Part III. OECD Policy Guidance on Online Identity Theft

The following are extracts from the OECD Policy Guidance on Online Identify Theft, which followed the OECD Ministerial Meeting on the Future of the Internet Economy in Seoul, Korea on 17-18 June 2008.

I. Introduction

Identity theft ("ID theft") is a longstanding problem which, as the Internet and E-commerce have developed, has expanded to include online forms. While the scope of online ID theft appears to be limited in most countries, its implications are significant as the growing risk of such theft can undermine consumer confidence in using the Internet for E-commerce. Governments have acted to fight against such fraud (both online and offline) at the domestic and international levels. The *1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* ("the 1999 Guidelines") and the *2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* ("the 2003 Guidelines"), for example, set out principles aimed at strengthening member countries' frameworks to fight offline and online fraud. Outside the OECD, international instruments such as the Council of Europe's *Cybercrime Convention* and the United Nations' *Convention against Transnational Organised Crime* have been developed to address the issue.

The principles in the 1999 and 2003 *Guidelines* serve as a solid basis for establishing a framework to fight online ID theft and other fraud. The purpose of this paper is to describe how the principles presented in these instruments could be elaborated to strengthen and develop effective member country strategies to combat online ID theft. It explores, in particular, how education and awareness of stakeholders could be enhanced to prevent such theft. The guidance draws largely on the research and analysis contained in a *Scoping Paper on Online Identity Theft* that was considered by the Committee on Consumer Policy in 2007 (OECD, 2008).

ID theft definition, forms and methods

ID theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes. Although this definition encompasses both individuals and legal entities, focus in the present guidance is limited to identity theft affecting consumers.

Traditionally, ID theft has been committed by accessing information acquired from public records, theft of personal belongings, improper use of databases, credit cards, and checking and saving accounts and misusing that information. As described in Box 1 below, off-line, unauthorised access to personal data can be carried out by various means, including dumpster diving, payment card theft, pretexting, shoulder surfing, skimming, or business record theft.

Box 1. Traditional ways to access personal data for ID theft

Dumpster diving: generally refers to the act whereby fraudsters go through bins to collect "trash" or discarded items. It is the means that identity thieves employ to obtain copies of individuals' cheques, credit card or bank statements, or other records that contain their personal information.

Pretexting: pretexters are parties who contact a financial institution or telephone company, impersonating a legitimate customer, and request that customer's account information. In other cases, the pretext is accomplished by an insider at the financial institution, or by fraudulently opening an online account in a customer's name.

Shoulder surfing: refers to the act of looking over someone's shoulder or from a nearby location as the victim enters a Personal Identification Number ("PIN") at an ATM machine.

Skimming: the capturing of personal data from the magnetic stripes on the backs of credit cards; data is then transmitted to another location where it is re-encoded onto fraudulently made credit cards.

Business record theft: refers to situations where someone steals data from a business (*e.g.* stolen computers or files) or bribes insiders to obtain the information from the business or organisation.

On line, there are principally three methods to obtain victims' personal information (see Box 2): *i*) software designed to collect personal information is secretly installed on someone's computer or device – fixed or mobile (*i.e.* malware); *ii*) deceptive e-mails or websites are used to trick persons into disclosing personal information (*i.e.* phishing – phishing e-mails are often mass-distributed via spam; they are increasingly used to install malware on the computers of recipients.); and *iii*) computers or mobile devices are hacked into or otherwise exploited to obtain personal data.

Box 2. Online methods for stealing personal information

Malware: a general term for a software code or programme inserted into an information system in order to cause harm to that system or to other systems, or to subvert them for use other than that intended by their own users. Viruses, worms, Trojan horses, backdoors, keystroke loggers, screen scrapers, rootkits, and spyware are all examples of malware (See Glossary for definitions of these terms).

Spam: commonly understood to mean unsolicited, unwanted and harmful electronic messages (OECD, 2006c) and is increasingly being viewed as a vector for malware and criminal phishing scams.

Phishing: a method that thieves use to lure unsuspecting Internet users' personal identifying information through emails and mirror-websites which look like those coming from legitimate businesses, such as financial institutions or government agencies. Typically, a phishing attack is composed of the following steps:

The phisher sends its potential victim an e-mail that appears to be from an existing company. The e-mail uses the colours, graphics, logos and wording of the company.

The potential victim reads the e-mail and provides the phisher with personal information by either responding to the e-mail or clicking on a link and providing the information via a form on a website that appears to be from the company in question.

Through this, the victim's personal information is directly transmitted to the scammer.

Hacking: exploiting vulnerabilities in electronic systems or computer software to steal personal data.

Prevalence

ID theft is an increasing problem victimising individuals across all ages and social categories. Box 3 describes the ways that identity thieves misuse consumers' personal information both off line and on line. Online ID theft has been recognised as the source of growing concerns for consumers in recent years, having a direct impact on E-commerce transactions, including mobile commerce (OECD, 2006c, p. 21). As noted in the *EU 2006 Special Eurobarometer* (European Commission, 2006, p. 12), the use of the Internet to purchase goods and services online is rather limited (only 27% of the EU population in 2005), and is mostly restricted to domestic commerce. Such

limited use reflects, in part, consumers' lack of trust in E-commerce transactions, fearing that their personal information could be stolen.[1]

Box 3. Traditional and online methods of misusing personal information

Misuse of existing accounts: Identity thieves use victims' existing accounts, including credit card accounts, cheque/savings accounts, telephone accounts (both landline and wireless service), Internet payment accounts, E-mail and other Internet accounts, and medical insurance accounts.

Opening new accounts: Identity thieves use victims' personal information to open new accounts, including telephone accounts (both landline and wireless service), credit card accounts, loan accounts, cheque and savings accounts, Internet payment accounts, auto insurance accounts, and medical payment accounts.

Commit other frauds: Identity thieves also misuse victims' personal information by giving it to the police when stopped or charged with a crime, by using it to obtain medical treatment, services, or supplies, by using it in rental housing situations, by using it to obtain government benefits, and by using it in employment situations.

Efforts to combat ID theft

In recent years, a number of member countries have put programmes in place for addressing ID theft. Such programmes, which tend to have strong educational and awareness aspects, target broad audiences including consumers, key employees from the public and private sector and law enforcement. An analysis of the challenges being faced suggests that efforts to combat online ID theft have three key aspects:

Prevention – what stakeholders can do to lower the risk of identities being stolen (*e.g.* ways to enhance identity security, ways to identify attempts and instances of identity theft, and ways to limit the magnitude and scope of incidents).

Deterrence – what stakeholders can do to discourage parties from engaging in ID theft (*e.g.* legal sanctions).

Recovery and redress – what stakeholders can do to facilitate recovery and redress of such harms as financial detriment, injury to reputation, and other non-monetary harms.

This guidance focuses on the prevention of the acquisition of personal information in the online environment. Section II provides ideas on how stakeholders can use education and enhanced awareness to *i*) help

consumers avoid falling victim to ID theft and *ii*) help business and government fight more effectively against the problem. Section III deals specifically with initiatives that could be taken to educate business on ways to improve data security, while Section IV addresses issues related to identity authentication. Finally, Section V identifies areas where further work on ways to combat online ID theft would be beneficial. While the guidance is geared to online ID theft, it should be noted that many of the measures suggested are equally applicable to offline ID theft.

II. Ways that education and awareness could be enhanced to prevent online ID theft

Educating consumers, business, government officials, and the media, and raising awareness about online ID theft are indispensable to reducing risks of theft. Reducing these risks would strengthen consumer trust in E-commerce. As stated in the *1999 Guidelines*, "Governments, businesses and consumers representatives should work together to educate consumers about electronic commerce... to increase business and consumer awareness of the consumer protection framework that applies to their online activities" (OECD, 1999, Section VIII). This recommendation, which also appears in the *2003 Guidelines* (OECD, 2003, Section II. F), is directly relevant to online ID theft. Online ID theft is a fraudulent activity which has become increasingly complex, relying on ever changing high-tech methods. Tackling it requires concerted, collaborative efforts by all stakeholders (*i.e.* government, business, and consumers). Education and awareness are therefore necessary to ensure that both consumers and businesses are aware of the importance of the problem, and knowledgeable about its evolving forms.

Structuring education and awareness programmes

Effective education and awareness programmes require: *i*) development of compelling and informative educational materials; and *ii*) development of institutions and techniques to deliver the materials and education to stakeholders in efficient ways. Moreover, co-operation and co-ordination of initiatives among parties can provide important opportunities to exploit synergies and strengthen efforts. It is thus important to involve stakeholders at an early point in developing programmes; insights from different perspectives can help to better determine what the precise education/awareness needs are, what the target audiences might be, and how they could best be reached.

Collection of relevant information on online ID theft

The collection and dissemination of basic information on online ID theft are key to raising awareness and knowledge of the importance of the problem and ways to combat it. There are five basic types of information that it would be useful to develop: *i*) statistical information showing developments and trends; *ii*) information on the non-economic effects of ID theft; *iii*) factual material on the methods that parties are using to steal identities, *iv*) general tips on how to protect identity, including tools that consumers and business could use to block online intrusions, and *v*) information on techniques that can be used to identify or recognise efforts to misuse identity information.

Statistical information showing developments and trends

In introducing and maintaining an effective framework to limit the incidence of fraudulent practices against consumers, the 2003 *Guidelines* call on member countries to provide for "effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent ... practices" (OECD, 2003, Section II. A. 2). Awareness of the scope and scale of the problem is a key element in support of education campaigns. However, to date, information on developments and trends in online ID theft is not generally available, despite growing member country warnings that it is on the rise. Moreover, when data are available, they rarely include sufficient detail on online forms of ID theft (OECD, 2008).

It would be beneficial for stakeholders to explore ways to enhance the development of statistical information tracking developments in ID theft. It would be helpful if this information provided specific information on online ID theft. One of the indicators that has been used in this regard is the number of consumer complaints. It would be interesting to explore what other indicators may be helpful.

In addition to measuring the magnitude of ID theft, it could be useful to monitor its economic impact on individuals and countries. Such information would further highlight and illustrate the scale of the problem.

Information that is comparable from one country to another and from different sources within one country would enhance its value. The development of such information should, where possible, draw on the efforts of multilateral groups (both public and private) that are active in the area. Private-sector platforms could be used to gather, analyse and disseminate phishing, spam and virus statistics on a worldwide basis. These could include: the Anti-Phishing Working Group ("APWG," at

www.antiphishing.org), which focuses on eliminating fraud and ID theft resulting from phishing and e-mail spoofing of all types; the Messaging Anti-Abuse Working Group ("MAAWG," at *www.maawg.org*), which aims at preserving the electronic messaging from online exploits and abuse such as messaging spam, malware attacks and other forms of abuse; and DigitalPhishNet ("DPN," *www.digitalphishnet.org/default.aspx*), which is a collaborative forum where Internet Service Providers, online auction sites, financial institutions, and law enforcement agencies share statistics and best practices in real time to tackle phishing and other online threats.

Information on the indirect effects of ID theft

In addition to having economic costs, ID theft can have other effects including the time victims spend to restore their reputation, the negative effects on their reputation, and the subsequent difficulties they have to re-establish creditworthiness. Collection of such information would help provide a more complete understanding of the implications of ID theft, thereby helping to raise awareness of the problems that theft can cause.

Factual material on the methods and techniques that parties are using to steal identities

Identifying the different techniques used to commit ID theft is crucial to effectively deterring and responding to the threat. To be useful, information on these techniques needs to be collected, analysed and updated on a regular basis to keep abreast of developments. Where possible, it would be beneficial to have such information processed and shared between and among not only consumer protection enforcement actors, but also other enforcement bodies addressing the ID theft issue. ID theft indeed raises, in many cases, security, privacy and spam issues. Over the past years, ID thieves have shown a certain degree of ingenuity to get access to personal information. As indicated above, increasingly, malware and spam have been coupled with phishing.

As described in Box 4 below, phishing attacks have become ever more sophisticated, taking a variety of forms and targeting both fixed and mobile electronic devices.

It should be noted that all stakeholders can play a role in developing and sharing information on the methods and techniques being employed. To maximise the utility of information that is collected, it is important that mechanisms be in place to facilitate the sharing of the information in an effective manner.

Box 4. Phishing variants

Pharming: this method, which uses the same kind of spoofed identifiers as in a classic phishing attack, redirects users from an authentic website (e.g. a bank website) to a fraudulent site that replicates the original. When the customer connects its computer to its bank web server, a hostname lookup is performed to translate the bank's domain name (e.g. "bank.com") into an IP address. During that process, the IP address will be changed.

SmiShing: cell phone users receive text messages ("SMS") where a company confirms their signing up for one of its dating services and that they will be charged a certain amount per day unless they cancel their order at the company's website. Such a website is in fact compromised and used to steal personal information.

Vishing: in a classic spoofed e-mail, appearing from legitimate businesses or institutions, the phisher invites the recipient to call a telephone number. When calling, the target reaches an automated attendant, requesting personal data such as account number, or password for pretended "security verification" purposes. Victims feel usually safer in this way as they are not required to go to a website to transmit their personal information.

Information on the level of sophistication of online ID techniques

In addition to understanding the process by which online ID theft can be committed, education campaigns need to warn consumers about the ever evolving forms of these methods. Phishing messages used to be quite unsophisticated and mostly text-based. For example, through the so-called "419 scam" (also well known as the online "Nigerian scam" or offline "Nigerian letter"), phishers tried to commit advance fee fraud by requesting upfront payment or money transfer from their targets. They usually offered to share a large amount of money with their potential victims that they would transfer out of their country. Victims were then asked to pay fees, charges or taxes to help release or transfer the money. However, victim of its own success, this scam is today very well known among Internet users and is not used as much anymore.

Thus, understanding the need for more complex scams, phishers have developed new ways to trick consumers into revealing passwords, bank account numbers and other personal data. Phishing scams now increasingly contain well-designed images and logos copied from legitimate commercial institutions. They have also become more personalised, sometimes containing the first digits of their targets' credit card numbers - which may actually be found on all credit cards of the same bank – to further convince

their potential victim that the message is coming from their own bank. Similar to real commercial offers, phishing scams contain multiple solicitations inviting targets to reveal the password, age, address, *etc*.

And while phishers traditionally used well-known top level domain names such as ".com", ".biz" or ".info", they now attempt to avoid detection by using domain names from small island countries, such as ".im" from the UK Isle of Man, which are in many cases unknown to spam filters (McAfee, 2006, p. 15). Some phishing scams now even contain self-signed digital certificates to use the "HTTPS" security protocol and trigger the security padlock icon on spoofed websites.

Keeping consumers and other stakeholders informed of new and evolving techniques is key to enhancing prevention.

General tips on how to protect identity while on line

Providing stakeholders with practical advice on ways to protect their identities (see Box 5) can contribute significantly to lowering the risk of, or preventing, online ID theft. A number of organisations and governments have developed tips in these areas. One of the most comprehensive and extensive initiatives was undertaken by the United States Government, which maintains a website providing information on ways to protect personal information and avoid Internet fraud (*http://onguardonline.gov/index.html*), including ID theft.

Box 5. Consumer anti-phishing tips from OnGuardOnline.gov

Install anti-virus and anti-spyware software, as well as a firewall on your fixed or mobile device and update them regularly.

Avoid clicking on a link in a message that you think is spam and also make it a policy never to respond to e-mail or pop up messages that ask for your personal or financial information. Also, do not cut and paste a link from the message into your web browser. Phishers can make links look like they go one place, but then they actually take you to a look-alike site.

Never disclose your credit card number or security digits in response to a message you suspect is spam. If you are concerned about your account, contact the organisation using a phone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself.

Forward the phishing scam to law enforcers and/or to industry groups such as the APWG, DPN or MAAWG. You may also forward phishing e-mails to the FTC at spam@uce.gov. In addition to industry groups and law enforcement agencies, you may also forward the phishing e-mail to the organisation that is being spoofed.

Dissemination of information

Assuring that stakeholders are aware of, and have ready access to information on ID theft is key to enhancing prevention. At the very least, such information should be available on the Internet. In addition, orientation or training sessions in schools or on a group basis would be beneficial. Moreover, television and radio also provide opportunities to engage the public, as would the availability of printed or electronic materials (*e.g.* CD and DVD). Finally, Internet service providers and heavily frequented websites, such as search engines or auction sites, could serve as an important vehicle for pointing consumers to relevant information developed by governments and other interested parties.

Co-ordination of education and awareness initiatives

Co-ordination of education and awareness initiatives provides opportunities for enhancing their effectiveness, especially to the extent that it increases coherence and simplifies efforts. Such co-ordination can take place within and between the private and government sectors, on local, national and international platforms. Such co-ordination would help identify and expand the use of particularly effective practices. Internet service providers, for example, are in an excellent position to highlight the importance of online ID theft, and point subscribers to educational resources.

It should be noted that education and awareness initiatives are multifaceted; within government, for example, the training of persons responsible for enforcement of laws covering ID theft is an important aspect of enhancing awareness and limiting the magnitude and scope of ID theft. A number of countries are already active on this front.

International law enforcement networks such as the International Consumer Protection Enforcement Network ("ICPEN") and the London Action Plan ("LAP") could be used as platforms to help co-ordinate and disseminate educational information across OECD member countries (OECD, 2003, Section III. D).

III. Data security

Data security is also a key component of any strategy to combat ID theft. Data compromises have many harmful consequences, including exposing consumers to the threat of ID theft, exposing the entity whose system was breached to legal liability for failure to secure the data, and imposing the risk of substantial costs for all parties involved. Accordingly,

member countries should develop and ensure compliance with data security safeguards, such as laws and regulations, industry standards and guidelines, and private contractual arrangements that impose data security requirements, including, if appropriate, initiating investigations and enforcement actions against entities that violate the laws governing data security.

- Member countries should better educate the private sector on safeguarding data and encourage organisations that collect and maintain sensitive consumer information to implement practical security measures to protect consumer data.

IV. Electronic authentication

Electronic authentication has been recognised as a useful process permitting the verification and management of identities on line. Under the 2006 OECD *Guidance on Electronic Authentication,* which sets out a number of operational principles aimed at helping member countries establish or modernise their approaches to authentication, the concept is understood as a function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communication system. As such, it can be an effective deterrent to the theft or misuse of personal information.

Education on the benefits and proper uses of authentication are critical for user confidence on line.

As set forth in the 2007 *OECD Recommendation on Electronic Authentication* encouraging member countries to establish compatible, technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities, OECD countries should take steps to raise the awareness of all participants of the benefits of the use of electronic authentication at both domestic and international levels.

Electronic authentication is today considered as an element of the emerging concept of identity management. Such a broader system, which would seek to allow users to interact on line while minimising the amount of personal information they reveal on line, will be the subject of strong consideration by OECD countries in the years to come.

V. Further work

As indicated at the outset, there are three key aspects of combating online ID theft: *i*) prevention, *ii*) deterrence and *iii*) recovery and redress. This paper focused on prevention, looking specifically at ways that

consumers and other stakeholders could be educated to prevent online ID theft. There is, however, a pressing need to address other aspects of the issue. Outside the OECD, the United Nations Office on Drugs and Crimes ("UNODC") is co-operating with the United Nations Commission for International Trade Law ("UNCITRAL"), developing recommendations for best practices in the prevention, deterrence, and recovery from ID theft. The European Commission is working on a harmonised definition of the concept and is considering whether online ID theft should be criminalised throughout the EU. As indicated in the *Scoping Paper on Online Identity Theft* (OECD, 2008), work is also being carried out within many OECD governments by different agencies, and by the private sector.

Some of the issues that need to be addressed at the domestic and international levels (by the OECD and other international bodies) include:

- Legal:
  - Should ID theft be defined legally as a specific offence?
  - What sorts of dissuasive sanctions might be appropriate (such as fines, confiscations, black lists, etc.)?
  - What legal remedies should be available for victims?
  - Should legislation require companies to take more steps to prevent identity theft, such as disclosing data security breaches affecting their customers when those breaches could result in identity theft, or improving authentication of consumers and customers when providing services or transactions?
- Cross-border enforcement co-operation between and among consumer protection enforcement authorities and the private sector.
  - How could cross-border co-operation among enforcement authorities be strengthened in the following areas?
  - Investigative and information sharing powers with foreign authorities, business and industry, consumer representatives.
  - Assistance, training, and support of other countries' law enforcement efforts.
  - Implementation and exchange of "best practices" in the area of consumer education.

- Identity recovery and redress
  - What assistance should government, industry, and/or civil society develop to help consumers restore their identity and recover from their monetary and non-monetary losses resulting from ID theft?
  - Should redress mechanisms be made available for consumers, and if so, what entities should be responsible for such redress?
  - What additional tools are needed by victims to ensure that they can restore their identity and otherwise recover fully from the identity theft?

Note

1. A 2006 *International Telecommunication Union Online Survey* (ITU, 2006) concluded that more than 40% of Internet users refrain from transacting on line for that reason.

Glossary

Backdoors: A malicious software program that allows an attacker to access a system by listening to commands on a certain User Diagram Protocol ("UDP") or Transmission Control Protocol (TCP) port. Backdoors facilitate the attacker's acquisition of information such as passwords and allows the attacker to execute remote commands.

Bots and botnets: Some malware is distributed using botnets, a group of "zombies" or bots infected computers compromised though malware and turned into malware that can be used to carry out attacks against other computer systems. These computers become compromised when a bot program, a type of malware, is installed on the system.

Dumpster diving: Generally refers to the act whereby fraudsters go through bins to collect "trash" or discarded items. It is the means that identity thieves employ to obtain copies of individuals' cheques, credit card or bank statements, or other records that hold their personal information.

Keystroke loggers: A program that records and "logs" how a keyboard is used. There are two types of keystroke loggers. The first type of keystroke logger requires the attacker to retrieve the logged data from the compromised system. The second type of keystroke logger actively transmits the logged data.

Man-in-the-middle attack: The process by which the phisher collects personal data through the interception of an Internet user's message that was intended to be sent to a legitimate site.

Pharming: The use of deceptive e-mail messages to redirect users from an authentic website to a fraudulent one, which replicates the original in appearance.

Phishing: The use deceptive e-mails to get users to divulge personal information, includes luring them to fake bank and credit-cards websites.

Pretexting: A form of social engineering used to obtain sensitive information. In many instances, pretexters contact a financial institution or telephone company, impersonating a legitimate customer, and request that customer's account information. In other cases, the pretext is accomplished

by an insider at the financial institution, or by fraudulently opening an online account in the customer's name.

Rootkit: A set of programs designed to conceal the compromise of a computer at the most privileged base or 'root' level. As with most malware, rootkits require administrative access to run effectively, and once achieved can be virtually impossible to detect.

Shoulder surfing: In relation to ID theft, refers to the act of looking over someone's shoulder or from a nearby location as the victim enters her Personal Identification Number ("PIN") at an ATM machine.

Skimming: The recording of personal data from the magnetic stripes on the backs of a credit cards; data is then transmitted to another location where it is re-encoded onto fraudulently made credit cards.

SMiShing: The sending of text messages ("SMS") to cell phone users that trick them into going to a website operated by the thieves.

Spam: Commonly understood to mean unsolicited, unwanted and harmful electronic messages. here appears to be a growing correlation between malware and spam.

Spyware: A form of malware that sends information from a computer to a third party without the user's permission or knowledge. Different types of Spyware may collect different types of information. Some Spyware tracks the websites a user visits and then sends this information to an advertising agency while malicious variants attempt to intercept passwords or credit card numbers as a user enters them into a web form or other applications.

Trojan horse: A computer program that appears legitimate but which actually has hidden functionality used to circumvent security measures and carry out attacks. Typically a Trojan enters a user's computer by exploiting a browser vulnerability or feature.

Virus: A hidden software program that spreads by infecting another program and inserting a copy of itself into that program. A virus requires a host program to run before the virus can become active. The term "virus" is increasingly used more generically to refer to both viruses and worms.

Vishing: Phishing via Voice over Internet Protocol ("VoIP").

VoIP: A new technique using phones to steal individuals' personal information.

Worm: A type of malware that self replicates without the need for a host program. Worms can exploit weaknesses in a computer's operating system or other installed software and spread rapidly via the Internet. A mass-mailing worm is a worm that is spread out through bulk e-mail.

Bibliography

ACCC (Australian Competition and Consumer Commission) (2003), Court declares imitation Sydney Opera House website illegal, press release, 28 August 2003: *www.accc.gov.au/content/index.phtml/itemId/360431/fromItemId/378016*.

ACPR (Australian Centre for Policing Research) (2006), Review of the legal status and rights of victims of identity theft in Australasia, Report Series No. 145.2, Commonwealth of Australia: *www.acpr.gov.au/pdf/ACPR145_2.pdf*.

ANSI (American National Standards Institute) and BBB (Better Business Bureau) (2008) ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel Final Report, 31 January 2008, *www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3*.

APEC (2006), Letter of Support from the Chair of the Telecommunications and Information Working Group, 20 March 2006, Strasbourg: *www.coe.int/T/E/Legal_affairs/Legal_cooperation/Combating_economic_crime/6_Cybercrime/T-CY/*.

APEC (Asian-Pacific Economic Co-operation) (2005), Strategy to Ensure a Trusted, Secure and Sustainable Online Environment, November 2005: *www.apec.org/apec/apec_groups/working_groups/telecommunications_and_information.html*.

APWG (Anti-Phishing Working Group) (2006a), Phishing Activity Trends, report for November 2006: *www.antiphishing.org/reports/apwg_report_november_2006.pdf*.

APWG (2006b), Phishing Activity Trends, report for December 2006: *www.antiphishing.org/reports/apwg_report_december_2006.pdf*.

APWG (2007), Phishing Activity Trends, report for April 2007: *www.antiphishing.org/reports/apwg_report_april_2007.pdf*.

ASWPRPCC (Australasian and South West Pacific Region Police Commissioners' Conference) (2005), Australasian Identity Crime Policing Strategy 2006-2008, report produced by the ACPR, December: 2005: *www.acpr.gov.au/pdf/ID%20Crime%20Strat%2006-08.pdf*.

British Telecom, CPP, Get Safe Online, Lloyds TSB, Metropolitan Police, Yahoo! (UK) (2006): Security Report, February 2006, *www.btplc.com/onlineidtheft/onlineidtheft.pdf*.

BWGCBMMF (2004), Report on Identity Theft, report to the Ministry of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, October 2004, *www.ps-sp.gc.ca/prg/le/bs/report-en.asp*.

BWGCBMMF (Bi-national Working Group on Cross-Border Mass Marketing Fraud) (US-Canada) (2006), Report on Phishing, October 2006, report to the Ministry of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States: *www.psepcsppcc.gc.ca/prg/le/_fl/Phishing%20for%20CBCF%202006-en.pdf*.

CAO (Cabinet Office) (Japan) (2006), Summary Report on the Enforcement Status of Act on the Protection of Personal Information in Fiscal Year 2005, June 2006: *www5.cao.go.jp/seikatsu/kojin/foreign/enforcement-status2005.pdf*.

CMC (Consumer Measures Committee) (Canada) (2005), Working Together to Prevent Identity Theft, A discussion paper for public consultation, 6 July 2005: *http://cmcweb.ic.gc.ca/epic/site/cmc-cmc.nsf/vwapj/Discussion%20Paper_IDTheft.pdf/$FILE/Discussion%20Paper_IDTheft.pdf*.

Deloitte Touche Tohmatsu, 2006 Global Security Survey: *www.deloitte.com/dtt/cda/doc/content//CA_FSI_2006%20Global%20Security%20Survey_2006-06-13.pdf*.

ENISA (European Network and Information Security Agency) (2006), Survey on Industry Measures taken to comply with National Measures implementing Provisions of the Regulatory Framework for Electronic Communications relating to the Security of Services, 2006: *www.enisa.europa.eu/pages/05_01.htm*.

European Commission (2007), Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, Towards a General Policy on the Fight against Cyber Crime, 22 May 2007, COM(2007) 267 FINAL, *http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf*.

European Commission (2006), DG SANCO, Special Eurobarometer, Consumer Protection in the Internal Market, September 2006, Brussels, *http://ec.europa.eu/public_opinion/archives/ebs/ebs252_en.pdf*.

European Commission (2004), Identity Theft: A Discussion Paper, Joint Research Centre, Institute of the Protection and Security of the Citizen, EUR 21098 EN, 2004.

European Commission FPEG (EC Fraud Prevention Expert Group) (2007), Report on Identity Theft/Fraud, FPEG, subgroup on identity theft, 22 October 2007: *http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf*.

Europol (2006), EU 2006 Organised Crime Threat Assessment ("OCTA"): *www.europol.eu.int/publications/OCTA/OCTA2006.pdf*.

GetSafeOnline (UK) (2006), The Get Safe Online Report, October 2006: *www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf*.

Home Office Identity Fraud Steering Committee (UK) (2006), Identity Crime Definitions: *www.identitytheft.org.uk/definition.html*.

IDTTF (Identity Theft Task Force) (US) (2007), Combating Identity Theft: A Strategic Plan, 23 April 2007: *www.idtheft.gov*.

INTERVICT (International Victimology Institute Tilburg) (2006), The Challenge of Countering Identity Theft, Report Commissioned by the National Infrastructure Cyber Crime program ("NICC"), 6 September 2006, *www.tilburguniversity.nl/intervict/publications/NicolevanderMeulen.pdf*

ITRC (Identity Theft Resource Center) (US) (2004), Identity Theft: the Aftermath 2004, September 2005: *www.idtheftcenter.org/prteen1006.pdf*.

ITTC (Identity Theft Technology Council) (US), Online Identity Theft: Phishing Technology, Chokepoints, and Countermeasures, 3 October 2005, *www.antiphishing.org/Phishing-dhs-report.pdf*.

International Telecommunication Union (2006), Cybersecurity Awareness Survey, results as of 17 May 2006, *www.itu.int/newsroom/wtd/2006/survey/charts/q_8.asp*.

Javelin Strategy and Research (2006), 2006 Identity Fraud Survey Report, *www.javelinstrategy.com/products/AD35BA/27/delivery.pdf*.

Javelin Strategy and Research (2007), 2007 Identity Fraud Survey Report - Identity Fraud Is Dropping, Continued Vigilance Necessary, Consumer Version, February 2007, *www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf*.

McAfee Avert Labs (2004), Anti-Phishing: Best Practices for Institutions and Consumers, White Paper, September 2004, *www.antiphishing.org/sponsors_technical_papers/AntiPhishing_Best_Practices_for_Institutions_Consumer0904.pdf*.

McAfee Avert Labs (2007), Identity Theft, White Paper, January 2007, *www.mcafee.com/us/threat_center/white_paper.html*.

McAfee (2006), Virtual Criminality Report, December 2006, *www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf*.

Microsoft (2006), presentation by Nancy Andersen, Microsoft Vice-President, contribution to the European Commission's conference on "Maintaining the integrity of identities and payments: Two challenges for fraud prevention," The Threat of Cybercrime: The Challenge of Online Identity Theft and Strengthening the Public-Private Partnership in a Changing Threat Environment, 22 November 2006, Brussels, *http://ec.europa.eu/justice_home/news/information_dossiers/conference_integrity/doc/Presentation_Anderson.pdf*

NCL (National Consumer League) (UK) (2006), A Call for Action: Report from the National Consumer League, Anti-Phishing Retreat, Washington D.C., March 2006, *www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf*.

OECD (2006c), OECD Anti-Spam Toolkit of Recommended Policies and Measures, OECD, Paris, *www.oecd-antispam.org/*.

OECD (2009) Computer Virues and Other Malicious Software: A Threat to the Internet Economy.

OECD (2007d), The Development of Policies for the Protection of Critical Information Infrastructures, OECD, Paris, [DSTI/ICCP/REG(2007)20/FINAL].

OECD (1999), Guidelines for Consumer Protection in the context of Electronic Commerce, OECD, Paris, *www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1, 00.html*.

OECD (2003), Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, OECD, Paris: *www.oecd.org/sti/consumer-policy*.

OECD (1980), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, Paris: *www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1, 00.html*.

OECD (2002), Guidelines for the Security of Information Systems and Networks, OECD.

OECD (2006b), Mobile Commerce, DSTI/CP(2006)7/FINAL, Directorate for Science, Technology and Industry, *www.oecd.org/sti/consumer-policy*.

OECD (2006b), OECD Anti-Spam Toolkit of Recommended Policies and Measures, OECD, Paris: *www.oecd-antispam.org/*.

OECD (2006d), Protecting Consumers from Cyberfraud, OECD Policy Brief, Paris, October 2006: www.oecd.org/sti/crossborderfraud.

OECD (2007c), Recommendation and Guidance on Electronic Authentication, OECD, Paris: *www.oecd.org/dataoecd/32/45/38921342.pdf*.

OECD (2007b), Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD, Paris: *www.oecd.org/dataoecd/43/28/38770483.pdf*.

OECD (2007), Recommendation on Consumer Dispute Resolution and Redress, OECD, Paris, *www.oecd.org/dataoecd/43/50/38960101.pdf*.

OECD (2006a), Report on the Implementation of the 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, OECD, Paris, www.oecd.org/dataoecd/45/53/37125909.pdf.

OECD (2008), Scoping Paper on Online Identity Theft, DSTI/CP(2007)3/FINAL, Directorate for Science, Technology and Industry.

Table of Contents

Executive Summary 7

Part I. The Scope of Online Identity Theft 13

Chapter 1. **The Problem Posed by Online Identity Theft** 15

A new Internet landscape 15
What is identity theft? 15
ID theft's main elements 16

Chapter 2. **Online Identity Theft: Tools of the Trade** 21

ID theft based solely on malware 21
Key drivers of online ID theft: Phishing and its variants 22
Phishing techniques 24
Phishing evolution and trends 27
What online ID thieves do with the data: credit card fraud and other abuses 29

Chapter 3. **The Impact of Online Identity Theft** 33

Defining the victims 33
Victims' direct and indirect losses 36
Are there more victims off line than on line? 39
Remediation tools for victims 40

Part II. Addressing Online Identity Theft 45

Chapter 4. **The Role of Government** 47

How OECD countries currently define ID theft 47
The option of criminalising ID theft 50
Public education and awareness campaigns 51

Annex 4.1 ID Theft: Education and Government Initiatives in OECD Countries 62

Annex 4.2 United States Initiatives to Combat Identity Theft 67

Chapter 5. **Private Sector Initiatives: What Role for Industry and Internet Service Providers?** 73

A serious private-sector threat 73

Annex 5.1 Private-Sector Initiatives to Educate Consumers about ID Theft 78

Chapter 6. **International, Bilateral and Regional Initiatives** 81

International organisations 81
International informal networks 84

Annex 6.1 Multilateral Instruments Addressing Online ID Theft 98

Annex 6.2 United Nations Study on Identity Fraud 100

Chapter 7. **Online Identity Theft: What Can Be Done?** 105

Enhancing education and awareness 105
Dissemination of information 109
Co-ordination of education initiatives 110
Authentication and data security 111
Electronic authentication 111
Areas for further work 112

Chapter 8. **Conclusions and Recommendations 115**

Part III. OECD Policy Guidance on Online Identity Theft 117

I. Introduction 118
II. Ways that education and awareness could be enhanced to prevent online ID theft 122
III. Data security 127
IV. Electronic authentication 128
V. Further work 128

Glossary 131

Bibliography 133