theft of Services/Non-provision of Services

As with other types of telecommunications, it is possible to steal Internet-related services by entering into a contract with an ISP and a telecommunications carrier, and then failing to pay for the services provided. Making use of a false identity or using someone else's bank account are the usual means of carrying out such conduct. Fraud of this nature may be committed by both individual consumers as well as business entities.

A related problem arises where a person visits a web site that manipulates the telephone billing system and results in large international calls being billed. One case 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 ISP, 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 United States Federal Trade Commission 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).

The other side of this problem concerns ISPs which fail to deliver the services they agree to provide. As online consumers continue to increase their use of the Internet, so the number of complaints about ISPs has also increased. In Australia, for example, complaints to the regulatory agency, the Australian Competition and Consumer Commission (ACCC), have included 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). Both individuals and business and government entities may be victimised in this way. Although the consequences of such conduct may result in civil action by way of proceedings for breach of contract, the present discussion focuses on criminal consequences such as prosecution for theft, dishonesty, and other offences involving misleading practices.

4.3.9 Information Piracy

The Internet can also be used to make illegal copies of data in breach of copyright laws. Any type of data transmission can be copied with the greatest concerns relating to audio and visual data such as music and films. As broadband services continue to become available with text, graphics, sound and video information being freely accessible via cable modems, the potential for copyright infringement involving such works will be enhanced enormously. It is now possible, for example, to download compact disks and feature films from the Internet. According to the *Straits Times* (8 November 1999), a copy of the James Bond Film *The World is Not Enough*, was available free on the Internet before its official release.

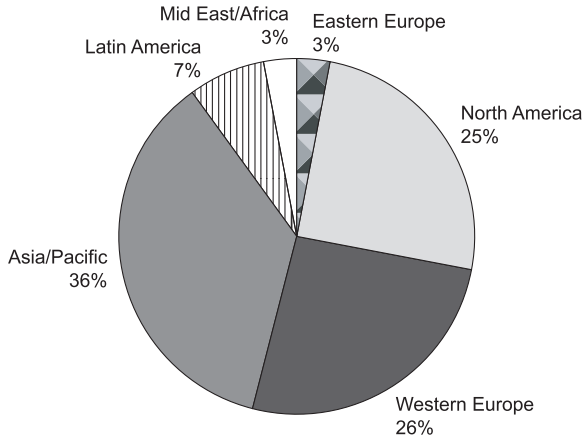
The Business Software Alliance's (2001) annual survey of software piracy for 2000 found that the Asia-Pacific region was the only area globally to increase its rate of piracy since the study began in 1994. Piracy rates were calculated by comparing the difference between software applications installed (demand) and software applications legally shipped (supply). The piracy rate was thus defined as the volume of software pirated as a percentage of total software installed in each country.

Several large countries in Asia experienced increases in their piracy rates in 2000. For example, Japan's rate increased to 37 per cent, China's rate increased to 94 per cent, and Korea's rate increased to 56 per cent. Several

other countries showed very little change in their piracy rates in 2000. India had a 63 per cent piracy rate, up from 61 per cent in 1999. Hong Kong had a 57 per cent piracy rate, up from 56 per cent in 1999. Australia had a 33 per cent piracy rate, up from 32 per cent in 1999. New Zealand, with a 28 per cent piracy rate in 2000, continued as the country with the lowest piracy rate in the Asia / Pacific region. Vietnam, with a piracy rate at 97 per cent, continued as the country with the highest piracy rate in the region. China, with 94 per cent, followed as the country with the second highest piracy rate.

In terms of the dollar value lost to piracy, the survey found that in 2000 the Asia-Pacific region sustained the highest percentage of losses (Figure 9) of all regions owing to its having an extensive PC and software market.

Figure 9: Percentage dollar losses due to software piracy by region

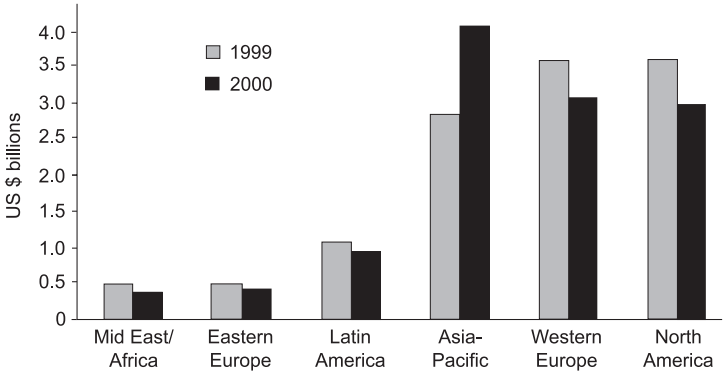


Source: Business Software Alliance 2001, p. 4

Globally, companies lost approximately US$11.7 billion in the 2000 calendar year. Losses in the Asia-Pacific region amounted to over US$4 billion, an increase of US$1 billion on the 1999 survey estimate of US$3 billion as shown in Figure 10.

Although these figures do not suggest that all software piracy losses were carried out through the Internet, clearly the theft of copyright material by downloading it from the Internet represents a considerable problem. An earlier estimate of software piracy by the Software Publishers' Association, for example, found that US$7.4 billion worth of software was lost to piracy in 1993 with US$2 billion of that being stolen from the Internet (Meyer and Underwood 1994).

Figure 10: Dollar losses due to software piracy by region



Source: Business Software Alliance 2001, p. 2

The campaign of the Microsoft Corporation (2000a; 2000b; 2001) against software piracy has resulted in the following action being taken in the Asia Pacific Region since 2000. In Hong Kong, in August 2000, the Anti-Internet Piracy Task Force of Hong Kong Customs took action against an Internet site allegedly involved in piracy and arrested two suspects. In April 2001, Hong Kong's Independent Commission Against Corruption seized over two-dozen counterfeit Microsoft CD stampers valued at approximately US$50 million from the offices of Optical Disk Manufacturers Association in Hong Kong, which resulted in the arrest of five individuals. In Macau, police seized more than 4,500 items of counterfeit software from vehicles passing the border between Macau and southern China and made two arrests.

On 19 August 2000, the Special Copyright Task Force led by the Malaysian Ministry of Domestic Trade and Consumer Affairs in conjunction with the Malaysian Police, Anti-Corruption Agency, and investigators from Microsoft, conducted a raid on a factory in the Klang Valley and seized more than 100 CD stampers / gold masters, 200,000 counterfeit CDs and 20 personal computers, worth an estimated US$480 million. The case began following the investigation of a Malaysian-based web site that allegedly offered counterfeit Microsoft products for sale in Australia via the Internet.

More recently, on 25 June 2001, the Enforcement Division of the Ministry of Domestic Trade and Consumer Affairs prosecuted the director of a graphic design company before the Sessions Court in Penang with possession of illegal software valued at MYR180,000 (approximately US$50,000). Under section 41(1)(d) of the *Copyright Act 1987*, the maximum penalty for copyright infringement for a company and its directors is a fine of up to MYR10,000 (approximately US$2,600) per infringement and or up to five years' imprisonment (Ching Yee Sing 2001).

In the Philippines in August 2000, an enforcement team of officials from the National Bureau of Investigations, Videogram Regulatory Board and the Council to Combat Video Piracy, raided a CD factory in the Clarkfield Special Economic Zone, Pampanga. More than 250,000 counterfeit CD-ROMs were seized along with a CD-printing machine and CD-production equipment.

In the People's Republic of China, officials recently raided a factory in Shenzhen and seized 2,600 pieces of high-quality counterfeit software, together with loose counterfeit manuals and related documentation. One investigation resulted in an offender, Wang Antao, being sentenced to four years' imprisonment by a court in Hangzhou for selling a slightly modified version of a company's software without permission. The court also ordered him to pay 20,000 yuan (US$2,400) in fines and 280,000 yuan (US$33,800) in compensation to the company. The case was the first one in which software piracy had resulted in a term of imprisonment being imposed (Wired News 1999).

In Thailand in March 2001, police officers from the Economic Crime Investigation Division raided two outlets located in Pantip Plaza and Mahboonkrong Shopping Centre for distribution of counterfeit CD-ROMs. The raids resulted in the seizure of 17,000 pirated CDs and CD-ROMs. Three shopkeepers were arrested and charged with copyright infringement.

These examples are indicative of the efforts being taken by police and industry organisations to deal with intellectual property infringements in the region which, although extending beyond Internet-based activities, are often greatly facilitated through the Internet (see further Smith 1997, Urbas 2000).

4.3.10 Page Jacking

Page jacking involves the appropriation of web site descriptions, key words, or meta-tags from other sites. Page-jackers insert these items into their own sites in an attempt to draw individuals to a particular site. The victim is then able to be defrauded in various ways, sometimes by having modem connections re-directed to international premium paid numbers, such as the Moldovan scam referred to above. Users' browsers can also be manipulated so that attempts to close the browser's windows or to use the 'back' or 'forward' button will simply direct the user to another site controlled by the fraudster (United States, Department of Justice 1999).

4.3.11 Digital Extortion

The Internet is also being used to carry out acts of criminal extortion which, although on the borderline of Internet fraud, can have substantial consequences for individual businesses. In one case, two individuals from Kazakhstan were arrested in London on 20 August 2000, for allegedly having broken into the computer network of Bloomberg LP, in Manhattan, in an attempt to extort money from the company. The arrest was made following a joint operation between the FBI's New York Field Office, the Metropolitan Police in London and authorities in Kazakhstan (Federal Bureau of Investigation 2000).

One Australian case involved a 27-year-old male, known as 'Optik Surfer', who was sentenced to three years' imprisonment (with 18 months' suspended) on 27 March 1998 in Sydney, for eight counts of obtaining unlawful access to a computer and one count of unlawfully inserting data into a computer.

The offender, who was a computer networking consultant, had been refused employment with an ISP in January 1994, and in March 1994 took revenge by illegally obtaining access to the company's computer network using the user account and password of the company's technical director. He then gained access to the company's database of 1,225 subscribers and publicised their credit card account details by disclosing them to various journalists. He also altered the company's home page on 17 April 1994, including a message that the company's security system had been compromised. The publicity resulted in the company losing more than A$2 million in lost clients and contracts. It was required to change its business name and sold the Internet access part of its business to another ISP (R. v *Stevens* unreported decision of the NSW District Court, 27 March 1998; appeal to the NSW Criminal Court of Appeal dismissed on 15 April 1999 [1999] NSWCCA 69).

4.3.12 Consumer Fraud

Although consumer-based Internet fraud is outside the scope of the present study, it is relevant in so far as consumers' experiences of fraud often involve business and government organisations, which could, themselves, be subject to victimisation of the same kinds. In addition, a number of the strategies used to perpetrate online consumer fraud are the same as those that could be used to defraud business and government organisations.

In the United States, the newly established Internet Fraud Complaint Centre—organised by the United States Department of Justice and the Federal Bureau of Investigation (2001)—received 19,490 complaints relating to Internet fraud from the time of its establishment on 8 May 2000 to 30 November 2000. The average monetary loss per complaint was US$665.00 with 49 per cent of complaints relating to auction fraud.

In 1999, Internet Fraud Watch reported an estimated 2 million instances of credit card fraud taking place with respect to online purchases in Europe, with a 600 per cent increase in Internet fraud complaints occurring in the United States since 1997 (Philippsohn 2000).

Also 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).

Finally, in a telephone survey of 1,006 online consumers conducted for the National Consumers League in the United States between April and May 1999, 24 per cent said they had purchased goods and services online. However seven per cent, which represents 6 million people, said that they had experienced fraud or unauthorised use of credit card or personal information online (Louis Harris and Associates Inc 1999).

In October 2000, the Internet Fraud Complaint Centre organised by the United States Department of Justice and Federal Bureau of Investigation (2001), reported having received complaints from victims of online consumer frauds from 103 different countries. The top 10 countries reporting Internet fraud were the United States, Canada, Australia, the United Kingdom, Singapore, Japan, Germany, Aruba, Uganda, and Hong Kong. Other complaints were received from victims in China, Malaysia, Armenia, Iceland, Saudi Arabia, Fiji, Pakistan, Wales, Ukraine, Tuvalu and Thailand. In another study of Internet fraud experienced by consumers in the United States, complaints against companies in other foreign countries rose from one per cent in 1999 to 2.3 per cent in 2000 (Internet Fraud Watch 2000), thus verifying the increasingly global nature of the problem.

In 1999 and 2000, the top 10 types of Internet fraud recorded by the United States Internet Fraud Watch were are shown in Table 8.

Table 8: Top 10 types of Internet fraud 1999–2000

Top 10 fraud types 1999		Top 10 fraud types 2000	
Type	%	Type	%
Online auctions	87	Online auctions	78
General merchandise sales	7	General merchandise sales	10
Internet access services	2	Internet access services	3
Computer equipment/software	1	Work-at-home	3
Work-at-home	1	Advance fee loans	2
Advance fee loans	0.2	Computer equipment/software	1
Magazine sales	0.2	Nigerian money offers	1
Information adult services	0.2	Credit card offers	0.5
Travel/vacations	0.1	Travel/vacations	0.5
Multilevel market/pyramids	0.1		
Total	98.4	Total	100

Source: Internet Fraud Watch (2000)

Web sites were by far the most common way in which consumers were solicited for fraudulent Internet offers (90% in 1999 and 82% in 2000), although an increase occurred between 1999 and 2000 in the number of initial contacts made through newsgroups (from 0.55% to 4% respectively). Contact through the use of email also increased from nine per cent in 1999 to 12 per cent in 2000.

The amount of money consumers lost to Internet fraud was also found to have increased with the average loss per person rising from US$310 in 1999 to US$427 in 2000. Losses overall were US$3,387,530.

There were also differences in the methods of payment used by the victims of Internet fraud (Table 9).

Table 9: Method of payment used by victims of five types of Internet fraud (percentages)

Method of payment	Online auctions	General sales	Internet access services	Work at home	Computer equipment/ software
Money order	48	25		23	27
Cheque	32	24	14	40	22
Credit card	6	28	37	19	24
Cashier's cheque	7	5			8
Cash	3			3	
Debit card		5	9		
Phone bill			15		
Bank account debit			13	9	
Wire transfer					13
Total	96%	87%	88%	94%	94%

Source: Internet Fraud Watch (2000)

An example of a recent case of abuse of credit card information disclosed in an unencrypted email message, involved a New Zealand consumer who had purchased a book from Amazon.com. The woman had purchased a book with her debit card and gave her cell phone number as a contact number. The book arrived, but a few days later she found her debit card had been used to make a number of unauthorised purchases from companies in Portugal, Indonesia and Brazil. All of the charges included the information she had given only to Amazon.com; namely, her card number, address and cell phone number. She also discovered that five new accounts had been opened with her details (Slane 2001).

Although online debit card fraud is relatively rare, it may result in more losses than credit card fraud, as credit card agreements usually limit the amount of loss per fraudulent transaction. In one case, an American victim discovered that all the funds in his debit card bank account had been removed by offenders based in Thailand who had obtained his account numbers from the Internet (Fenton-Jones 2000).

Cases of Internet fraud directed at consumers occasionally result in prosecution and punishment by the courts, although the sentences given are sometimes relatively low. In one recent New Zealand case, for example, three Christchurch youths aged 17, 18 and 19, were sentenced to community service by the Christchurch District Court in August 1999 and ordered to pay reparation on charges relating to credit card fraud using the Internet. Two of the youths were sentenced to 85 hours' community service and ordered to pay reparation (of NZ$160 and NZ$1,010), and the other youth was sentenced to 45 hours' community service (Mills 1999).

5 Business and Government Policy Framework

5.1 Relevant Policy Developments

In the early 1990s, the large Western democracies began introducing national policy frameworks designed to enhance electronic communication and to facilitate the growth of electronic commerce (Braithwaite and Drahos 2000, pp. 340–1). In September 1993, for example, the United States government released its National Information Infrastructure (NII) Agenda for Action. By February 1995, this policy framework had become the Global Information Infrastructure (GII). These initiatives have been taken up by other advanced countries globally. They have sought to liberalise telecommunications sectors globally and to harmonise regulatory measures in order to facilitate the spread of electronic commerce.

Individual countries have begun building their own policies for the expansion of information technology and the use of electronic commerce. In 1994, for example, Australia introduced its information infrastructure policy entitled *Networking Australia's Future,* while the United States released its policy paper entitled *A Framework for Global Electronic Commerce* in 1997.

In the Asia-Pacific region, the Chinese government has expressed its desire to develop the Internet as the number of users in the country doubles every six months. Over the past two years, the Chinese authorities have considerably changed their policy on controlling the Internet. The 'Great Cyber Wall' strategy, implemented in 1997 by the Ministry of Public Security and the Ministry of State Security, was abandoned in favour of selective enforcement and control carried out by ISPs and site managers themselves. Provincial governments have a certain level of autonomy in implementing Internet control policies. In the spring of 2000, for example, authorities in the Hubei province temporarily closed a site that published information about a financial scandal involving the vice-governor of the province (Reporters Sans Frontières 2001). Most government attention is being paid to Internet content deemed to be dissident or which contains politically subversive or

objectionable content, rather than deceptive, misleading or dishonest material. As such, Internet fraud does not have a high place on the policy agenda in China at present.

In Malaysia, the policy focus on Internet regulation has principally been on content that infringes social, political and religious values. Although fraud-related material may come within the scope of the regulation of general property crimes, there appear to be no specific policies on Internet fraud as such.

In India, the government has introduced various measures designed to increase productivity and quality of service in information technology. At present the government retains strict controls on access to the Internet by limiting the number of ISPs, making it possible to screen objectionable content more readily than in other countries (Amarnathan 2000, p. 69).

In Japan in August 1994, the government established the Advanced Information and Telecommunications Society Promotion Headquarters headed by the Prime Minister. In February 1995, it adopted basic guidelines on the promotion of Advanced Information and Telecommunications Society (Australasian Centre for Policing Research 2000, p. 84). These guidelines, and a subsequent report by the Working Group on Electronic Commerce, identified security and crime countermeasures as a key issue. On 16 February 1998, the Prime Minister stated that the government would 'implement suitable measures against high-tech crime and other problems relating to the development of an information society' (National Police Agency, Japan 1998, p. 1). As a member of the G8, Japan has moved to implement this plan of action including plans to establish a Cyber Police Force, to streamline the legal system, to cooperate with industry, to establish a framework of international cooperation, and to deal with electronic money-related issues (National Police Agency, Japan 1999, pp. 19–21). Crime involving electronic commerce has specifically been identified as a threat for the coming years.

In Pakistan, an Information Technology Commission was established by the Pakistan Government to promote the use of information technologies in all aspects of federal, provincial and local government activities. In 2001, the Pakistan Electronic Government Program was approved which will enable government services to be provided either through the Internet or through kiosks or automated teller machines. This project involves development of

web sites for the 34 ministries / divisions of the government. Information provided will include organisational details, rules and procedures, contact persons and their email, downloadable forms and data of interest to the general public. The project will entail the construction and maintenance of web sites which will enable queries to be dealt with and databases searchable for customised information. In addition to general web sites, three special purpose web sites will be developed to provide a range of facilities to the general public. These will include the provision of official forms, information on educational institutes, and information on Haj, Ziarah and Zakat. All the latest acts, regulations and notifications issued by government will be available and online access will be provided to private firms to electronically file tax returns. Electronic payment of bills will also be available and in the future electronic voting may be introduced. The project will be carried out by the private sector and will involve the establishment of 1,000 kiosks in 12 major cities of Pakistan (Pakistan Information Technology Commission 2001).

South Korea was one of the first countries in the world to adopt a law regulating the broadcasting and viewing of online information. Since 1995, the Electronic Communication Business Law has led to the creation of an Information and Communication Ethics Office—a public body that reviews sites, discussion forums and chat rooms, and can recommend that certain sites be blocked. South Korea's national security law also covers the Internet and forbids South Koreans from having any contact with their North Korean neighbours (Reporters Sans Frontières 2001).

There is no specific law governing the Internet in Sri Lanka but telecommunications regulators give technical licenses to ISPs—most of them private—but editors and managers of sites must register (identity card or commercial registration) with Cintec, the Council for Information Technology. Site managers are therefore easily identifiable by authorities.

Various steps have also been taken in the region to coordinate law enforcement policy responses with respect to cybercrime and Internet fraud. In March 2001, a meeting was held of police chiefs of a number of Asia-Pacific countries to devise ways in which to combat transnational crime through collaborative efforts with the European Union (*Bangkok Post*, 20 March 2001). Although cooperation would facilitate policing of traditional forms of transnational crime such as sea piracy, it would also be helpful for dealing with electronic crimes such as Internet fraud.

In Hong Kong, an Inter-Departmental Government Working Party was established in 2000 to examine computer-related crime and to review existing legislation. This working group is chaired by the Security Bureau of Hong Kong and held its first meeting on 28 March 2000 (Australasian Centre for Policing Research 2000, p. 86). Internet-related consumer fraud has already emerged in Hong Kong and is being dealt with by the Commercial Crime Bureau of the Hong Kong Police Force and the newly-established Computer Forensic Examination, Network Security and Investigation Group. In addition, the Computer Crime Section of the Commercial Crime Bureau has been expanded and a Computer Crime Investigation Cadre with 83 specially trained officers has been established (Australasian Centre for Policing Research 2000, p. 86).

In Australia, the National Office for the Information Economy (2000) was established in 1997 to coordinate Commonwealth Government policy on electronic commerce, online services and the Internet. In relation to electronic commerce it aims to facilitate the move of all sectors in the Australian economy towards the use of electronic commerce and to identify, develop and implement world leading-edge electronic commerce solutions. In particular, the office seeks to develop a comprehensive labour force strategy that will facilitate rollout of electronic commerce across Australian industries, and to develop strategies to overcome impediments to the adoption of electronic commerce.

In addition, a number of specialist groups have been established in Australia to examine the security and legal issues associated with electronic commerce. The Action Group into the Law Enforcement Implications of Electronic Commerce, for example, is a cross-agency government initiative designed to assess the technical implications of electronic commerce on law enforcement. It has produced a major report entitled *Contributions to Electronic Commerce: What Law Enforcement and Revenue Agencies Can Do* (Attorney-General's Department, Australia 1999) and continues its work into all aspects of the regulation of electronic commerce.

The other major development in Australia has been the work of the Australasian Centre for Policing Research which has reviewed current law enforcement capabilities to deal with electronic crime for the Australasian Police Commissioners' Conference. Its scoping paper, entitled *The Virtual Horizon: Meeting the Law Enforcement Challenges* appeared in 2000 and has led to a number of policy proposals being suggested.

In Australia, content on the Internet has been regulated to some extent by the *Broadcasting Services Act 1999* (Cwlth) which came into effect on 1 January 2000. This federal law, applicable in all the States and Territories making up the Australian Commonwealth, strictly defines content forbidden on the Internet: child pornography, bestiality, excessive violence, specific representations of sexual acts, and information on crime, violence and the use of narcotics. Sites with this sort of content must present the symbol RC (refused classification), X (adults only) or R (parental authorisation required). The evaluation and classification of content is the responsibility of the Australian Broadcasting Authority (ABA—the Australian authority that regulates radio and television services). When a site's content is rated according to this law, the ABA asks the ISP hosting the site to 'take reasonable measures to block access to it'. The authority also provides a list of sites rated RC or X to all ISPs.

This law does not, however, seek to regulate content that could be dishonest, misleading, deceptive or fraudulent other than if it fulfils the other criteria set out above. Advertising and other content relating to electronic commerce are not regulated in this way, although complaints could be made to the Australian Securities and Investments Commission where a breach of the Corporations Law is involved, or the Australian Competition and Consumer Commission, if a breach of the Trade Practices Act and certain other pieces of legislation is involved. These latter two agencies have primary responsibility for regulating commercial transactions, including those that take place online.

5.2 Fraud Control Policies

Other policy initiatives that have relevance to the control of Internet fraud lie within the realm of fraud control policies generally. Fraud control policies are now increasingly being used in both the public and private sectors. In Australia, for example, the fraud victimisation survey conducted by Deakin University in 1994, found that 27 per cent of those surveyed had fraud prevention policies in place (Deakin University 1994). In November 1995, 48 per cent of the 123 Australian respondents to Ernst and Young's fraud survey had a fraud prevention policy in place and 51 per cent had conducted fraud reviews (Ernst and Young 1996). In Ernst and Young's (1998) subsequent fraud survey, almost three quarters of the 84 Australian respondents indicated that their organisation had an explicit policy on fraud reporting (1998).

One half of the respondents to KPMG's Global eFraud survey (2001) had incident response procedures in place to deal with security breaches of their electronic commerce systems—although of those respondents who had procedures in place, 43 per cent had procedures that included computer forensic response guidelines to deal with wilful intrusions into their networks and to ensure proper gathering of evidence. Over 50 per cent of the Asia-Pacific respondents—from each of Australia, Hong Kong and India—all had procedures in place to deal with security breaches, somewhat higher than in other countries.

Various standards have been designed to assist business and government in the creation and use of fraud control measures. Australian Standard No. AS 3806-98 Compliance Programs, for example, provides guidelines for both private and public sector organisations on the establishment, implementation and management of effective compliance programs. The Standard also provides principles which organisations are able to use to identify and to remedy any deficiencies in their compliance with laws, industry codes and in-house company standards, and to develop processes for continuous improvement in risk management (Standards Australia 1998).

Most government agencies now have detailed fraud control policies in place which provide guidelines on the establishment, implementation, and management of agencies in order to reduce fraud risks (see, for example, the Fraud Control Policy of the Commonwealth of Australia; Attorney-General's Department, Australia 2001). There has also been recognition in recent times of the need to create an ethical environment in the workplace by educating employees of all levels about the desirability of complying with laws and codes of practice.

Policies, however, need to be established to deal with specific computer-related matters such as Internet fraud. Both businesses and government agencies should establish guidelines, for example, on the allocation and use of passwords, on access to and use of the Internet for private purposes, personal use of email, downloading government software, the use of copyright material, and reporting of inappropriate conduct. In Australia in March 2000, the Office of the Federal Privacy Commissioner (2000) published guidelines on workplace email, web browsing and privacy. These guidelines aim to assist public sector agencies in developing appropriate workplace practices regarding the use of information technologies by employees. These generally require openness in agencies communicating

with staff about what is, and what is not permitted in the workplace. They also require agencies to inform staff about the nature and extent to which their computer-related activities are logged and who in the organisation has access to the logged information.

An example of the kind of difficulties that can arise in applying policies concerning the use of email, came before the Federal Court of Australia in April 2000. In that case, an employee of Ansett Australia was dismissed for having, as a union delegate, distributed a union bulletin to other union members using Ansett's internal email system. Ansett's policy on the use of email by staff permitted use 'for the purpose of performing authorised lawful business activities'. Although Ansett argued that the distribution of the bulletin did not fall within the terms of this policy, the court held that the employee had implied authorisation to use the internal email system for this purpose. It was accordingly decided that she had been improperly dismissed because of her union activities in contravention of the *Workplace Relations Act 1996* (Cwlth) (*Australian Municipal, Administrative, Clerical & Services Union* v *Ansett Australia Ltd* [2000] FCA 441, Federal Court of Australia, 6 April 2000, Merkel J).

5.3 Codes of Practice

In addition to having fraud control policies in place as part of a general risk management strategy, codes of practice are able to provide not only a widely disseminated statement of existing laws and acceptable practices which help to create a culture of compliance within specific industries, but also often include dispute resolution procedures and sanctions for non-compliance with the rules in question. Although many countries now have codes of practice to regulate online activities, the following discussion, drawn from Grabosky, Smith and Dempsey (2001), will focus primarily on Australia which has been a leader in this area, particularly in codifying desirable practices on the Internet.

Codes of practice established by the marketing and media industries in Australia have targeted particularly vulnerable groups of consumers such as children, as well as specific content and products such as obscene materials, therapeutic goods, tobacco and alcohol. The Media Council of Australia, for example, administers a variety of voluntary codes of practice relating to advertising of therapeutic goods, slimming products, alcohol and tobacco products (see Pearson 1996).

The Australian Competition and Consumer Commission has developed Guidelines for Advertisers, while State and Territory departments of consumer affairs also have guidelines on complying with local laws such as those relating to the protection of privacy. Some industry groups also have their own codes of practice such as the Australian Publishers' Bureau Advertising Code of Practice which sets out its requirements for acceptable advertising in six short paragraphs. These codes and guidelines reflect the provisions of the general law and do not take away rights which consumers have under existing legislative regimes. They also often operate across traditional jurisdictional boundaries which increases the possibility of uniform practices emerging.

In December 1997, the Australian Ministerial Council on Consumer Affairs released the Direct Marketing Model Code of Conduct to regulate the conduct of those involved in the direct-selling industry. The Code is administered by the Australian Direct Marketing Association (ADMA) which was established in 1966 as the peak industry body for companies and individuals engaged in direct marketing in Australia, and applies to telemarketing, mail-order and Internet sales. Membership of ADMA is open to corporations, organisations, charities and partnerships, whilst individuals are able to join as Associate members. In 1996, ADMA began providing a training program in competency-based direct marketing at certificate and diploma levels.

All ADMA members must undertake to abide by the voluntary Direct Marketing Code of Practice published by the Association which seeks to ensure that direct marketing engaged in by members complies with the highest standards of integrity. The 'Standards of Fair Conduct' within the Code govern the making of an offer, identification of the advertiser, the use of incentives, the placing of orders, fulfilment of orders and the use of mailing and telephone lists. Arrangements are also made for the arbitration of disputes and members agree to comply with all legal requirements governing their activities.

The Code also specifically refers to direct marketing carried on electronically, such as via the Internet. The Code states, for example:

> *Clear, complete and current information about the identity of businesses engaged in electronic commerce and about the goods and/or services they offer, should be provided to customers. Additional information should be provided to address particular aspects of digitised goods and services, such as technical requirements or transmission details (cl. D2).*

Of particular concern is the problem of online advertising directed at children, as it is they who are often attracted to advertising material and are likely to be misled. Some responsible businesses are aware of the problem, such as Motorola (which sells mobile telephones) whose site contains the following message (Motorola 2001):

> *Motorola products and services are directed at an adult market, and therefore this site is intended for use by adults only. Motorola encourages parents to take an active role in their children's use of the Internet, and to inform them of the dangers of providing information about themselves over the Internet. No information should be submitted to or posted on this web site by users under 13 years of age without the consent of their parent or guardian.*
>
> *Users that Motorola knows to be under the age of 13 are required to provide the email address of their parent or guardian so that Motorola may alert the parent or guardian of their child's use of this web site. The parent or guardian must consent to Motorola's collection of their child's personal information. A known child user will be restricted from providing personal information until such consent is received. No information collected from users known to be under age 13 will be used for any marketing or promotional purposes outside Motorola, Inc.*

Failure to comply with the code may result in members' conduct being investigated by a Code Authority established by the Association. Sanctions include orders requiring members to take remedial action or give an undertaking not to repeat the breach of the code, to issue a formal written admonition and / or to publish that admonition for serious breaches of the code, or to recommend revocation of membership.

Internet service providers have also established a variety of industry-based organisations, a number of which have their own codes of practice. The Internet Industry Association, for example, has a code of practice (Version 4.2 of 12 February 1999) which was based on generally accepted international standards, such as Australian Standard AS-4269-1995, a wide range of existing and related codes, the Ministerial Council of Consumer Affairs' Guide to Fair Trading Codes of Conduct and various regulatory schemes in related industries.

A number of local groups within Australia also have Codes such as the South Australian Internet Association's Code of Ethics and Conduct and the Western Australian Internet Association's Code of Conduct. Similarly, the

Committee of Australian University Directors of Information Technology have a Code of Practice relating to content that may infringe censorship laws which not only sets out guidelines for ISPs but also for content providers and service users as well. There remain, however, many industry groups which have yet to agree on codes of practice (see Clarke 2001).

In addition, in Australia, an Internet Code of Conduct has been created to deal specifically with business-to-consumer electronic commerce transactions. The code, *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business* (Department of Treasury, Consumer Affairs Division 2000), builds on the recommendations of the Council of the Organisation for Economic Cooperation and Development (OECD, 1999) concerning guidelines for consumer protection in the context of electronic commerce. These OECD recommendations include a set of general guidelines to protect consumers participating in electronic commerce without erecting barriers to trade. They represent a recommendation to governments, businesses, consumers and their representatives as to the core characteristics of effective consumer protection for electronic commerce.

The Australian Best Practice Model sets out the responsibilities of businesses that trade online and provides guidance to businesses for enhancing consumer sovereignty by giving consumers information on what businesses should do when dealing with consumers over the Internet. The Best Practice Model aims to increase consumer confidence in business-to-consumer electronic commerce and provides guidance to industry and consumers on the elements of an effective self-regulatory framework. The model provides guidance on:

- fair business practices;
- advertising and marketing;
- disclosure of a business's identity and location;
- disclosure of a contract's terms and conditions;
- the implementation of mechanisms for concluding contracts;
- the establishment of fair and effective procedures for handling complaints and resolving disputes;
- adopting privacy principles;
- using and disclosing information about payment, security and authentication mechanisms; and
- the processes and policies necessary to administer a code based on the Best Practice Model.

This model could provide a basis for the development of similar guidelines for business-to-business and government-to-business electronic commerce in the region.

In the United Kingdom in 1995, the Internet Service Providers' Association was formed to represent the interests of those within the industry. Over 80 companies involved in the provision of Internet services are now members, representing some 90 per cent of the dial-up market. Included are ISPs, Internet access providers, network solution managers, web designers, Internet watchdog bodies such as the Internet Watch Foundation and also multimedia law practices.

The Internet Service Providers' Association established a voluntary code of practice in May 1996 (the current version of which is dated 25 January 1999) which sets out the responsibilities of members in ensuring that their services are not used for illegal and unethical purposes. Complaints procedures are specified and a range of sanctions included for failure to comply with the code.

In Britain, the New Media Council was set up by the Direct Marketing Association to act as a forum for those who market across non-broadcast electronic media, including the Internet whilst British Codes of Advertising and Sales Promotion Codes from the Advertising Standards Authority, Direct Marketing Association and Independent Committee for the supervision of Standards of Telephone Information Services all provide specific guidelines on acceptable conduct with respect to their own areas of interest. With such a proliferation of guidelines, part of the challenge lies in establishing which organisation is the most appropriate to be involved in any specific case.

The possible application of the Control of Misleading Advertisements Regulations 1998 (Eng) to Internet trading is currently under debate in Britain. Internet service providers argue that, like a telecommunications or postal company, they are providing the medium but should not be held responsible for the messages people transmit.

Non-compliance with codes of practice is an area of continuing concern as some organisations have few, if any, consequences for failure to comply with the provisions of their code. Occasionally consequences of non-compliance are provided for, such as in the *Fair Trading Act 1987* (New South Wales), section 74 of which provides that failure to comply with an industry code of practice may result in the agency requiring the individual to give an

undertaking to discontinue the offending conduct, to comply with the code in the future, or to take action to rectify the consequences of the contravention. Stronger consequences may involve suspension or disqualification of the offending person from continuing membership of the industry group in question which could entail substantial financial repercussions.

In Australia, in April 1998, Part IVB (ss. 51ACA to 51AE) was inserted in the *Trade Practices Act 1974* (Cwlth). These provisions permit industry codes of conduct, whether mandatory or voluntary, to be enforceable under the Act, with legal action able to be taken for breaches of the codes, or specified parts of them. The first code to be mandated under Part IVB was the Franchising Code of Conduct, with effect from 1 July 1998. Hopefully, codes governing online misleading and deceptive practices will come within the jurisdiction of the Act in the future.

The principal limitation with codes of practice as a regulatory mechanism is that their operation is limited to those who have agreed to comply with their provisions. Although this may be adequate for large organisations such as those which regulate direct marketing, the controls are usually restricted to specific geographical regions. In the world of online marketing and advertising in which information travels so easily across borders, the possibility of consumers being misled by information from some overseas entity is greatly increased. The possibility also arises of conflicting guidelines having been established in different countries to regulate essentially similar activities.

In the global electronic commerce marketplace, ideally international codes of practice will need to be agreed upon by groups representing essentially similar interests. One could imagine, for example, that an international code of practice could be created which would apply to all entities engaging in electronic commerce throughout the world. As already noted, OECD countries have acted to create a set of guidelines to enable self-regulatory regimes to be constructed along similar lines in different OECD countries (Bridgeman 1997). The problem which uniform international codes of practice face is ensuring that local public sentiment can be accommodated in setting standards. In regulating obscene and objectionable content, for example, this has proved to be a considerable hurdle (Butler 1996). In the field of misleading and deceptive practices, however, international consensus might be more easily achieved.

6 Investigatory Framework

6.1 Problems of Investigation and Policing

Many problems arise in investigating cases of electronic fraud as they often involve the use of highly sophisticated techniques of deception and planning. Offenders often go to considerable lengths to disguise their identity and to make financial trails of evidence difficult to follow.

Those who seek to mask their identity through the use of computer networks are often able to do so, by means of 'looping', or 'weaving' through multiple sites in a variety of nations. Electronic impersonation, colloquially termed 'spoofing', can be used in furtherance of a variety of criminal activities, including fraud. Anonymous remailers and encryption can shield one from the scrutiny of all but the most determined and technologically sophisticated regulatory and enforcement agencies. As a result, some crimes may not result in detection or loss until some time after the event, thus making the process of investigation even more challenging.

Other issues which may complicate the investigation of computer-based fraud entail the logistics of search and seizure during real time, the sheer volume of material within which incriminating evidence may be contained, and the encryption of information, which may render it entirely inaccessible, or accessible only after a massive application of decryption technology. In a recent investigation by the New South Wales Independent Commission Against Corruption into allegations that two State Government employees had downloaded and exchanged child pornography at their office workstations, much of the material was unable to be used in evidence as it was in encrypted form (Bell 2000, p. 34, n. 68).

In this often highly technological area, law enforcement agencies invariably need specially trained units to handle investigations. In some cases, forensic accountants from the private sector may be engaged by police fraud squads to carry out investigations, or part of investigations. In other cases, independent statutory anti-corruption agencies may take action; and they, too, may need to develop expertise in this area. In New South Wales, for example, the Independent Commission Against Corruption is developing a

new strategy, *Project Mercury*, to deal with electronic corruption and already a number of its investigations have involved cases of electronic fraud (Bell 2000).

Taking criminal action in cases involving electronic fraud is neither simple nor quick. Financial considerations have also meant that only the most serious cases involving substantial monetary losses are likely to be fully investigated and tried, with the attendant possibility of convicted offenders receiving the most severe sanction of a term of imprisonment. The legal response to fraud control has, therefore, been severely restricted, although the possibility of criminal prosecution and sanction has always remained open.

Although computer technologies may make some aspects of fraud investigation difficult, they may also be able to assist law enforcement officers. Computers, for example, are able to handle with ease substantial quantities of evidence and complex financial records which cases of serious fraud entail, and are also able to record patterns of conduct used in previous cases which facilitate the identification of repeat offending by the same individual or others utilising the same fraudulent techniques.

In the Asia-Pacific region, however, problems sometimes emerge in dealing with Internet fraud investigations owing to police being under-resourced in terms of forensic computer capabilities. In the case referred to above involving two Indian computer trainers who allegedly sought to obtain access to the State Bank of India, it was reported that police were hampered during the investigation owing to an absence of computers to analyse the transactions. Lawyers and the courts were also unfamiliar with the forensic issues that the case raised (Bloomberg News 2001).

6.2 Trans-jurisdictional Problems

Because electronic fraud often does not involve face-to-face communication, it is possible for offenders and victims to be located in more than one jurisdiction. More sophisticated conspiracies may involve individuals in three or more jurisdictions within Australia or overseas. Few remedies are available to agencies that fall victim to such activities. Even if one is able to mobilise the law, the chances of locating the fraudsters, obtaining extradition, mounting a prosecution, or recovering compensation may be impossible.

Even where a perpetrator has been identified, two problems arise in relation to the prosecution of offences which have an international aspect: first, the determination of where the offence occurred in order to decide which law to apply; and, second, obtaining evidence and ensuring that the offender can be located and tried before a court. Both these questions raise complex legal problems of jurisdiction and extradition.

Although many of the legal and procedural impediments to the successful prosecution of electronic forms of fraud have been removed, a number of practical difficulties still remain. The most problematic relate to cost and delay in cases of extraterritorial law enforcement which makes some prosecutions practically impossible. Moreover, cooperation across international boundaries in furtherance of such enforcement usually requires a congruence of values and priorities across nations which, despite prevailing trends towards globalisation, exists only infrequently.

6.3 Regional Initiatives

Throughout the 1990s, a number of initiatives have taken place to address the problem of computer-related crime globally. In the Asia-Pacific region, a Working Group on Information Technology Crime was established in the region which reports to the INTERPOL Steering Committee on Information Technology Crime. The Australasian Centre for Policing Research has acted as chair of the regional working group and conducted an extensive analysis of the law enforcement issues arising out of electronic crime in its scoping paper entitled *The Virtual Horizon: Meeting the Law Enforcement Challenges* (2000).

In addition, the Research Group into the Law Enforcement Implications of Electronic Commerce has conducted a number of studies into electronic crime, principally with an Australian focus, although having relevance to the region generally.

Other international initiatives have been the work of the Expert Group on Crimes Related to the Computer Network chaired by the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI 2000).

According to Gilley and Crispin (2000, p. 50):

> *law enforcement agencies in the Asian region are hamstrung by a lack of resources and an absence of law to tackle the problem—more so than their counterparts in the United States and Europe.*

Computer security officials from this region indicate a massive effort is required from governments to enact new laws, bolster the forces of fighting computer crime, educate people and companies about cybercriminality, and enhance cross-border cooperation (Australasian Centre for Policing Research 2000, p. 83).

In Hong Kong, for example, the Commercial Crimes Bureau has found that cases of computer crime reported to it have increased from 25 incidents in 1997 to 89 in the first five months of 1999. Incidents of alleged computer hacking increased from seven incidents in 1997 to 51 in the first five months of 1999. Most of the recent cases prosecuted by police in Hong Kong involved music piracy and fraudulent use of credit card information on the Internet (Farber 1999).

In another initiative in the United States, the Federal Bureau of Investigation and the National White Collar Crime Centre have co-sponsored the establishment of a central repository for complaints relating to Internet fraud. The Internet Fraud Complaint Centre (IFCC) hopes to ensure that Internet fraud can be addressed at all levels of law enforcement (local, state, and federal).

The IFCC was created to identify, track and investigate new fraudulent schemes on the Internet on a national and international level. IFCC personnel collect, analyse, evaluate and disseminate Internet fraud complaints to the appropriate law enforcement agency. The IFCC provides a mechanism by which Internet fraud schemes are identified and addressed through a criminal investigative effort. The IFCC also provides analytical support, and aid in the development of training modules to address Internet fraud. The information obtained from the data collected provides the foundation for the development of a national strategic plan to address Internet fraud.

In 1996, the G-8 countries established a group of experts (‘The Lyon Group’) to examine better ways in which to fight international crime. The group produced 40 recommendations that were endorsed by the G-8 heads of state

at the Lyon Summit in June 1996. This group has met regularly and has discussed ways of enhancing the ability of law enforcement agencies to investigate and prosecute international crime. In January 1997 it created a sub-group to look specifically at high-technology crime and this sub-group has examined law reform, investigatory and procedural issues to do with prosecuting cross-border computer crime (Sussmann 1999).

The G-8's High-Tech Crime Group, as it is known, has also recommended the establishment of cooperative arrangements between public sector police and regulatory agencies and the private sector. For example, there is a need for telecommunications carriers and ISPs to make certain information available to investigators on production of an appropriate search warrant. Ideally, such arrangements need to be uniform across jurisdictions.

One example of a cooperative venture involving public and private sector bodies is the Cybercrime Unit created by the International Chamber of Commerce's Commercial Crime Bureau in London in 1999. This brings together law enforcement bodies such as Interpol, Scotland Yard and the FBI, as well organisations within the private sector including major financial institutions and businesses. The Unit acts as a clearinghouse for information on electronic crime and passes details of frauds and solutions between companies and the police.

6.4 Specialist Law Enforcement Agencies

Recognising the highly specialised knowledge and skills required for investigation and evidence gathering in relation to cybercrime, a number of countries have moved towards establishing specialist computer crime police agencies.

The Australian Federal Police has an Electronic Evidence Team of 12 federal agents who deal specifically with electronic crime. Cases referred to the Team for investigation have grown in seriousness and sophistication in recent years in addition to the number of cases referred more than doubling annually.

In Canada, the Royal Canadian Mounted Police (RCMP) is responsible for the investigation of all computer crime offences within its jurisdiction, as well as those where the Government of Canada is the victim regardless of the source of the offence, as well as offences involving organised crime or affecting the national interest. Commercial crime sections of the RCMP

operate in every major city in Canada, and contain at least one investigator trained in the investigation of computer crimes. These investigators are supported by the RCMP High-Tech Crime Forensics Unit (HTCFU) located at RCMP Headquarters in Ottawa. Technical guidance and expertise from HTCFU is also offered to all Canadian police departments and federal government agencies in relation to computer and telecommunication crime investigation (RCMP 2001).

The Hong Kong Police Crime Prevention Bureau (2001) has established a Computer Security Unit (CSU) whose primary duty is:

> *to provide the means to educate the public of Hong Kong on matters relating to computer security. This will entail providing advice and guidelines … to advise computer users of ways to secure both their data and equipment from the more common computer security threats.*

The CSU targets hacking, Internet pornography and gambling as well as computer and Internet fraud (Buddle 2001).

In India, the Central Bureau of Investigation is the premier law enforcement agency of the Government of India for the investigation of corruption cases, economic crimes and special crimes. It also coordinates investigations on behalf of Interpol member countries and State police agencies. On 3 March 2000, the CBI established a Cyber Crime Investigation Cell which is headed by a Superintendent of Police and has one Deputy Superintendent of Police, three inspectors and one sub-inspector, in addition to other supporting staff. The jurisdiction of the cell extends throughout India, and besides offences punishable under Chapter XI, of the *IT Act 2000*, it also has power to look into other high-tech crimes (Central Bureau of Investigation, India 2001).

In Japan, a HITEC (Hi-tech Crime Technical Expert Centre) was established in 1999 to act as a 'Cyber Police Force' by the National Police Agency (NPA Japan 1998). The National Police Agency has arrested six people on suspicion of Internet fraud since the new law banning unlawful access to the global online network came into force in February 2000. In a report presented to a meeting of the National Public Safety Commission, the NPA said the arrests were among 35 cases of Internet fraud handled by police across the country since the law was introduced. In 15 of the 35 cases, charges related to unauthorised changes being made in web site contents or unauthorised use of user identities and passwords (Japan Times Online 2000).

A Cyber Terrorism Response Centre operates within the Korean National Police Agency, and the establishment of a General Investigation Centre of Computer Crimes under the Prosecutor-General's Office was recently announced (*Korea Herald*, 17 November 2000).

The Philippines' National Bureau of Investigation (NBI) has also established an Anti-Fraud and Computer Crimes Division (AFCCD), which has been active in enforcing the new hacking and piracy provisions of the *Electronic Commerce Act 2000* (Villafania 2001).

On 8 August 2000, the official Chinese news agency Xinhua announced that some 20 Chinese provinces and cities were setting up Internet police brigades to 'administer and maintain order' on computer networks. Their mission is to censor anti-governmental, pornographic or simply 'negative' information, such as reports on corruption. Shortly thereafter, the first specialised brigade was created in the eastern province of Anhui. According to the official press, in several weeks they solved a series of 'online crimes', ranging from 'fraud' to 'pornography', and helped set up Internet filters to protect children (Reporters Sans Frontières 2001).

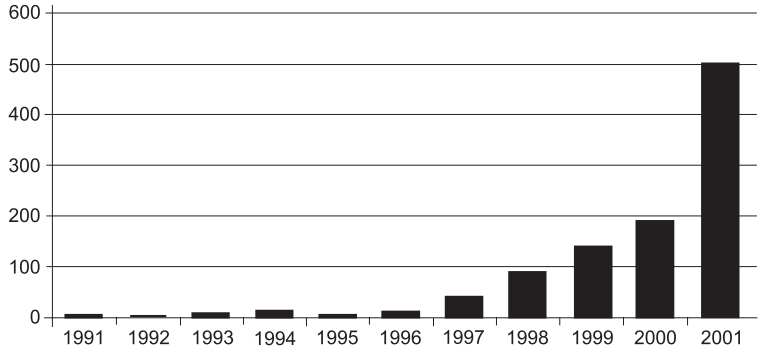
In Australia, both the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) are involved in identifying and protecting against Internet fraud. In 1997 the ACCC oversaw an international effort involving 25 countries (including Canada, Japan, Korea, New Zealand and the Philippines) targeting 'get rich quick' schemes on the Internet (FTC 1998, p6). The Australian Investments and Securities Commission established an Electronic Enforcement Unit in the late 1990s to deal specifically with online fraud. Since it was established the number of matters referred for investigation has increased over 500 per cent to 50 matters a quarter in July 2000.

In New Zealand, the government plans to establish a dedicated unit within the Government Communications Security Bureau to detect and monitor online security threats, principally relating to the transmission of viruses and instances of unauthorised access. The Centre for Critical Infrastructure Protection will coordinate security programs in both the public and private sectors in New Zealand and will provide a 24-hour service to alert infrastructure providers of intrusions (Creed 2001).

6.5 Resources Devoted to Investigating Internet Fraud

Even in developed countries such as Australia, the resources devoted to policing the Internet are insufficient to cope with the number of crimes being reported. Many law enforcement agencies have reported increased instances of Internet-related crime being reported to them for investigation. Although not all computer crime cases referred to the Australian Federal Police involved Internet fraud, over the last 10 years the computer crime caseload has increased substantially as we can see from Figure 11 (see Geurts 2000).

Figure 11: Number of computer crime referrals to the Australian Federal Police, 1991–2001



Note: 2001 is estimated only
Source: Geurts 2000

Law enforcement agencies have generally found the investigation of such cases to be costly, slow, and difficult. There have been relatively few successful prosecutions and sentences have tended to be in the lower range of severity for white-collar offences. In the past, police computer crime squads tended to be composed of interested amateurs who acquired considerable experience and expertise during the course of investigations. Often their skills were recognised by the private sector to which they invariably gravitated in the pursuit of more remunerative positions. More recently, however, police services have begun to recruit highly-trained personnel to deal specifically with computer crime. Whether they remain within public sector law enforcement, however, remains to be seen.

6.6 Mutual Assistance

International cooperation amongst national law enforcement agencies faced with the borderless problem of cybercrime is beginning to emerge. For example, INTERPOL has established a series of working parties organised around world regions, including the Asia-Pacific Working Party on Information Technology Crime (INTERPOL 2001):

> *This working party conducted its second meeting which was hosted in India during November 2000 and was attended by representative from Australia, China, Hong Kong China, India, Japan, Nepal and Sri Lanka. This working party has accepted the model of the European working party in principle and has taken initiatives in the region on a project basis. The working party has especially recognised sharing expertise in the region and seeking practical standards for the region, as a priority at the current stage. According to the concept, three projects (intelligence scoping project, forensic project and training project) have been launched so far. The group has agreed to meet once a year, utilising an email-based reporting system to update progress on the projects.*

The Australasian Police Commissioners' meeting held in Adelaide in March 2001 announced a regional cooperative strategy aimed at targeting cybercrime (NZPA 2001).

6.7 Forensic Computing and Accounting

A private sector organisation operating throughout the region is the Civil Investigation Agency incorporated in the United Kingdom but based in Islamabad, Pakistan. This company conducts investigations into fraud and related matters for clients throughout the region and represents an example of inter-jurisdictional cooperation that is required for investigating Internet-related economic crimes.

The Hong Kong University of Science and Technology has recently instituted Hong Kong's first postgraduate diploma courses in computer forensics, among the first such programs in Asia. The courses are based on those available in the United States, Canada and Britain, but have been adapted for the region's legal and software systems (Pawlyna 2001).

6.8 Specialist Legal Expertise

Increasingly, law firms and legal practitioners are tending towards specialist expertise in areas relating to intellectual property, electronic commerce and the Internet. Among international law firms offering such expertise and maintaining a strong presence in the Asia-Pacific region are Gilbert & Tobin (Australia), Ladas & Parry (United States and international), and Baker & McKenzie (international). The latter offers a useful news service on legal developments in cybercrime and electronic commerce covering many countries in the Asia-Pacific region (Baker & McKenzie 2001).

Globalisation of legal practice will greatly expand the opportunities for specialist legal advice to be available throughout the region. Already, for example, six Australian law firms now practice in China with China being Australia's third largest overseas legal services market after the United States and the United Kingdom (Williams 1999, p. 63). In addition, the Internet itself is becoming an effective means of disseminating legal advice. One of the largest English firms of solicitors now provides online information and advice about local laws, regulations and other details to global investment banks operating in Europe, the United Kingdom and Asia for a yearly fee of up to £125,000 for unlimited access to the service (Gray 1999, p. 89).

In a 1998 survey conducted of Victorian legal practitioners, 2,684 responses were obtained out of 8,500 surveys distributed by the Law Institute of Victoria (Kriegler 1999). Forty-four per cent of respondents indicated that they had access to the Internet on their desks, 57 per cent had Internet access elsewhere in their office and 35 per at home. Forty-eight per cent of respondents used the Internet for legal research, 57 per cent for electronic mail and 37 per cent for web browsing (Kriegler 1999, p. 55).

A less formal way of offering specialist legal expertise has emerged with the establishment of a non-profit group in Japan, called 'Shirogane Cyberpol', which involves lawyers, scholars, bureaucrats and others providing free advice on Internet problems such as libel and fraud (Japan Times Online 2001).

7 Legal Framework

7.1 Legal Problems

A variety of legal problems arise in prosecuting Internet fraud. These relate to the multiplicity of rules that exist in the various jurisdictions and the fact that many of the rules are complex, unclear and contradictory. A range of different approaches have been taken to law reform throughout the region in order to accommodate electronic transactions with some parliaments enacting highly specific reforms to define words such as 'documents', 'writing', and 'signatures' as well as to specify the rules which govern the attribution of communications.

In Australia, a more generalised approach has been adopted with the enactment of broad, technology-neutral provisions which constitute a basis for more specific legal changes which will be introduced subsequently. In addition, the Model Criminal Code Officers Committee (2000) in its discussion paper on computer crimes and jurisdiction has addressed many of the problems that arise in prosecuting crimes of dishonesty committed electronically. The draft Model Code provisions have been enacted (with minor variations) or are currently before legislatures in several Australian jurisdictions: *Crimes Amendment (Computer Offences) Act 2001* (NSW); *Cybercrime Bill 2001* (Cwlth) (see also Ellison 2001a, 2001b; Weir 2001). There remain, however, a number of forensic difficulties associated with gathering evidence from computers in a number of different jurisdictions that often make proceedings both difficult and costly.

Only some of the remaining Asia-Pacific jurisdictions incorporate specific fraud and forgery offences into their main computer crime legislation. An example is sections 246–2 of Japan's Computer Crime Act under the Penal Code, which relates to intentionally obtaining a profit by introducing false information or wrong instructions into any computer system used in the course of business transactions (Natsui 1998). Similarly in Canada, under section 342.1 of the Criminal Code, fraudulent use of or interference with computer systems is an indictable offence punishable by 10 years' imprisonment (Canada 2001).

It should be stressed, however, that fraud and forgery can usually be prosecuted under the commercial and criminal laws of most jurisdictions whether committed using a computer or by more traditional paper-based means. In addition, many countries within the Asia-Pacific region have enacted laws governing electronic transactions, digital signatures and other aspects of electronic commerce. To varying degrees, this type of legislation also apportions liability in the case of fraudulent use or circumvention of technological protections.

7.2 Court Processes

There are also numerous problems associated with conducting criminal trials in cases involving electronic fraud. The principal difficulties relate to the presentation of computerised business and accounting records to a court, the difficulty of presenting complex financial transactions to a jury in such a way as to permit lay people, perhaps unfamiliar with the technologies used, to understand the factual issues involved, and the length of time which such trials take, which is often exacerbated in cases of criminal conspiracy by having multiple defendants and multiple charges.

Various reforms to court procedures have been introduced throughout the region in recent years to reduce the length, complexity and cost of prosecutions, particularly those which involve substantial sums of money or complex factual circumstances. Computer technology, for example, has greatly facilitated the presentation and analysis of complex business dealings in some courts. In addition, legal practitioners are often closely regulated with respect to the length, manner and nature of material which they present to the courts.

In view of the complexities associated with the conduct of criminal trials involving allegations of electronic fraud, it is necessary for all those involved to be thoroughly trained in carrying out their various duties in an efficient and effective way. Witnesses, particularly forensic accountants, need to be trained in the presentation of technical information to courts and juries in much the same way as expert medical witnesses have specialised in presenting complex medical testimony in clear and simple terms to courts. Legal practitioners also need to be trained not only in the particular evidentiary and procedural rules which apply in such cases, but in liaising effectively with accountants and financial advisers, particularly when

presenting lengthy and complex computer-based financial records. Just as specialist groups of lawyers now exist for dealing with such cases, so a specialist judiciary needs to be established in order to ensure that judges with appropriate experience and financial and information technology skills are allocated to these trials. Finally, jurors and those lay witnesses who give evidence in such cases should be provided with information which will enable them to understand the latest court procedures and arrive at decisions in an efficient manner.

7.3 Law Reforms Already Undertaken

A recent report on cybercrime laws in 52 countries assesses the following Asia-Pacific countries as having updated their laws in relation to the prosecution of cybercrime: Australia, China, Japan, Malaysia, and the Philippines. New Zealand is assessed as being in the process of developing such laws (McConnell International 2000). The basis used for comparison was a list of:

> *Ten different types of cyber crime in four categories: data-related crimes including interception, modification, and theft; network-related crimes, including interference and sabotage; crimes of access, including hacking and virus distribution; and associated computer-related crimes, including aiding and abetting cyber criminals, computer fraud, and computer forgery.*

However, the McConnell International report itself notes that such crimes are not treated uniformly across countries, or even in some instances within countries (such as Australia, which has both Federal and State laws in relation to unauthorised computer access), and that penalty levels vary widely.

In Australia, various Federal and State / Territory laws prohibit the use of computers for fraudulent purposes. An example is section 135L of the *Crimes Act 1900* (Australian Capital Territory), which prohibits 'dishonest use of computers' and imposes a maximum term of imprisonment of 10 years. A new Cybercrime Bill 2001 was introduced in the Australian Federal Parliament on 27 June 2001 (Ellison 2001a, 2001b). If enacted, this Bill will significantly revise Commonwealth computer offences, imposing a maximum penalty of 10 years' imprisonment for offences including (s. 477.1) unauthorised computer access, (s. 477.2) modification or impairment with

intent to commit a serious offence, unauthorised modification of data to cause impairment, (s. 477.3) and unauthorised impairment of electronic communication (Parliament of the Commonwealth of Australia 2001).

Internet regulation in China relies on both specific laws and administrative pronouncements. It has been noted (Clarke 1999, p. 33) that:

> *a sharp distinction between law and policy does not exist in China. Stated government policy can have exactly the same effect as formally enacted legislation.*

The situation until quite recently was as described below (Bao 2000):

> *In China, most of the regulations governing the net are administrative or procedural ones. Only a few clauses in the Criminal Law make a clear-cut definition of net crime. These administrative and procedural regulations play a certain role in strengthening management of the network. But they only set standards for protection of the safety of computer information systems, the supervisory right, and users' obligations. The issues they can handle are just safety of the computer system and intrusion of the network. Detailed and comprehensive regulations on the net in such substantive law as the Civil law and the Criminal law haven't yet been formulated.*

On 28 December 2000, the 19th Session of the Standing Committee of the Ninth National People's Congress of China passed a resolution on maintaining security of computer networks. The resolution made it a criminal offence to carry out a range of computer-related activities. Those relating to Internet fraud include selling fake or substandard products, advertising goods and services in a deceitful way through the Internet, infringing the intellectual property of others through the Internet, fabricating false information affecting securities and futures trading or otherwise disturbing the financial order through the Internet, and committing theft and fraud through the Internet (Zhongguo Xinwen She 2000).

Clearly this resolution can be applied to cases of Internet fraud. It remains to be seen whether significant prosecutions of offences under these provisions will follow.

Hong Kong retains its own criminal laws pertaining to computer misuse. Under section 85 of the Crimes Ordinance (cap. 200), the offence of falsification of bank computer records carries a penalty of life imprisonment;

while under section 19 of the Theft Ordinance (cap. 210), a 10-year sentence may be imposed for the offence of false accounting by falsifying computer records. Other provisions of these laws cover criminal damage to computers and unlawful interference with computers (Urbas 2001).

India is one of a small number of countries with a specific statute on cybercrime. On 17 May 2000, India's parliament passed the *Information Technology Act 2000* (Ministry of Information Technology, India 2001). This law criminalises unauthorised access to electronic information (s. 43), tampering with computer source documents (s. 65) and hacking (s. 66). These offences are punishable by fines and sentences of up to three years' imprisonment and the law allows police officers to search the homes or offices of Internet users, at any time and without a warrant, and to close a cybercafé if they consider that a computer crime is being committed there (Reporters Sans Frontières 2001). Publishing obscene information in electronic form (s. 43) carries a maximum penalty of five years' imprisonment and fines, while unauthorised access to a protected computer system is punishable by 10 years' imprisonment and unspecified fines (Urbas 2001). The *Information Technology Act 2000* also provides for the establishment of electronic commerce through electronic signatures using public key cryptography (Mehta 2000).

Japan's Unauthorised Computer Access Law of 1999 is designed to 'prevent computer-related crimes that are committed through telecommunication lines and to maintain the telecommunications-related order that is realised by access control functions, and, thereby, to contribute to the sound development of the advanced information and telecommunications society' (National Police Agency 2000). Unauthorised computer access is punishable by one year's imprisonment or a fine of up to ¥500,000. Under the Computer Crime Act of the Japanese Penal Code, computer-related forgery (s. 161) and computer fraud (s. 246) each carry a maximum penalty of five years' imprisonment (Urbas 2001).

Korea has had legislation in place governing electronic commerce since 1999 (Reuters 1999). The legislative scheme includes criminal penalties for computer misuse ranging up to five years' imprisonment or fines of 50 million won (Urbas 2001).

In 1997, Malaysia passed a package of four new 'cyberlaws': the Computer Crimes Act, Digital Signatures Act, the Copyright (Amendment) Act and the Telemedicine Act. Section 4 of the *Computer Crimes Act 1997* creates a specific

offence of unauthorised access to a computer with intent to commit an offence involving fraud or dishonesty (Ministry of Energy, Communications and Multimedia, Malaysia 2001). Unauthorised access (s. 3) carries a maximum penalty of five years' imprisonment and / or fines up to RM50,000, increasing to 10 years and RM150,000 (s. 4) if with intent to commit a further offence (Urbas 2001).

The New Zealand Parliament is currently considering the Crimes Amendment Bill (No. 6), which would amend the Crimes Act by adding specific offences in relation to activities such as hacking and Internet fraud (Swain 2000; NZPA 2000).

The government of Pakistan is reportedly also considering a proposal for the drafting of a new Computer Crimes Act (Suddle 2000).

In mid-2000, the Philippines legislature enacted a new *Electronic Commerce Act 2000* (Department of Trade and Industry, Phillipines 2000; Gana 2000). Under the new law, a penalty of six months' to three years' imprisonment applies to 'hacking', 'cracking' and computer virus offences (s. 33(a)), with fines ranging from P100,000 (approx. US$2,350) to a maximum commensurate to the damage incurred. This provision was a response to events of May 2000, involving the creation and dissemination of the 'ILOVEYOU' computer virus which spread to millions of Internet-connected computers throughout the world and caused an estimated US$7 billion in damage (Associated Press 2000). Similar penalties apply to intellectual property piracy (s. 33(b)). There are no specific provisions in relation to Internet fraud.

A modernised Computer Crime law has reportedly been drafted in Thailand among a package of IT-related laws initiated by the National Electronics and Computer Technology Centre (NECTECH), including laws governing electronic commerce, electronic funds transfer, and universal access and data protection (Koanantakool 1999; Pongvutitham 2000; Karnjanatawe 2001).

7.4 How Laws Could be Improved

The creation of multilateral treaties is one way of reforming laws internationally, although this process is not without problems. The Council of Europe's (2001) Draft Convention on Cybercrime (draft no. 27, released 25 May 2001) has taken almost four years to reach its present form. Having been approved by the Parliamentary Assembly on 24 April 2001, with

recommendations to include provisions on human rights and a protocol to ban 'hate speech', the Convention must still be revised by the European Committee on Crime Problems—which is expected to take place in December 2001, before it is finally submitted to the Committee of Ministers for adoption—presumably sometime in 2002.

The Convention will be the first international treaty to address criminal law and procedural aspects of various types of criminal behaviour directed against computer systems, networks, or data and other types of similar misuse. As such it will hopefully provide a framework for international reform in this area (Sussmann 1999, Tan 2000).

Signatories to the Convention include the 43 member states of the Council of Europe (COE) plus the United States, Canada and Japan. There are some indications that the COE Convention will be seen as a model in the Asia-Pacific region for countries seeking to update their computer crime laws (Urbas 2001).

In November 2000, another milestone was achieved with the adoption by the United Nations of the *Convention Against Transnational Organised Crime*. The Convention is intended to provide a legal framework for concerted action against organised crime, and the basis for the harmonisation of national legislation. It contains provisions requiring the criminalising of certain conduct (including participation in an organised criminal group, money laundering and corruption), as well as provisions on corporate liability, special investigative techniques, witness and victim protection, cooperation between law enforcement authorities, exchange of information on organised crime, training and technical assistance, and prevention at the national and international levels.

The Convention offers great potential for enhanced cooperation among countries with respect to implementation of anti-money laundering measures, confiscation of criminal assets, promotion of extradition and mutual legal assistance mechanisms, and the application of modern technology in the fight against crime.

Even in those countries with relatively advanced laws against cybercrime and specialised enforcement agencies, prosecution can be difficult due to traditional rules of evidence and criminal procedure (Clark 2001; Clark, Cho and Hoyle 2000). An Internet piracy taskforce set up in December 1999 within the Hong Kong Customs and Excise Department, for example, had

not prosecuted any cases by November 2000 despite numerous arrests, due to the difficulty of producing admissible evidence in court proceedings. This was despite the fact that HK$2.6 million had been spent on setting up a computer forensic laboratory to examine electronic evidence (Chow 2000).

Similarly in Malaysia, despite the enactment of new 'cyber laws', difficulties have emerged in the areas of legal interpretation, enforcement, assessment of damages, search and seizure of evidence, and international cooperation (Lau 2000).

Reforms could also be made to the range of sanctions that can be used against those convicted of Internet fraud. 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 conduct. These include adverse publicity, professional disciplinary sanctions, civil action, injunctive orders and, most recently, various forms of reconciliation or community conferencing. The confiscation of an offender's assets represents an effective means of deterrence as long as such sanctions receive wide publicity. Both adverse publicity and forms of reintegrative shaming can be effective in public sector workplaces where reputations are important. One form of this which has been found to be effective in reducing the extent to which staff use the Internet for unauthorised purposes, involves employers publicising details of web sites visited by their staff and naming the staff in question.

7.5 Criminal Proceedings Undertaken

Little information is available publicly concerning the judicial outcomes of cases involving Internet fraud in the region as police and courts generally do not maintain records in such a way as to isolate the precise manner in which fraud offences are committed. As such, reliance has to be placed on anecdotal accounts, such as those described in the earlier review of the types of Internet fraud incidents.

8 Fraud Prevention Initiatives

8.1 Introduction

The solutions to Internet-related crime and particularly fraud involve a wide range of strategies which extend from traditional crime control measures to novel technology-based means of preventing illegal conduct from being carried out electronically (see Grabosky and Smith 1998). Fraud prevention in the digital age requires the use and adaptation of traditional measures (such as the use of appropriate fraud control policies and the provision of information) as well as the use of novel technological approaches (such as the use of effective means to authenticate users of computers and to track how they are using computers). Fraudulent conduct may also be deterred through the use of prosecution and punishment, although in the digital age this is often difficult and costly to achieve.

The so-called 'onion model' of fraud prevention is likely to yield the greatest benefits. This entails the use of various layers of protection including encryption, firewalls, intrusion detection systems, incident response procedures, and monitoring of systems by external auditors (KPMG 2001).

8.2 Regional Initiatives

As noted by McConnell International, a degree of international cooperation in the response to Internet crime is emerging, particularly with the establishment of the Council of Europe's (COE) Draft Convention Against Cybercrime. However, the consensus needs to extend beyond the 43 COE countries to other regions, including the Asia-Pacific region (McConnell International 2001):

> *Because of cyber crime's international potential, all countries, and all companies, are affected. Interested parties, including national governments from outside Europe, and businesses and non-governmental organisations from around the world, should participate vigorously in a consensus process to develop measures that support effective international law enforcement and foster continued growth and innovation.*

An example of recent international cooperation involving the United States Federal Trade Commission (2001a) and 12 other countries—including Australia, Canada, New Zealand and Korea—is the creation of a multilingual public web site called 'econsumer.gov' (2001), that allows Internet users and law enforcement agencies to share information about misuse of the Internet (Greenwood 2001).

Attempts are also being made to improve methods of identification of individuals throughout the region in order to reduce the risk of identity-related fraud. The Malaysian National Registration Department, for example, plans to issue all newborn children with a chip-based identity card, if their parents so desire. The card will contain a number, name, parents' names, address and citizenship status, and will be in addition to the birth certificate—which is a mandatory document at present and which includes a thumbprint. The identity card will later include blood group and other health information. The card will be used initially for school registration and medical care purposes. A fingerprint will be required to obtain an original card or replacements. Fingerprints will be maintained separately and will not be recorded on the card (Krishnamoorthy 2000, cited by Ringin 2000).

In China, the government has introduced a requirement for bank customers to use their real names and have proof of identity, such as passports or the People's Republic of China citizen identity card, before opening new accounts. A National Statistics Bureau report indicated that more than 1,000 billion yuan (approximately A$250 billion) in public funds are illegally deposited in banks which is estimated to amount to one-fifth of the total amount of savings. This ruling does not apply to existing account holders as there is concern that, should a large proportion of these account holders withdraw their funds, it could destabilise the banking system and initiate a credit flow crisis. Of concern, however, is the lack of verification of identity documents relied upon, such as occurs in Australia. False identity cards circulate widely in China, and are available cheaply. There is a likelihood of increased demand for, and use of false identity papers in order to circumvent these new rules. Although changes to the banking system indicate a willingness by the Chinese Government to comply with international money-laundering initiatives, the larger problem of false identification may overshadow these changes (Ringin 2000).

8.3 Risk Management

Companies wishing to prevent Internet fraud need to ensure that they have in place the range of risk management and fraud control measures that apply in other aspects of their business. Sometimes, however, obvious fraud control measures are overlooked because of the speed with which electronic commerce procedures have been implemented, or simply because those in charge of fraud control do not fully understand the nature of the risks that arise.

In KPMG's Global eFraud survey (2001), 30 per cent of respondents reported not having adequate segregation of duties in place with respect to their electronic commerce systems, while 60 per cent did not perform security audits. Some 62 per cent did not carry out background checks on entities that assisted them in developing, maintaining and or administering their electronic commerce systems, while 56 per cent did not carry out background checks on entities with which they did business electronically. Of the Asia-Pacific respondents from Australia, Hong Kong and India, some 70 per cent conducted background checks on electronic commerce system suppliers—which was a higher percentage than respondents from most other countries.

The need for effective risk management in electronic commerce is highlighted in view of the results of a survey of the backgrounds of management of Internet companies conducted by Kroll between June and August 2000. The global survey of 70 Internet corporations found that executives of Internet corporations were four times as likely to have 'unsavoury' backgrounds, as executives from other industries. The 20 respondents from Internet corporations in Asia, Australia and New Zealand were particularly likely to have executives with prior bad characters—including individuals who had allegedly been arms dealers, convicted criminals, smugglers and thieves. One Internet company hired an alleged arms dealer to run its operations across two Asian countries. Two Internet companies in the region were found to have had links with organised crime. The survey also found that executives of Internet companies based in Asia tended to be less concerned about security than their counterparts in the United States (Needham 2000). Although these allegations may be difficult to verify, they do raise the problem of Internet companies sometimes failing to have adequate internal controls and procedures in place to screen staff adequately when recruiting.

8.4 Site Certification

Some organisations are providing certification services to enable users to identify legal, safe Internet sites. Users are then free to decide whether or not they wish to make use of the material in question. The World Wide Web Consortium (W3C 2001), for example, has developed the Platform for Internet Content Selection (PICS) which is a voluntary content rating system designed to help 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, certifies Internet sites which demonstrate sound online business practices after having undergone an extensive auditing procedure (AICPA 2001). 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 Certified Professional Accountant or accounting company. Since the AICPA began the WebTrust program, some 1,500 Certified Professional Accountants and 75 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 online merchants and users, which, hopefully, will be achieved in time.

Certification and endorsement services have two primary benefits. First, individuals are able to rely upon the fact of a business being certified in order to have some measure of confidence in the trustworthiness of that business 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 businesses who have agreed to comply with a code of conduct which meets certain minimum standards. This would provide a powerful industry-based inducement for businesses 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 20 so-called 'Webseals' are in circulation in Australia with the government providing a comparative table which sets out their various attributes (see Cook 1999). Determining acceptable standards and publicising these will represent a major challenge for the future.

In KPMG's Global eFraud survey (2001), only 12 per cent of respondents stated that their web site had a seal identifying that their system had passed a security audit (similar percentages were evident for all countries except Australia and the United Kingdom where only two per cent of respondents reported having seals in place. This low level of usage of seals was said to be due to security audits not being well known or understood or not regarded as being an effective security measure.

8.5 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 minimised 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 online 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.

8.6 Information Services

Once policies have been established they need to be communicated and fully explained in order to prevent misunderstandings as to their meaning and effect. Often policies are established but not adequately implemented or publicised.

Providing educational material concerning fraud prevention and reporting procedures on internal agency web sites is also now widely used in the public sector. In the survey conducted by the Australian National Audit Office (2000, p. 48) of Commonwealth fraud control arrangements, approximately 30 per cent of agencies used email, and 35 per cent of agencies used their Intranet or public databases to disseminate fraud control information to staff.

In addition, direct email fraud reporting facilities can be used, although if anonymity is required then telephone hotlines or even anonymous paper-based reporting may be preferable.

Of particular importance is the need to provide information to staff on aspects of computer security along with appropriate guidelines on reporting computer misuse and abuse. Many jurisdictions now have public interest disclosure legislation which aims to ensure that those who report illegal conduct are not disadvantaged by their conduct. In the case of computer-based illegality, as in other areas of crime, severe penalties could be imposed on individuals who engage in, or attempt or conspire with others to carry out acts of reprisal against those who disclose illegality in the public interest. To date such remedies have rarely been used.

A delicate balance needs to be struck between providing information to staff about the computer security measures that have been adopted to prevent fraud, and keeping such information private so as not to alert potential fraudsters to the security measures that they will need to circumvent in order to perpetrate fraud. Unfortunately, experience has shown that it is often upper level staff who already have knowledge of an agency's security measures who are most likely to commit computer-related fraud. This raises the need for agencies to monitor the activities of staff at all levels regularly, without unduly infringing personal privacy.

An example of the way in which information and services directed against Internet fraud may reduce business vulnerability is the simple 'Fraud Test' to be found on the Worldwide Electronic Commerce Fraud Prevention

Network web site (WECFPN 2001a). The main question 'How vulnerable are you to fraud?' is broken down into the following series of questions, with a yes / no / don't know response choice:

- Does your web site have a firewall?
- Do you employ effective data security and hiring practices?
- Do you avoid storing card account numbers on a server connected to the Internet?
- Have you installed the latest fraud detection software?
- Do you default to the highest SSL (secure sockets layer) encryption that a consumer's browser can support?
- Do you keep informed about the latest fraud trends and news?
- Do you know what law enforcement agency to contact if your business is victimised by fraud?
- Do you take advantage of card companies' address verification systems?

The Worldwide Electronic Commerce Fraud Prevention Network also offers practical advice on security and privacy protection for Internet purchases (WECFPN 2001b).

Similar advice is available from the Internet Fraud Complaint Center (IFCC 2001) on topics including:

- Internet auction fraud;
- non-delivery of merchandise;
- credit card fraud;
- investment fraud;
- Nigerian letter scams; and
- business fraud.

The National Fraud Information Center, based in the United States, also provides advice through its Internet Fraud Watch web site (NFIC 2001).

In another international initiative against consumer-related Internet fraud, a multi-lingual web site (http: / / www.econsumer.gov) was established to provide information on consumer protection legislation and other online fraud prevention measures, as well as a coordinated complaints mechanism. Countries participating are Australia, Canada, Denmark, Finland, Hungary, Mexico, New Zealand, Norway, South Korea, Sweden, Switzerland, the United Kingdom and the United States. The scheme is maintained by the Federal Trade Commission in the United States and is supported by

consumer affairs organisations in each country, the International Marketing Supervision Network, the Consumer Sentinel Network, and the Organisation for Economic Cooperation and Development.

Although initially introduced for the purposes of reducing consumer fraud on the Internet, many of these initiatives could be applied to the problem of Internet fraud in business and government contexts.

8.7 Educational Responses

One of the most effective strategies used to prevent Internet fraud is education of the public as to the nature of the security risks which they face, and how they may best protect themselves.

Most regulatory agencies throughout the world provide information in paper form and electronically through web sites which alert consumers to misleading and deceptive practices—the Consumer World (2001) web site has over 1,400 links to consumer protection and regulatory agencies.

The Australian Competition and Consumer Commission's web site also gives advice on pyramid selling schemes, business opportunity schemes, and fraudulent prizes and lotteries (ACCC 2001). 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's Department of Communication, Information Technology and the Arts has produced a series of fact sheets which provide information to consumers about the risks of shopping online, and certain other issues such as paying tax and duty, and privacy issues (DCITA 2001). Similar advice is available in Britain at the Office of Fair Trading (OFT 2001) and in the United States at the Federal Trade Commission (2001b).

Consumer groups also represent a good source of trusted information for consumers. Groups such as the Australian Consumers' Association, the Consumers' Union of the United States and the Great Britain Consumers' Association, conduct their own testing of products and services and publicise the results through subscriber-based magazines such as *Choice* (Australia), *Which* (United Kingdom) and *Consumer Reports* (United States). Although consumer organisations already provide consumer information by various means, including the Internet, perhaps the role of these groups in providing information services could be increased.

A novel business education campaign has been recently conducted by the Australian Securities and Investments Commission during 1999–2000 (ASIC 2001c):

> *Our longest running April Fool's Day joke convinced more than 233 people to part with more than A$4 million over the Internet.*
>
> *On April 1, 1999 we set up a fake Internet investment site, www.smbi.com.au telling people it was a sure thing they would triple their money in 15 months if they invested in Millennium Bug Insurance (MBI). The site claimed MBI was offering blue chip companies insurance against losses from the Year 2000 Millennium Bug.*
>
> *The web page claimed that because the Millennium Bug was considered to be high risk, the insurance company would be able to charge high premiums, giving investors a good rate of return. Over the period of a month, 10,200 people visited the fake site, 233 people committed themselves to $10,000 and $50,000 investment packages and 1,212 people asked for more information about the investment.*

The people who fell for the scam received a return email from ASIC telling them it was an April Fool's Day joke and giving them advice on how to protect themselves.

8.8 Internet Sweeps

Consumer protection agencies now regularly conduct sweeps of the Internet in order to identify illegal practices and sites that contain misleading and deceptive information. For example, in 1998, a worldwide clean-up operation, involving the Office of Fair Trading in Britain and its counterparts in 22 other countries, identified 1,159 potential 'get rich quick' schemes being advertised on Internet sites (Office of Fair Trading 1998). Once identified, these sites were then able to be investigated and, where appropriate, advice given to members of the public to avoid dealing with them. A similar sweep coordinated by the Federal Trade Commission in the United States, entitled 'GetRichQuick.Con', was conducted in 2000 (Brown and Johnston 2000).

8.9 Technological Responses

There is also an established and continually expanding industry that provides electronic security measures associated with electronic commerce. Some products are clearly better suited to the risks of Internet fraud than others and the challenge lies in choosing appropriate measures tailored to suit individual needs. The nature of this market is such, however, that there are likely to be numerous equally effective solutions to the problems associated with electronic commerce. It remains to be seen which will capture the global market of the future. In the short-term, businesses and government agencies need to be made aware of products that are inappropriate, unreliable, overly expensive and unsuited to their needs.

8.9.1 User Authentication

Authentication of one's identity is crucial in preventing Internet fraud. Identity-related crime is a substantial problem which has become easier to perpetrate through the use of so-called desktop publishing equipment (Smith 1999). As businesses and government agencies continue to make use of electronic commerce and electronic procurement, the need to authenticate users' identities will become of critical importance. A report by the House of Representatives Standing Committee on Economics, Finance and Public Administration (2000) in Australia recommended, *inter alia*, that the Australian Taxation Office improve its internal processes for establishing identity and preventing identity fraud and that the Commonwealth Government formalise a process for working with other levels of government and industry to develop options for reducing and preventing identity fraud. A wide range of technological solutions has been devised to address the problems associated with user authentication, and it remains to be seen which solution, or which combination of solutions, will be most effective.

As most online payment systems require the use of a PIN or password in order for users to gain access to personal computers, protection of access codes is the primary crime prevention strategy available. Passwords are, however, 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).

Users are best placed to protect themselves by taking basic security precautions to ensure that access codes and other personal information are not stolen. Simple precautions such as not choosing obvious numbers, not sharing numbers and changing numbers regularly are recommended. Studies reveal, however, that between 20 and 70 per cent of people are negligent in using access code information (Sullivan 1987).

There are various ways of enhancing access security controls through the use of technology. Systems have been devised which change passwords regularly, or which deny access after a specified number of consecutive tries using invalid passwords. Some work stations 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, are also available.

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. Such a system is, however, able to be overcome through the use of call-forwarding arrangements (Denning 1998, p. 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 a location signature sensor which uses signals transmitted by satellite to provide a location on earth at any given time. Users can thus 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).

8.9.2 Biometrics

In the future biometric user authentication technologies will greatly enhance security, although privacy concerns will need to be addressed. Already there is 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). Fingerprint identification systems are now being used to restrict access to keyboards and when using a computer mouse.

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 computer networks. An initiative designed to reduce social security fraud in Toronto has been the enactment of legislation which would enable welfare benefit recipients to use fingerprint authentication when dealing with the Ontario government in Canada. Detailed privacy protections are built into the legislation which includes requirements for all biometric data to be encrypted and for the original biometric to be destroyed after the encryption process has been completed (Cavoukian 1999).

8.9.3 Digital Signature Security

Public key encryption systems represent one of the most effective ways of conducting electronic commerce transactions securely. 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 or birth certificate) along with matching secondary documentation (such as a bank statement or car registration papers) 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 desktop publishing equipment.

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 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 be needed 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 personal identification numbers (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.

An example of the risks associated with the use of encrypted authentication systems arose recently when the Microsoft product, VeriSign, was tricked into issuing false digital certificates in Microsoft's name (Bader 2001, Markoff 2001). The certificates in question were not used for electronic commerce transactions, but for checking the authenticity of the name of the developer of software programs. The problem arose in the human verification part of the process of issuing digital certificates which could also occur in electronic commerce authentication procedures.

8.9.4 Document Security

All systems of user authentication for electronic commerce transactions require users to prove their identity. Although the security of electronic communications may be greatly enhanced through the use of encryption, some of the greatest risks associated with electronic commerce arise when individuals seek to establish their identity when registering with authorities. Often identity documents are presented which are counterfeit or have been altered.

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.

Second, 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.

Third, modern security features should be incorporated on all documents used for identification purposes. 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. The use of these technologies makes counterfeiting extremely difficult.

8.9.5 Fraud Detection Software

If one is unable to prevent online fraud from taking place entirely, it may at least 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 Internet 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. The success of such an approach depends, however, upon the extent to which the software cannot be interfered with or modified.

8.9.6 Tracking and Surveillance

It is also possible for technology to keep the activities of Internet users under surveillance. Employees' use of computers and their online 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, or if funds are being moved to specified accounts for unauthorised purposes. Ideally, agreed procedures and rules should be established which enable staff to know precisely the extent to which computers can be used for private activities, if at all. If agencies do permit staff 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 online activities have been prohibited, many government agencies now monitor the activities of their employees, sometimes covertly (such as through video surveillance or checking email 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. Although this can be an effective risk management tool for managers, it is possible to by-pass filtering software by obtaining the password of the person who installs the software.

The use of computer software to monitor the business activities of government agencies also provides an effective means of detecting fraud and deterring individuals from acting illegally. The Australian Health Insurance Commission, for example, employs artificial neural networks to detect inappropriate claims made by health care providers and members of the public in respect of various government-funded health services and benefits. In 1997–98, this technology contributed to the Commission locating $7.6 million in benefits which were paid incorrectly to providers and the public (Health Insurance Commission 1998).

In addition, revenue authorities are able to make use of information derived from financial transaction reporting requirements to identify suspicious patterns of cash transactions which could involve illegality or money laundering. In Australia, in 1997–98, the Australian Taxation Office attributed more than A$47 million in revenue assessed to its direct use of information provided by the Australian Transaction Reports and Analysis Centre. In one case, a taxpayer and associated entities had transferred more than A$1.3 million to a tax haven. Following an investigation, more than A$6 million in undeclared income was detected (AUSTRAC 1999).

9 Conclusions

9.1 Introduction

This report has provided a preliminary assessment of the problem of Internet fraud in a selection of Asia-Pacific countries. An attempt was made to determine the level of information that is currently available in order to establish the nature and significance of the problem in the region and to establish a strategy for conducting further research in the future. Although the use of the Internet is expanding rapidly throughout the region, most identified fraud-related activities have arisen in consumer contexts rather than in relation to electronic commerce involving business and government entities. As electronic service delivery in these latter realms develops, it is likely that crimes of deception will increase considerably.

9.2 Theories of Internet Fraud

A number of theoretical models have been constructed in the past in an attempt to explain why people commit fraud (see Krambia-Kapardis 2001 for a review). Some of the key characteristics of recent models include the following:

- a perceived *opportunity*, such as the absence of, or circumvention of controls that enable fraud to be prevented or detected;
- an offender with a *motivation* to steal money, whether through cupidity, living beyond one's means, the existence of debts—sometimes associated with an addiction to drugs or gambling—the presence of a financial crisis, or various work-related pressures;
- the presence of a *rationalisation* for acting illegally, such as a belief that the victim can afford the loss, that the funds stolen will be repaid, or that the money will be used for a good purpose by the offender; and finally,
- the absence of a *capable guardian*, whether through poor business administration, lack of fraud prevention resources, or the absence of an effective police service or regulatory authority.

In the case of economic commerce-related fraud, motivations and rationalisations remain much the same as in other cases of conventional

fraud. However, the introduction of electronic commerce has created many new opportunities, sometimes due to fraud prevention measures being overlooked, or flaws that exist in the technological framework that supports these new business models.

In addition, capable guardians are often absent or less effective in the online world where transactions take place across borders, police and regulators may be unfamiliar with the technologies in question or inadequately funded to conduct investigations, and sanctions often rarely imposed.

These two factors—the presence of opportunities and the absence of guardians—have created a criminogenic environment highly conducive to fraud. They have also, however, provided a focus for fraud control measures, as opportunities may be reduced and guardianship enhanced through the use of a range of measures.

9.3 Risks and Remedies

Substantial resources are being devoted to the prevention of Internet fraud by consumer protection agencies, largely through the provision of information to users of these technologies as to ways in which they may avoid personal victimisation. To date, however, businesses and government agencies have not engaged in similarly widespread educational initiatives designed to inform managers and employees as to the risks associated with electronic commerce.

Considerable reliance has been placed on technological solutions, which have yet to achieve widespread application in a uniform model. In addition, although technological solutions such as public key solutions have much to offer, they need to be used in conjunction with effective risk management and user education programs designed to ensure that the technologies adopted are well suited to the risks involved and well understood by those who will make use of them. Sophisticated encryption may well prevent data from being manipulated electronically, but is unlikely to have an impact on identity-related fraud or theft of passwords or keys which may lie at the heart of many Internet-related fraud strategies.

Policy reforms and associated legislative solutions designed to deal with the problems of electronic commerce are taking place throughout the region with most countries now having identified weaknesses in their regulatory controls and having embarked upon a process of reform. Whether the

solutions adopted will be effective to meet existing and future issues remains to be seen, although workable legislative models have now been identified in a number of jurisdictions.

Although some may question their effectiveness, Internet-related 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. The last 30 years have seen continual improvements in legislation and dispute resolution procedures and many online activities fall within the scope of these initiatives.

Unfortunately, the remedies which are available to those who have been victimised on the Internet 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 often beyond the means of individual businesses or government departments and costs far in excess of the amount lost in many cases. The perpetrators of many Internet-related crimes 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.

Much remains to be done, however, in applying new solutions to Internet fraud, as law enforcement agencies continue to suffer from inadequate funding, courts are only now beginning to deal with the legal problems that have arisen in specific cases, and suitably trained forensic accountants are often in short-supply. It is also clear that the deterrent effects of criminal prosecution and punishment are limited in this area as offenders often receive relatively lenient sentences in cases of economic crimes.

The problem of electronic crime has brought home to policy-makers and legislators the need to harmonise efforts globally. Already considerable achievements have been made in devising uniform approaches to dealing with computer crime internationally with a number of countries having agreed to conventions and treaties to deal with some of the more difficult problems, such as transnational and organised criminal activities that are carried out electronically.

Allied to the harmonisation of laws, however, is the need to harmonise other aspects of business practices in order to provide a global environment in which economic crime is difficult to perpetrate and yet simple to detect. Bodies such as the International Accounting Standards Committee (IASC), for example, help to promote uniform accounting practices and procedures within the business community that seek to reduce the risk of improper conduct being engaged in. Similarly, international professional bodies have a role to play in creating uniform ethical practices globally which militate against fraud (Braithwaite and Drahos 2000, p. 121).

In addition, international bodies such as the World Bank and the Asian Development Bank may be able to assist developing nations to establish effective preventive strategies through the provision of resources and funding. Other networks, such as the OECD and ASEAN, could also assist in harmonising policy and legislative approaches to dealing with electronic commerce.

Those who make use of the Internet need, however, to be made aware of the risks they face and informed about the nature of the various objectionable online practices which are present. Already there are substantial amounts of information of this nature available. The challenge lies in ensuring that users are made aware of its existence. In this regard, certification and notification systems, which permit users to readily identify 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. 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 after they have been closed down because of improper practices.

The challenge facing those who would seek to minimise Internet fraud is to seek a balance which would allow a tolerable degree of illegality in return for creative exploitation of the technology. Even at this early stage in the development of electronic commerce, it may be useful for individuals, interest groups and governments to articulate their preferences and let these serve as signals to the market. Markets may then be able to provide appropriate responses which governments are unwilling or unable to achieve. Internet fraud is bound to increase as the new century unfolds. However, by making effective use of traditional crime control measures, coupled with some sophisticated technological solutions, it may be possible to keep Internet fraud within manageable limits.

9.4 Guidelines on Fraud Minimisation

In an attempt to achieve a uniform approach to dealing with Internet fraud in the Asia-Pacific region, CAPA could play an important role by promulgating a set of guidelines designed to minimise victimisation in business and government contexts. A number of codes of practice and guidelines have been suggested to deal with various aspects of online activities, although these have mainly been focused on consumer transactions and activities.

Appended to this report are draft *Guidelines on Fraud Minimisation for Organisations Engaged in Electronic Commerce* which could be used as the basis for assisting businesses and government agencies in preventing and controlling Internet fraud in the region. These draft guidelines make use of the OECD's guidelines on consumer transactions, but have expanded them to accommodate the issues involved in business and government electronic commerce within the region.

By widely disseminating such guidelines, CAPA could help businesses and government agencies acknowledge the problem of Internet fraud and commence the process of devising suitable and uniform solutions. The Asia-Pacific Region is well placed to make use of such Guidelines as development of electronic commerce is generally still in its infancy in the region and, thus, practices and procedures have not become entrenched and immoveable. The creation and use of guidelines setting out best practice would accordingly help to enable electronic commerce to be established in the region in such a way as to minimise fraud risks.

9.5 The Future

The risk of Internet fraud in the region in the future is likely to correlate highly with the extent to which online activities are engaged in. As the telecommunications infrastructure develops throughout the region, government agencies and private sector businesses are likely to take up electronic commerce to a substantial degree. In the not-too-distant future, most government activities may be carried out electronically and a considerable proportion of business transactions may also be conducted online. The extent to which this expansion of electronic service delivery will create opportunities for fraud will be dependent upon the nature and

effectiveness of the policies, laws and technological measures that are introduced to prevent its occurrence. Without effective controls, fraud could become rife in the region. If appropriate control measures are in place, fraud may exist to the same, or even less extent than occurs in the previous non-digital environment.

9.6 Suggested Initiatives

The following measures may help to prevent and to control Internet fraud in the future, as well as to facilitate the on-going monitoring of the nature and scope of the problem. Some of these initiatives could be introduced with little difficulty and expense, while others may require substantial resources to be expended. As many of the issues are common throughout the region, it would be appropriate for uniform measures to be taken with respect to each of the following matters.

9.6.1 Guidelines

Countries within the region should aim to establish guidelines, similar to the OECD's best practice recommendations with respect to business-to-consumer electronic commerce, for business and government electronic transactions. (The appended draft guidelines could form the basis of an agreed framework for adoption throughout the region.)

9.6.2 Law and Policy Stocktake

A stocktake could be undertaken of the specific policies and laws throughout the region that seek to address the problem of Internet fraud in business and government contexts. Any gaps in policy and legal frameworks could then be identified and appropriate uniform solutions adopted.

9.6.3 Police Incident Database

Uniform practices should be implemented within national law enforcement and regulatory agencies to identify and record all cases involving Internet fraud. A database could then be created that would permit a regional assessment to be undertaken of the precise extent of the problem, and how agencies and courts have responded.

9.6.4 Sentencing Database

Justice departments throughout the region should establish a sentencing database of Internet fraud cases in order to assist judicial decision-makers in arriving at consistent decisions and to publicise cases that have been successfully prosecuted. This would help to enhance general deterrent effects of the judicial process throughout the region.

9.6.5 Regional Internet Fraud Desk

A confidential electronic database could be created throughout the region in which individuals could report cases of business and government Internet fraud to the police. A Regional Internet Fraud Desk could be used as a vehicle to collect and collate reports and to share information between law enforcement bodies. Certain unrestricted information from the database could be provided publicly to publicise new areas of risk.

9.6.6 Certification Services Stocktake

A stocktake could be undertaken of existing certification and authorisation services available throughout the region that provide information on the trustworthiness of businesses and agencies that engage in electronic commerce.

9.6.7 Skilled Professionals Register

A register could be created listing individuals and organisations with appropriate qualifications and expertise in dealing with Internet fraud. Included could be forensic accountants, lawyers, investigators, prosecutors, policy officers and those skilled in fraud prevention activities.

9.6.8 Resource Assessment

On the basis of the information gathered using the above techniques, an assessment could then be made of the level of resources required by agencies to deal with Internet fraud.

9.6.9 Legal and Law Enforcement Partnerships

Because of the borderless nature of the Internet, partnerships should be created and extended throughout the region and with other nations to encourage the enactment of uniform laws that adequately address Internet fraud and to provide mutual assistance in the conduct of investigations.

9.6.10 Educational Programs

Efforts could also be taken to educate those involved in using the technologies of electronic commerce as to their ethical and legal obligations designed to prevent dishonest and fraudulent activities from taking place. Such educational initiatives could be provided in schools and tertiary educational institutions, as well as by business and professional bodies such as CAPA.

References

ACNielsen 2001, 'South Korea and Taiwan Dominate Asian Internet usage', News Release, 8 March 2001: http://www.eratings.com/news/20010308.htm (visited 15 August 2001).

Amarnathan, S.L.C. 2000, 'Crimes Related to the Computer Network: Commentary and Contributions to UNAFEI Discussion Guide', in Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI), *Crimes Related to the Computer Network: Challenges of the Twenty-First Century*, UNAFEI, Tokyo, pp. 67–74.

American Institute of Certified Professional Accountants (AICPA) 2001, 'WebTrust': http://www.cpawebtrust.org (visited 15 August 2001).

Anonymous 2000, 'IT 1 News', *The Age* (Melbourne), 11 July, p. 2.

Arnold, W. 2001, 'Hook up Rural Asia, Some Say, and Poverty can be Mitigated', *New York Times*, Technology Section, 19 January 2001.

Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) 2000, *Crimes Related to the Computer Network: Challenges of the Twenty-First Century*, UNAFEI, Tokyo.

Asia Internet Report 2001, 'Asian Internet Cafes: Asia at 14K', *Asia Internet Report*, No. 4, March 2001: http://www.asianinternetreport.com/AIR_0103.html (visited 19 June 2001).

Associated Press 2000, 'Philippine President Signs Law to Punish Computer Crimes', 15 June 2000, *New York Times*, Technology Section.

Attorney-General's Department, Australia 1999, *Contributions to Electronic Commerce: What Law Enforcement and Revenue Agencies Can Do*, Report of the Action Group into the Law Enforcement Implications of Electronic Commerce, Australian Government Publishing Service, Canberra.

—— 2001, *Commonwealth Fraud Control Policy and Guidelines*, Consultation Draft No. 2, April 2001: http://www.law.gov.au/aghome/commprot/crjd/lecd/FCPConsultDraft2.htm (visited 15 August 2001).

Australasian Centre for Policing Research (ACPR) 2000, *The Virtual Horizon: Meeting the Law Enforcement Challenges*, Scoping Paper Report Series No. 134.1, Police Commissioners' Conference Electronic Crime Working Party, Australasian Centre for Policing Research, Adelaide.

Australian Bureau of Statistics (ABS) 1998, *Household Use of Information Technology, Australia 1998,* Cat. No. 8146.0, Australian Bureau of Statistics, Canberra.

—— 1999, *Household Use of Information Technology, Australia 1999,* Cat. No. 8146.0, Australian Bureau of Statistics, Canberra.

—— 2000, *Use of the Internet by Householders, Australia,* February and May 2000 editions, Cat. No. 8147.0, Australian Bureau of Statistics, Canberra.

Australian Competition and Consumer Commission (ACCC) 1999, *Internet Service Providers:* http://www.accc.gov.au/docs/catalog.htm (visited 30 April 1999).

—— 2001: http://www.accc.gov.au (visited 15 August 2001).

Australian National Audit Office (ANAO) 2000, *Survey of Fraud Control Arrangements in APS Agencies*, Audit Report No 47, 1999–2000, Performance Audit, Australian National Audit Office, Canberra.

Australian Municipal, Administrative, Clerical & Services Union v Ansett Australia Ltd [2000] FCA 441, Federal Court of Australia, 6 April 2000.

Australian Securities and Investments Commission (ASIC) 2000, *Complaints Made Under the EFT Code of Conduct 1999–2000*, ASIC, Sydney.

—— 2001a, 'Two Years Jail – Suspended – For Internet Spammer', *Media and Information Releases*, 22 May 2001: http://www.fido.asic.gov.au (visited 30 July 2001).

—— 2001b, 'ASIC Welcomes Thai Cold Calling Action', *Media and Information Releases*, 27 July 2001: http://www.asic.gov.au (visited 30 July 2001).

—— 2001c, 'Millennium Bug Insurance: Our April Fool's Day Internet Investment Scam': http://www.watchdog.asic.gov.au (visited 30 July 2001).

Australian Transaction Reports and Analysis Centre (AUSTRAC) 1999, 'Great Tax Results', *AUSTRAC Newsletter*, Spring, p. 1.

Bachner, B. and Jiang, M. 2000, 'Governing Trademarks in Cyberspace: A Comparative Study of the Regulation of Domain Names in China', *Asia Pacific Law Review*, vol. 8, no. 2, pp. 191–209.

Bader, J.L. 2001, 'Paranoid Lately? You May Have Good Reason', *New York Times Online*, 24 March.

Bain, D. 2000, *E-Finance Asia Pacific: Strategic and Statistical Analysis of Online Financial Services*, Lafferty Publications, Dublin: http://www.lafferty.com/manreports/efinasiapacif.shtml (visited 29 July 2001).

Baker, M. 2001, 'ASIC Warns of Asian Scams', *The Age* (Melbourne), 20 July, Business p. 1.

Baker & McKenzie 2001, 'E-commerce Law Resources–What's New': http://www.bakernet.com/ecommerce (visited 10 August 2001).

Bao, S. 2000, 'Crimes Committed on the Internet and in Other High-tech Areas', (China perspective), *8th Asia Crime Prevention Foundation (ACPF) Conference on Crime Prevention and Criminal Justice*, 11–15 October 2000, Beijing: http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Bao,Fiji.html (visited 15 August 2001).

BBC Online Network 2000, 'Pakistan to Increase Internet access', *NUA*, 4 September: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356017&rel=true (visited 10 August 2001).

Bell, C. 2000, *E-Corruption: Exploiting Emerging Technology Corruptly in the New South Wales Public Sector*, Unpublished Strategic Assessment, New South Wales Independent Commission Against Corruption, Sydney.

Berinato, S. 2000, 'Are Killer Hack Attacks Coming?', ZDNet, 17 December, http://www.zdnet.com/zdnn/stories/news/0,4586,2665640,00.html (visited 8 August 2001).

Berwick, D. 2001, 'eCrime: The Australasian Law Enforcement Response', Paper presented to the New South Wales Independent Commission Against Corruption Symposium, *The Need to Know: eCorruption and Unmanaged Risk*, 21–22 May, Sydney.

Bloomberg News 2001, 'Indian Techies Arrested in Bank Hacking Case', *CNET News*, 25 January: http://news.cnet.com/news/0-1003-200-4602814.html?tag=prntfr (visited 8 August 2001).

Boston Consulting Group 1999, 'Boom in B2B Transactions Expected', 23 December 1999: http://nua.ie/surveys/index.cgi?f=VS&art_id=905355489&rel=true (visited 10 August 2001).

Braithwaite, J. and Drahos, P. 2000, *Global Business Regulation*, Cambridge University Press, Cambridge.

Brandquiver/Yahoo 2001, 'Strong Interest in Web Shopping Among Indians', *NUA*, 22 March 2001): http://nua.ie/surveys/index.cgi?f=VS&art_id=905356581&rel=true (visited 10 August 2001).

Bridgeman, J.S. 1997, 'Keynote Speech to the Electronic Shopping Forum', *Fair Trading Magazine*, 6 May, Office of Fair Trading, London.

Brown, R. and Johnston, M. 2000, 'Internet Fraud Sweep Fails to Turn up any NZ Sites', *IDG-Net*, 27 March 2000: http://idg.net.nz/webhome.nsf/UNID/35166639324F7B5DCC2568AC0010C1D3!opendocument (visited 10 August 2001).

Buddle, C. 2001, 'Special Team Set up to Tackle Dramatic Surge in Number of Computer Offences', *South China Morning Post*, 20 January 2000, p. 2.

Burns, S. 2000, 'How Companies Use the Internet', *Far Eastern Economic Review and Deloitte Consulting E-business Survey*, 3 November 2000: http://www.feer.com/ebiz/30Nov00/p056.html (visited 15 August 2001).

Business Software Alliance (BSA) 2001, *Sixth Annual BSA Global Software Piracy Study:* http://www.bsa.org (visited 10 August 2001).

Butler, A. 1996, 'Regulation of Content of Online Information Services: Can Technology Itself Solve the Problem it has Created?', *University of New South Wales Law Journal*, vol. 19, no. 2, pp. 193–221.

Campbell, R. 1999, 'DOFA Review in Wake of Alleged $8m Fraud', *Canberra Times*, 17 February, pp. 1–2.

Canada 2001, Criminal Code, s. 342.1, 'Unauthorized Use of Computer': http://insight.mcmaster.ca/org/efc/pages/law/cc/cc.342.1.html (visited 10 August 2001).

Cant, S. 2001, 'New Digital ID On the Way', *The Age* (Melbourne), 20 March, IT1 p. 6.

Cavoukian, A. 1999, 'Privacy and Biometrics', Paper presented to the 21st International Conference on *Privacy and Personal Data Protection*, Hong Kong, 13 September: http://www.pco.org.hk/conproceed.html (visited 17 December 1999).

Central Bureau of Investigation India 2001, 'Cyber Crime Investigation Cell': http://cbi.nic.in/cyber1.htm (visited 10 August 2001).

Central Intelligence Agency (CIA) 2000, *The World Factbook 2000:* http://www.cia.gov/cia/publications/factbook/indexgeo.html (visited 10 August 2001).

Chandrasekaran, R. 2001, 'Isolated Cambodians Join the Global Village', *The Guardian Weekly*, 14–20 June 2001, p. 22.

Chow, C. 2000, 'Cyber-pirates Escape Judicial Net: Customs Taskforce Finds Digital Data Difficult to Submit as Evidence in Court', *South China Morning Post*, 28 November 2000, p. 4.

Ching Yee Sing 2001, 'First Penang Company Director Charged In Court ', *Business Software Alliance Asia*, 25 June: http://www.bsa.org/malaysia/press/newsreleases//2001-06-25.656.phtml (visited 15 August 2001).

China Internet Network Information Centre (CNNIC) 2001a, 'Semiannual Survey Report on the Development of China's Internet', February: http://www.cnnic.net.cn/develst/e-cnnic200101.shtml (visited 19 August 2001).

—— 2001b, 'Internet Development in China: The CNNIC Survey Report', undated: http://www.89-64.com/english/net-china.html (visited 6 August 2001).

Clark, D., Bowden, S., Corner, P., Gibb, J., Kearins, K. and Pavlovich, K. 2001, 'Adoption and Implementation of E-Business in New Zealand: Empirical Results', University of Waikato Management School, Research Report Series, April: http://www.mngt.waikato.ac.nz/ict/E-BusadoptionApril01a.asp (visited 30 July 2001).

Clark, E. 2001, 'Cybercrime: Can Legislation Do the Job?', *Canberra Times*, 8 January 2001.

Clark, E., Cho. G. and Hoyle, A. 2000, *E-Business: Law and Management for the 21st Century*, Info-Sys Law International, Canberra, Australia.

Clarke, D. 1999, 'Private Enforcement of Intellectual Property Rights in China', in *Intellectual Property Rights in China: Evolving Business and Legal Frameworks*, National Bureau of Research Analysis, vol. 10, no. 2, Seattle, United States.

Clarke, R. 2001, 'Internet Industry and Community Groups': http://www.anu.edu.au/people/Roger.Clarke/II/NetGroups.html (visited 15 August 2001).

CNN Interactive 2001, 'Mobile Use to Boost Japanese Net Audience', *NUA*, 21 March 2001: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356589&rel=true (visited 10 August 2001).

Computer Security Institute and Federal Bureau of Investigation, Computer Intrusion Squad 2001, *Computer Crime and Security Survey*, CSI/FBI, San Francisco: http://www.gocsi.com/prelea_000321.htm (visited 17 July 2001).

Consumer World 2001: http://www.consumerworld.org (visited 15 August 2001).

Cook, V. 1999, 'Trust Me, I'm a Computer', *Communications Newsletter*, September, pp. 14–15.

Council of Europe 2001, *Final Draft Convention on Cybercrime*, European Committee on Crime Problems (CDPC) and Committee of Experts on Crime in Cyber-Space (PC-CY), Strasbourg: http://conventions.coe.int/treaty/EN/projets/projets.htm (visited 15 August 2001).

Creed, A. 2001, 'New Zealand Centre to Combat Cyber Threats', *Newsbytes*, 8 August: http://www.newsbytes.com/news/01/168792.html (visited 12 September 2001).

CyberAtlas 2000, 'Online Population of the Philippines', 6 April 2000: http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_335811,00.html (visited 10 August 2001).

—— 2001a, 'Asian B2B E-Commerce Approaches Quarter of World's Total', Internet.com, 5 April: http://cyberatlas.internet.com/markets/b2b/article/0,,10091_735181,00.html (visited 10 August 2001).

—— 2001b, 'China's Online Population', 25 April: http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_752081,00.html (visited 6 August 2001).

—— 2001c, 'Thailand's Online Population', 29 June: http://cyberatlas.internet.com/big_picture/geographics/article/1,1323,5911_794141,00.html (visited 10 August 2001).

Daily Excelsior 2000, 'Fijian Island Duped in US-based Internet Fraud', 25 July: http://www.dailyexcelsior.com/00july25/inter.htm#3 (visited 15 August 2001).

Dancer, H. 2000, 'K2 uncovers GST keyhole', *The Bulletin* (Australia), 11 July, p. 76.

Dataquest 2001, 'Asia to Become Largest Net Market', *NUA*, 7 August 2001: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905357053&rel=true (visited 7 August 2001).

Deakin University 1994, *Fraud Against Organisations in Victoria*, Deakin University, Geelong, Victoria.

Denning, D.E. 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.

Department of Communication, Information Technology and the Arts (DCITA) Australia 2001, 'Shopping on the Internet: Facts for Consumers': http://www.dcita.gov.au/shoponline (visited 9 August 2001).

Department of Public Works and Services, New South Wales 1999, *Electronic Procurement: Taking Up the Challenge*, Sydney.

Department of Trade and Industry, Philippines 2000, *Electronic Commerce Act 2000:* http://www.iconn.com.ph/dti/ecom.htm (visited 6 August 2001).

Department of Treasury, Consumer Affairs Division, Australia 2000, *Building Consumer Confidence in Electronic Commerce: A Best Practice Model for Business*, Commonwealth of Australia, Canberra.

econsumer.gov 2001: http://www.econsumer.gov (visited 10 August 2001).

Ellison, C. (Federal Minister for Justice and Customs, Australia) 2001a, 'United Efforts Against Cybercrime', 27 June 2001: http://law.gov.au/aghome/agnews/2001newsjus/e137_01.htm (visited 15 August 2001).

—— 2001b, 'New Laws Combat Cybercrime', 25 July 2001: http://law.gov.au/aghome/agnews/2001newsjus/e160_01.htm (visited 15 August 2001).

Ernst & Young 1996, *Fraud: The Unmanaged Risk*, Ernst & Young, London.

—— 1998, *Fraud: The Unmanaged Risk*, Ernst & Young, London.

eTForecasts 2001a, 'Internet User Forecasts by Country, Executive Summary': http://www.etforecasts.com/products/ES_intusers.htm (visited 15 August 2001).

—— 2001b, 'Computers in Use by Country, Executive Summary': http://www.etforecasts.com/products/ES_cinuse.htm (visited 15 August 2001).

Far Eastern Economic Review (FEER)/Deloitte Consulting 2000, *E-Business Survey:* http://www.feer.com/ebiz/ebizindex.html (visited 10 August 2001).

Farber, D. 1999, 'Hong Kong Police Calls for Stronger Encryption to Fight Hackers', *Newsbytes*, 28 June: http://www.newsbytes.com (visited 31 May 2001).

Federal Bureau of Investigation 2000, Press Release, 14 August: http://www.fbi.gov/pressrm/pressrel/pressrel100/vatis08142000.htm (visited 17 January 2001).

Federal Trade Commission (FTC) 1998, *Prepared Statement of the Federal Trade Commission on 'Internet Fraud'*, before United States Senate Subcommittee of the Governmental Affairs Committee, 10 February: http://www.ftc.gov/os/1998/9802/internet.test.htm (visited 15 August 2001).

—— 2001a, *Prepared Statement of the Federal Trade Commission on 'Internet Fraud'*, before United States Senate Subcommittee on Commerce, Trade and Consumer Protection, 23 May: http://www.ftc.gov/os/2001/05/internetfraudttmy.htm (visited 15 August 2001).

—— 2001b, 'E-commerce and the Internet': http://www.ftc.gov/bcp/menu-internet.htm (visited 9 August 2001).

Fenton-Jones, M. 2000, 'Net Closing on Cyber-Pillagers', *West Australian*, 20 November, p. 37.

Forrester Research 2001, 'B2B Trade in Canada to Reach CAD272 billion', *NUA*, 11 January 2001: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356332&rel=true (visited 10 August 2001).

Gana Jr., S.H. 2000, 'Prosecution of Cyber Crimes through Appropriate Cyber Legislation in the Republic of the Philippines', *8th Asia Crime Prevention Foundation (ACPF) Conference on Crime Prevention and Criminal Justice*, 11–15 October, Beijing: http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana,Phillipine.html (visited 15 August 2001).

Gartner Group 2001, 'B2B Market Matures in Asia Pacific', *Newsbytes*, 2 January: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356296&rel=true (visited 10 August 2001).

Geurts, J. 2000, 'The Role of the Australian Federal Police in the Investigation of High-Tech Crimes', *Platypus Magazine: The Journal of the Australian Federal Police*, March: http://www.afp.gov.au/publica/platypus/mar00/intfrd.htm (visited 5 February 2000).

Gilley, B. and Crispin, S. 2000, 'A New Game of Cops and Robbers', *Far Eastern Economic Review*, 20 April, pp. 50–4.

Gosnell, P. 2000, 'Chamber's E-commerce Bid', *Melbourne Sun*, 3 May 2000, p. 52.

Grabosky, P.N. and Smith, R.G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Federation Press, Sydney.

Grabosky, P.N., Smith, R.G. and Dempsey, G. 2001, *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, Cambridge.

Gray, G. 1999, 'The Changing Face of Legal Practice and Implications for Professional Indemnity Insurance', *Insurance Law Journal*, vol. 11, no. 1, pp. 72–90.

Greenberg, P.A. 2000, 'Asian B2B E-Commerce to Top $272B by 2003', *E-Commerce Times*, 14 January 2000: http://www.ecommercetimes.com/perl/story/2220.html (visited 15 August 2001).

Greenwood, D. 2001, 'Government Backs International E-consumer Site', 27 April: http://netnow.co.nz/webhome.nsf/UNID/3C9DB254FC0CBD5ACC256A3A000D9682!opendocument (visited 10 August 2001).

Health Insurance Commission 1997, *Annual Report 1996–97*, Professional Review Supplement, Australian Government Publishing Service, Canberra, p. 23.

—— 1998, *Annual Report 1997–98*, Australian Government Publishing Service, Canberra.

Hong Kong Police Crime Prevention Bureau 2001: http://www.info.gov.hk/police/cpb/english/comp/com01.htm (visited 6 August 2001).

House of Representatives Standing Committee on Economics, Finance and Public Administration 2000, *Numbers on the Run: Review of the ANAO Report No. 37 1998–99 on the Management of Tax File Numbers*, Parliament of the Commonwealth of Australia, Canberra.

IDC 1999, 'Asia-Pacific Development Outpaces Europe', *NUA*, 14 April 1999: http://nua.ie/surveys/index.cgi?f=VS&art_id=905354838&rel=true (visited 10 August 2001).

—— 2001, 'Malaysia's Online Population', *CyberAtlas*, 25 January 2001: http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_334251,00.html (visited 10 August 2001).

Independent Bangladesh Staff Reporter 2001, 'Rise in Cybercrime Worries Experts', 14 January: http://independent-bangladesh.com/news/jan/14/text/140101cr.htm (visited 18 May 2001).

Internet Fraud Complaint Center (IFCC) 2001, 'Internet Fraud Preventive Measures': http://www.ifccfbi.gov/strategy/fraudtips.asp (visited 8 August 2001).

Internet Fraud Watch 2000, 'Internet Fraud Statistics 2000': http://www.fraud.org/internet/lt00totstats.htm (visited 1 August 2001).

Internet Software Consortium (ISC) 2001, 'Domain Survey': http://www.isc.org/ds (visited 6 August 2001).

International Telecommunication Union (ITU) 2001, 'Telecommunications Indicators': http://www.itu.int/ti (visited 6 August 2001).

INTERPOL 2001, 'Asia-South Pacific Working Party on Information Technology Crime': http://www.interpol.int/Public/TechnologyCrime/WorkingParties/asia (visited 9 August 2001).

Japan Economic Foundation 2000, 'e-Commerce in Japan: What is the Japanese e-Commerce Market Worth?', *Journal of Japanese Trade and Industry*, Nov/Dec: http://www.jef.or.jp/en/jti/200011_009.html (visited 15 August 2001).

Japan Internet Report 2001, No. 57, May: http://jir.net/jir5_01.html (visited 15 August 2001).

Japan Times Online 1999, 'Man Arrested Over Bogus Bank Accounts', 13 September: http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn19990913a7.htm (visited 8 August 2001).

—— 2000, 'Six Held for Net Fraud Since New Law Enacted', 1 September: http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20000901b5.htm (visited 9 August 2001).

—— 2001, 'NPO Tackles Cybercrime as Government Drags its Feet', 2 May: http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20010502b4.htm (visited 10 August 2001).

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

Karnjanatawe, K. 2001, 'First Draft of Computer Crime Law Almost Ready for Public Hearing, says Chief Justice', *Bangkok Post*, 21 March.

Kennedy, D. 2001, 'Beyond Reasonable Doubt', *The Age* (Melbourne), 24 April, p. 3.

Koanantakool, T. 1999, 'Electronic Commerce Development in Thailand', *National Electronics and Computer Technology Center (NECTECH):* http://www.nectec.or.th/users/htk/e-commerce/intro.html (visited 10 August 2001).

Korea Times 2001, 'Online Stock Trading Appeals to Koreans', *NUA*, 25 June: http://nua.ie/surveys/?f=VS&art_id=905356903&rel=true (visited 10 August 2001).

KPMG 1999, *1999 Fraud Survey*, KPMG, Sydney.

—— 2001, *Global e.fr@ud Survey*, KPMG Forensic and Litigation Services.

Krambia-Kapardis, M. 2001, *Enhancing the Auditor's Fraud Detection Ability: An Interdisciplinary Approach*, Peter Lang, Frankfurt-am-Main.

Kriegler, R. 1999, 'LIV Annual Survey of Legal Practitioners', *Law Institute Journal*, March, pp. 52–57.

Krishnamoorthy, M. 2000, 'Government to Issue Identity Cards to Newborn Babies', *Star Newspaper* (Malaysia), 16 March.

Lau, P. 2000, 'Cyberlaws: The Road Ahead', *Business Times (Malaysia)*, 8 December 2000, p. 5.

Legard, D. 2000, 'China Internet Users Top 12 Million', *IDG News Service*, Singapore, 8 June: http://www.iamasia.com (visited 10 August 2001).

Lemon, S. 1999, 'Hong Kong Web Shopping Gathers Steam', *Computerworld*, Hong Kong, 15 June: http://www.cw.com.hk/News/n990615001.htm (visited 13 May 2001).

Lintner, B. 1998, 'Fantasy Island: Melchizedek Passport Scam Reveals How the Internet Can Take Fraud to New Frontiers', *Netgain*, 10 December: http://www.netgain.co.nz/library/fraud_melchizedek.htm (visited 18 August 2001).

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.

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

Markoff, J. 2001, 'Warning From Microsoft on False Digital Signatures', *New York Times Online*, 23 March 2001.

McConnell International LLC 2000, 'Cyber Crime…and Punishment? Archaic Laws Threaten Global Information', December: http://www.mcconnellinternational.com (visited 15 August 2001).

—— 2001, 'Combating Cybercrime: A Proactive Approach', E-lert No. 2, February: http://www.mcconnellinternational.com/pressroom/elert2.cfm (visited 15 August 2001).

Mehta, P.K. 2000, 'Internet-related and Other High-tech Crime' (India Perspective), *8th Asia Crime Prevention Foundation (ACPF) Conference on Crime Prevention and Criminal Justice*, 11–15 October, Beijing: http://www.acpf.org/WC8th/AgendaItem2/I2PpPKMehtaIn.html (visited 15 August 2001).

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.

Melchizedek 2001: http://www.melchizedek.com (visited 25 June 2001).

Meyer, M. and Underwood, A. 1994, 'Crimes of the Net', *Bulletin/Newsweek*, 15 November, pp. 68–69.

Microsoft Corporation 2000a, 'Microsoft Launches Worldwide Campaign to Crack Down on Internet Fraud', 1 August: http://www.microsoft.com/presspass/press/2000/aug00/DigitalPiracy2PR.asp (visited 15 August 2001).

—— 2000b, 'Software Piracy Crime Fact Sheet', 1 August: http://www.microsoft.com/piracy (visited 10 August 2001).

—— 2001, 'Software Piracy Crime Fact Sheet', 2 April: http://www.microsoft.com/piracy (visited 10 August 2001).

Millar, S. 2001, 'Handheld PC Bridges the Digital Divide', *Guardian Weekly*, 26 July 2001, p. 23.

Mills, K. 1999, 'Christchurch Youths Sentenced on Internet Card Fraud', *Computerworld*, 30 August: http://idg.net.nz/webhome.nsf/ArchiveDate/E5F7561E326D0217CC25684C000D4FEA!OpenDocument (visited 15 August 2001).

Ministry of Energy, Communications and Multimedia, Malaysia 2001, *Computer Crimes Act 1997:* http://www.ktkm.gov.my/organisation/acts/crimeact.html (visited 6 August 2001).

Ministry of Information Technology, India 2001, *IT Act 2000:* http://www.mit.gov.in/itbillmain.htm (visited 6 August 2001).

Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000, *Report: Chapter 4—Damage and Computer Offences; Amendment to Chapter 2—Jurisdiction*, Commonwealth Attorney-General's Department, Canberra.

Motorola 2001, 'Privacy Practices': http://commerce.motorola.com/consumer/QWhtml/privacy.html#child (visited 15 August 2001).

Nando Times 1997, 'Bangladesh's Youth Embrace the Net', *NUA*, 19 September: http://nua.ie/surveys/index.cgi?f=VS&art_id=874670209&rel=true (visited 10 August 2001).

National Fraud Information Center (NFIC) 2001, 'Internet Fraud Watch': http://www.fraud.org/internet/intset.htm (visited 9 August 2001).

National Office for the Information Economy (NOIE) 1999, 'E-commerce to Benefit Australian Economy', *NUA*, 22 November: http://nua.ie/surveys/index.cgi?f=VS&art_id=905355420&rel=true (visited 10 August 2001).

—— 2000, *E-Commerce: Beyond 2000*, NOIE, Canberra: http://www.noie.gov.au/publications/NOIE/ecommerce_analysis/beyond2k_final_report.pdf (visited 23 April 2000).

National Police Agency (NPA) Japan 1998, 'Priority Program of Measures Against High-Tech Crime', NPA, Tokyo: http://www.npa.go.jp/soumu5/pro_eng.htm (visited 30 March 2000).

—— 1999, *White Paper on Police*, NPA, Tokyo.

—— 2000, 'Unauthorized Computer Access Law': http://www.npa.go.jp/hightech/fusei_ac2/UCAlaw.html (visited 6 August 2001).

Natsui, T. 1998, 'Computer Crime Act (Japan Penal Code)' (unofficial translation): http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm (visited 6 August 2001).

Needham, K. 2000, 'It's a Tangled Web They Thieve', *Sydney Morning Herald*, 25 October, p. 23–6.

New Straits Times 2001, 'Malaysia's Banks Using Tech To Compete', 22 May: http://www.nstpi.com.my (visited 2 August 2001).

Nielsen NetRatings 2001, 'South Korea Dominates Asia in Internet Use', *NUA*, 14 March 2001: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356555&rel=true (visited 10 August 2001).

NUA Internet Surveys 2001: http://nua.ie/surveys (visited 10 August 2001).

NZPA 2000, 'NZ to Label Computer Hacking a Crime', *IT*, 13 July: http://it.mycareer.com.au/breaking/20000713/A4539-2000Jul13.html (visited 10 August 2001).

—— 2001, 'Police Commissioners Make Plans for Cyber-cops', *Infotech*, 9 March: http://www.stuff.co.nz/inl/index/0,1008,691740a28,FF.html (visited 10 August 2001).

Office of Fair Trading (OFT) United Kingdom 1998, 'Internet Scams Deleted, Sweep Identifies "Get Rich Quick" Schemes', *Fair Trading Magazine*, Spring, Office of Fair Trading, London.

—— 2001, 'Online Shopping Advice from the OFT': http://www.oft.gov.uk/html/shopping/index.html (visited 9 August 2001).

Office of the Federal Privacy Commissioner 2000, 'Guidelines of the Commonwealth Privacy Commissioner on Workplace Email, Web Browsing and Privacy', 30 March: http://www.privacy.gov.au/issues/p7_4.html (visited 15 January 2001).

Organisation for Economic Cooperation and Development (OECD) 1980, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980, OECD, Paris: http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM (visited 19 August 2001).

—— 1998, *Ministerial Declaration on the Protection of Privacy on Global Networks*, 18 December, OECD, Paris: http://appli1.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)10-final (visited 19 August 2001).

—— 1999, *Recommendation of the Council of the OECD Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce*, 9 December, OECD, Paris: http://www.oecd.org//dsti/sti/it/consumer/prod/guidelines.htm (visited 19 August 2001).

Pakistan Information Technology Commission 2001, 'Electronic Government Program': http://www.itcommission.gov.pk/itnews/pakistan_electronic_gov.htm (visited 8 August 2001).

Parliament of the Commonwealth of Australia 2001, 'Cybercrime Bill 2001 (Cwlth)': http://www.aph.gov.au/legis.htm (visited 10 August 2001).

Pawlyna, A. 2001, 'Programmes all Set to Bust Computer Crime', *South China Morning Post*, Supplement, 13 January, p. 7.

Pearson, G. 1996, 'Naked Men, Food and Water: Marketing Law and Codes of Practice', *Current Commercial Law*, vol. 4, no. 1, pp. 21–32.

Phillips, T. 1999, 'Internet Fraud and the Financial Services Sector', Paper presented to the 1999 *Internet Fraud Summit*, 19 April, Sydney.

Philippsohn, S. 2000, 'An Overview of Electronic Crime in the 21st Century', *Intersec: The Journal of International Security*, April: http://www.afp.gov.au/ecrime/21c.htm (visited 16 January 2001).

Pongvutitham, A. 2000, 'Thai Ministry Pushes New E-Commerce Laws', *The Nation*, 2 March: http://www.newsbytes.com/news/00/144933.html (visited 12 September 2001).

Quatloos 2001, 'Dominion of Melchizedek: Fake Nation Scam': http://www.quatloos.com/groups/melchiz.htm (visited 10 August 2001).

Rai, S. 2001, 'In Rural India, a Passage to Wirelessness', *The New York Times*, Technology Section, 4 August.

Reporters Sans Frontières 2001: http://www.rsf.fr/uk/homennemis.html (visited 1 August 2001).

Reserve Bank of Australia 2000, 'The Australian Payments System': http://www.rba.gov.au (visited 21 November 2000).

Reuters 1999, 'South Korea Passes E-commerce Legislation', *NUA*, 13 January: http://nua.ie/surveys/index.cgi?f=VS&art_id=905354623&rel=true (visited 10 August 2001).

Ringin, S. 2000, *Report to the Winston Churchill Memorial Trust of Australia on Fellowship to Investigate Ways to Counter the Production and Use of Counterfeit Documents*, Melbourne.

Royal Canadian Mounted Police (RCMP) 2001, 'What is Computer and Telecommunication Crime?': http://www.rcmp-grc.gc.ca/html/cpu-cri.htm (visited 10 July 2001).

SES Research 2001, 'B2B Growing for Canadian Small Firms', *NUA*, 14 May: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356759&rel=true (visited 10 August 2001).

Schauble, J. 2001, 'Internet Use on the Rise in China', *The Age* (Melbourne), 14 August, p. 8: http://www.theage.com.au/news/world/2001/08/14/FFX0SX25BQC.html (visited 18 August 2001).

Silicon Valley News 2001, 'Church on Crusade to Wire the Philippines', *NUA*, 5 January: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356314&rel=true (visited 10 August 2001).

Sinclair, J. 2001, 'Korean Trade Visit a Boon for Local Firms', *The Age* (Melbourne), 31 July, pp. IT1–IT7.

Slane, B. 2001, 'Catching the Fast Slithering Tail of E-Privacy', Address by the Privacy Commissioner of New Zealand to IIR *Web Law Conference*, Auckland, 25–26 June: http://www.privacy.org.nz/news5.html (visited 9 August 2001).

Smith, C.G. 2001, 'In China, New Economy is Being Absorbed into the Old', *New York Times*, 6 July: http://www.nytimes.com/2001/07/06/technology/06NET.html?todaysheadlines (visited 6 August 2001).

Smith R.G. 1997, 'Internet Piracy', *Trends and Issues in Crime and Criminal Justice*, No. 65, Australian Institute of Criminology, Canberra: http://www.aic.gov.au/publications/tandi/tandi65.html (visited 15 August 2001).

—— 1999, 'Identity-Related Economic Crime: Risks and Countermeasures', *Trends and Issues in Crime and Criminal Justice*, No. 129, Australian Institute of Criminology, Canberra: http://www.aic.gov.au/publications/tandi/tandi129.html (visited 15 August 2001).

Smith, R.G., Holmes, M.N. and Kaufmann, P. 1999, 'Nigerian Advance Fee Fraud', *Trends and Issues in Crime and Criminal Justice*, No. 121, Australian Institute of Criminology, Canberra: http://www.aic.gov.au/publications/tandi/tandi121.html (visited 15 August 2001).

Standards Australia 1998, *Compliance Programs*, AS 3806-1998, Standards Association of Australia, Sydney.

Suddle, M.S.S. 2000, 'Internet-related and Other High-tech Crime' (Pakistan perspective), *8th Asia Crime Prevention Foundation (ACPF) Conference on Crime Prevention and Criminal Justice*, 11–15 October, Beijing: http://www.acpf.org/WC8th/AgendaItem2/I2%20PpSuddle,Islamabad.html (visited 15 August 2001).

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.

Sussmann, M.A. 1999, 'The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium', *Duke Journal of Comparative and International Law*, vol. 9, no. 2, pp. 451–89.

Swain, P. (Hon. Associate Minister for Justice, New Zealand) 2000, 'Crimes Amendment Bill (No. 6): Referral to Law and Order Committee', *New Zealand Parliament Hansard*, 16 November: http://rangi.knowledge-basket.co.nz/hansard/han/text/2000/11/16_032.html (visited 15 August 2001).

Tan, K.H. 2000, 'Prosecuting Foreign-Based Computer Crime: International Law and Technology Collide', paper presented to the *Symposium on Rule of Law in the Global Village*, Palermo, Sicily, 12–14 December.

Tomazin, F. 2001, 'Internet Fraud Man Sentenced', *The Age* (Melbourne), 23 May 2001.

Tweney, D. 1998, 'Sex Scam Points Out Lack of Safeguards in Online Business', 3 August: http://cnn.com/TECH/computing/9903/11/net.schemes.ap/ (visited 15 March 1999).

United States, Department of Justice 1999, *Report of the Computer Crime and Intellectual Property Section, Working Group on Unlawful Conduct on the Internet:* http://www.cybercrime.gov/index.html (visited 5 July 2000).

—— 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).

United States Department of Justice and Federal Bureau of Investigation 2001, 'Internet Fraud Complaint Center': http://www.ifccfbi.gov (visited 15 August 2001).

Urbas, G. 2000, 'Public Enforcement of Intellectual Property Rights', *Trends and Issues in Crime and Criminal Justice*, No. 177, Australian Institute of Criminology, Canberra: http://www.aic.gov.au/publications/tandi/tandi177.html (visited 15 August 2001).

—— 2001, 'Cybercrime Legislation in the Asia Pacific Region', Background Paper prepared for the *Asia Cybercrime Summit (First Regional Conference on Piracy and Cybercrime)* held at the Centre for Criminology at the University of Hong Kong, 25–26 April 2001.

Victoria Police and Deloitte Touche Tohmatsu 1999, *Computer Crime and Security Survey*, Victoria Police Computer Crime Squad and Deloitte Touche Tohmatsu, Melbourne.

Villafania, A.F. 2001, 'Philippines' NBI Clamps Down on "Cyberthieves"', *Metropolitan Computer Times*, 13 June: http://www.newsbytes.com/news/01/166778.html (visited 10 August 2001).

Visa International 2001: http://www.visa.com (visited 15 August 2001).

Warton, A. 1999, 'Electronic Benefit Transfer Fraud: The Challenge for Federal Law Enforcement', *Platypus Magazine: The Journal of the Australian Federal Police*, No. 65, December, pp. 38–44.

Weir, S. 2001, 'Cyber Crime High on Penalty Hit-list', *The Advertiser* (Adelaide), 3 July 2001.

Williams, D. 1999, 'Law and the Government: Past, Present and the Future', *Law Institute Journal*, vol. 73, no. 12, pp. 62–66.

Wired News 1999, 'China Jails a Software Pirate', *Wired News*, Reuters Ltd: http://www.wired.com/news/politics/0,1283,21003,00.html (visited 15 August 2001).

World Bank 2001, '2001 Development Indicators, Power and Communications (5.9)': http://www.worldbank.org (visited 7 August 2001).

Worldwide Electronic Commerce Fraud Prevention Network (WECFPN) 2001a, 'How Vulnerable Are You to Fraud?': http://www.merchantfraudsquad.com/pages/test.html (visited 9 August 2001).

—— 2001b, 'Security on the Internet': http://www.merchantfraudsquad.com/pages/shopsafe.html#secure (visited 9 August 2001).

World Wide Web Consortium (W3C) 2001, 'Platform for Internet Content Selection (PICS)': http://www.w3.org/PICS/ (visited 15 August 2001).

Yankee Group 2001, 'E-commerce Thriving in South Korea', *NUA*, 3 May: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356724&rel=true (visited 10 August 2001).

Yeang, S.C. 2001, 'Curbing Attacks on Websites', *New Straits Times*, 14 January, p. 23.

Zhongguo Xinwen She 2000, 'China Passes Internet Security Law', 29 December: http://www.chinaonline.com/issues/internet_policy/NewsArchive/Secure/2000/December/C00122805.asp (visited 31 May 2001).

Appendix

Guidelines on Fraud Minimisation for Organisations Engaged in Electronic Commerce

Adapted from: Organisation for Economic Co-operation and Development (OECD) 1999, *Recommendation of the Council of the OECD Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce*, 9 December 1999, OECD, Paris; http://www.oecd.org//dsti/sti/it/consumer/prod/guidelines.htm.

Part One: Scope

- These guidelines apply to business-to-business and business-to-government transactions. (Business-to-consumer transactions are dealt with in the OECD's Guidelines for Consumer Protection in the Context of Electronic Commerce).
- Reference to an organisation in these guidelines includes businesses and corporations as well as government agencies engaged in electronic commerce.

Part Two: General Principles

I. Transparent and Effective Protection

- Parties engaged in electronic commerce should be afforded transparent and effective protection that is not less than the level of protection afforded in other forms of commerce.
- Governments and businesses should work together to achieve such protection and determine what changes may be necessary to address the special circumstances of electronic commerce.

II. Fair Business, Advertising and Marketing Practices

- Organisations engaged in electronic commerce should pay due regard to the interests of other parties to transactions and act in accordance with fair business, advertising and marketing practices.

- Organisations engaged in electronic commerce should not make any representation, or omission, or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair.
- Organisations selling, promoting or marketing goods or services should not engage in practices that are likely to cause unreasonable risk of harm to other parties.
- Whenever organisations make information available about themselves or the goods or services they provide, they should present such information in a clear, conspicuous, accurate and easily accessible manner.
- Organisations engaged in electronic commerce should comply with any representations they make regarding policies or practices relating to their transactions with other parties.
- Organisations engaged in electronic commerce should take into account the global nature of electronic commerce and, wherever possible, should consider the various regulatory characteristics of the markets they target.
- Organisations engaged in electronic commerce should not exploit the special characteristics of electronic commerce to hide their true identity or location, or to avoid compliance with business protection standards and / or enforcement mechanisms.
- Organisations engaged in electronic commerce should not use unfair contract terms.
- Advertising and marketing should be clearly identifiable as such.
- Advertising and marketing should identify the organisation on whose behalf the marketing or advertising is being conducted where failure to do so would be deceptive.
- Organisations engaged in electronic commerce should be able to substantiate any express or implied representations as long as the representations are maintained, and for a reasonable time thereafter.
- Organisations engaged in electronic commerce should develop and implement effective and easy-to-use procedures that allow other parties to choose whether or not they wish to receive unsolicited commercial email messages.
- Where parties have indicated that they do not want to receive unsolicited commercial email messages, such choice should be respected.
- In a number of countries, unsolicited commercial email is subject to specific legal or self-regulatory requirements.

III. Online Disclosures

A. Information about the Business or Agency

- Organisations engaged in electronic commerce should provide accurate, clear and easily accessible information about themselves sufficient to allow, at a minimum:
  - (i) identification of the organisation—including the legal name of the organisation and the name under which the organisation trades or operates; the principal geographic address for the organisation; email address or other electronic means of contact, or telephone number; and, where applicable, an address for registration purposes and any relevant government registration or licence numbers;
  - (ii) prompt, easy and effective communication with the organisation;
  - (iii) appropriate and effective resolution of disputes;
  - (iv) service of legal process; and
  - (v) location of the organisation and its principals by law enforcement and regulatory officials.
- Where an organisation publicises its membership in any relevant self-regulatory scheme, business association, dispute resolution mechanism or other certification body, the organisation should provide appropriate contact details and an easy method of verifying that membership and of accessing the relevant codes and practices of the certification body.

B. Information about the Goods or Services

- Organisations engaged in electronic commerce should provide accurate and easily accessible information describing the goods or services offered; sufficient to enable other parties to make an informed decision about whether to enter into the transaction and in a manner that makes it possible for those parties to maintain an adequate record of such information.

C. Information about the Transaction

- Organisations engaged in electronic commerce should provide sufficient information about the terms, conditions and costs associated with a transaction to enable other parties to make an informed decision about whether to enter into the transaction.

- Such information should be clear, accurate, easily accessible, and provided in manner that gives other parties an adequate opportunity for review before entering into the transaction.
- Where more than one language is available to conduct a transaction, organisations should make available in those same languages all information necessary for other parties to make an informed decision about the transaction.
- Organisations engaged in electronic commerce should provide to other parties a clear and full text of the relevant terms and conditions of the transaction in a manner that makes it possible for those parties to access and maintain an adequate record of such information.
- Where applicable and appropriate given the transaction, such information should include the following:
  - (i) an itemisation of total costs collected and / or imposed by the organisation;
  - (ii) notice of the existence of other routinely applicable costs that are not collected and / or imposed by the organisation;
  - (iii) terms of delivery or performance;
  - (iv) terms, conditions, and methods of payment;
  - (v) restrictions, limitations or conditions of purchase, such as approval requirements, geographic or time restrictions;
  - (vi) instructions for proper use including safety and health care warnings;
  - (vii) information relating to available after-sales service;
  - (viii) details of and conditions related to withdrawal, termination, return, exchange, cancellation and / or refund policy information; and
  - (ix) available warranties and guarantees.
- All information that refers to costs should indicate the applicable currency.

IV. Confirmation Process

- To avoid ambiguity concerning another party's intent to enter into a transaction, the other party should be able to identify precisely the nature of the transaction; identify and correct any errors; express an informed and deliberate consent to the transaction; and retain a complete and accurate record of the transaction.

- Another party should be able to cancel the transaction before concluding the purchase.

V. Payment

- Organisations engaged in electronic commerce should provide easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford.
- Limitations of liability for unauthorised or fraudulent use of payment systems, and chargeback mechanisms offer powerful tools to enhance business confidence and their development and use should be encouraged in the context of electronic commerce.

VI. Dispute Resolution and Redress

A. Applicable Law and Jurisdiction

- Business-to-business and business-to-government cross-border transactions, whether carried out electronically or otherwise, are subject to the existing framework on applicable law and jurisdiction.
- Electronic commerce poses challenges to this existing framework. Therefore, consideration should be given to whether the existing framework for applicable law and jurisdiction should be modified, or applied differently, to ensure effective and transparent protection in the context of the continued growth of electronic commerce.
- In considering whether to modify the existing framework, governments should seek to ensure that the framework provides fairness to all parties to such transactions, facilitates electronic commerce, results in parties having a level of protection not less than that afforded in other forms of commerce, and provides parties with meaningful access to fair and timely dispute resolution and redress without undue cost or burden.

B. Alternative Dispute Resolution and Redress

- Organisations engaged in electronic commerce should ensure access to fair and timely alternative dispute resolution and redress without undue cost or burden.
- Businesses and governments should work together to continue to use and develop fair, effective and transparent self-regulatory and other policies and procedures, including alternative dispute resolution mechanisms, to address complaints and to resolve disputes arising from business-to-business and business-to-government electronic commerce, with special attention to cross-border transactions.

- Business and government representatives should continue to establish fair, effective and transparent internal mechanisms to address and respond to complaints and difficulties in a fair and timely manner and without undue cost or burden. Parties transacting with businesses and governments should be encouraged to take advantage of such mechanisms.
- Business and government representatives should continue to establish co-operative self-regulatory programs to address complaints and to assist in resolving disputes arising from business-to-business and business-to-government electronic commerce.
- Businesses and governments should work together to continue to provide the option of alternative dispute resolution mechanisms that provide effective resolution of the dispute in a fair and timely manner and without undue cost or burden.
- In implementing the above, businesses and governments should employ information technologies innovatively and use them to enhance business awareness and freedom of choice.
- In addition, further study is required to meet the objectives of Section VI at an international level.

VII. Privacy

- Business-to-business and business-to-government electronic commerce should be conducted in accordance with the recognised privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980), and taking into account the OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998).

VIII. Education and Awareness

- Business and government representatives should work together to promote education about electronic commerce, to foster informed decision-making by parties engaging in electronic commerce, and to increase business and government awareness of the protection framework that applies to their online activities.
- Business and government representatives, the media and educational institutions should make use of all effective means to educate parties engaging in electronic commerce, including innovative techniques made possible by global networks.

- Business and government representatives should work together to provide information to parties engaging in electronic commerce globally about relevant protection laws and remedies in an easily accessible and understandable form.

Part Three: Implementation

- Countries to which these guidelines apply should, at the national and international level, and in cooperation with business and government representatives:
  - (i) review and, if necessary, promote self-regulatory practices and / or adopt and adapt laws and practices to make such laws and practices applicable to electronic commerce, having in mind the principles of technology and media neutrality;
  - (ii) encourage continued private sector leadership that includes the participation of business and government representatives in the development of effective self-regulatory mechanisms that contain specific, substantive rules for dispute resolution and compliance mechanisms;
  - (iii) encourage continued private sector leadership in the development of technology as a tool to protect and empower parties transacting with business and government;
  - (iv) promote the existence, purpose and contents of the guidelines as widely as possible and encourage their use; and
  - (v) facilitate parties' ability to both access education information and advice, and file complaints related to electronic commerce.

Part Four: Global Cooperation

- In order to provide effective protection in the context of global electronic commerce, countries to which these guidelines apply should:
  - (i) facilitate communication, cooperation and, where appropriate, the development and enforcement of joint initiatives at the international level among businesses and governments;
  - (ii) through their judicial, regulatory and law enforcement authorities cooperate at the international level, as appropriate, through information exchange, coordination, communication and joint action to combat cross-border fraudulent, misleading and unfair commercial conduct;

(iii) make use of existing international networks and enter into bilateral and / or multilateral agreements or other arrangements as necessary and appropriate, to accomplish such cooperation;

(iv) work toward building consensus, both at the national and international levels, on core protections to further the goals of enhancing business confidence, ensuring predictability for businesses and governments, and protecting parties engaging in electronic commerce;

(v) cooperate and work toward developing agreements or other arrangements for the mutual recognition and enforcement of judgments resulting from disputes arising from electronic commerce transactions, and judgments resulting from law enforcement actions taken to combat fraudulent, misleading or unfair commercial conduct.