Part I. The Scope of Online Identity Theft

Part I of this book examines the multiple facets of the ID theft problem and the different methods used to perpetrate ID theft via the Internet. Chapter 2 describes the techniques implemented by ID thieves to lure victims online, which increasingly involve the use of spam and malware, and how thieves abuse this stolen information. Chapter 3 focuses on ID theft victims. It draws on the available statistical data reflecting victims' complaints and losses trends, and it questions whether ID theft is more prevalent off line than on line.

Chapter 1. The Problem Posed by Online Identity Theft

A new Internet landscape

Over the past 10 years, the Internet has evolved into a single and integrated infrastructure where audiovisual media, publishing, and telecommunications are all converging. This low-cost and seamless communications system not only fosters growth for existing and new industries but also serves society by promoting diffusion of culture and knowledge. Today, the Internet is enhancing commercial opportunities for businesses. It is also serving as a vehicle for providing public services directly to businesses and consumers, as well as innovative personal and social activities. As such, the Internet has substantially changed both our global economy and society and its impact in the coming years is expected to be significant.

Anticipating this evolution, as early as in 1998,[1] the OECD pointed out the importance of sustainable electronic transactions for the global economy and society. At the same time, however, it warned its member economies about the dangerous sides this changing scheme could bring, one of them being the emergence of new types of online threats to the detriment of consumers and users. By nature, face-to-face client-relationships are nonexistent on the Internet. Establishing one's real identity for online transactions is complicated, thereby making fraud easier.

What is identity theft?

There is no standard definition of online, or offline, ID theft at the international level. While some countries have adopted a broad view of the concept, which usually applies to both on and offline ID theft, very few consider it as a specific offence. As a result of these different approaches, the legal nature of ID theft varies from one jurisdiction to another, leading to the application of different regimes of prevention, prosecution and sanctions.

ONLINE IDENTITY THEFT – ISBN- 978-92-64-05658-9 – © OECD 2009

ID theft is an illicit activity with multiple facets. It is generally included in a larger chain of wrongs or crimes. More specifically, ID theft is committed over different sequences of actions. This complexity has opened the path for different legal categorisations of the concept in OECD member countries, which either qualify ID theft as a specific crime, a civil wrong, or as a preparatory step in the commission of other offences such as fraud, forgery, terrorism, or money laundering.

In the absence of a globally accepted definition, this book will use the term "ID theft" as follows:

> *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 paper is limited to identity theft affecting consumers.

While some OECD member countries employ different terminology to describe the problem,[2] all of the countries addressing the issue aim to prevent fraudulent or criminal activity resulting from the misuse of personal information.[3]

ID theft's main elements

The concept of "identity" and "personal information"

ID theft is a problem involving personal information. Our society is increasingly relying on personal information to identify individuals in many circumstances. For instance, it is used to establish accounts with merchants, ISPs, phone companies, *etc.* It may also be used to get access to various accounts and record systems with financial institutions, health organisations, schools, government agencies, and other entities.

Understanding the concept of "identity" and how its components operate in different media is crucial to determine the appropriate means to protect it. The core components of identity are relatively easy to grasp. They are generally based on fixed and verifiable attributes, which are usually officially provided and registered by public authorities.[4] These attributes include individuals' gender, first and last name, date and place of birth, parents' first and last name and in some countries, individuals' assigned social security number.[5] Individuals also can be identified with a variety of

other attributes including a computer username and password, a web page, a blog, an Internet Protocol ("IP") address that identifies computers on the Internet, an e-mail address, a bank account and PIN number.

An effective fight against online ID theft will be difficult if the ways in which the different components of identity are used in the online medium are not defined. As concluded in a 2006 *Security Report on Online ID theft*, "after all, we cannot protect what we cannot define," (BT, 2006). Responding to this issue is thus a first essential step to determine how digital personal information can be made harder to steal. In Korea, an improved online identity system was introduced in October 2006 to help verify Korean citizens' identity in cyberspace.[6] The old 13-digit citizen registration number, which contains Korean citizens' personal information, was used as an identity verification means on line. However, this number, which was stored on firms' online databases, had been the subject of numerous thefts.[7] The Korean authorities thus decided to replace it by a new i-PIN number which does not contain any personal data and can be replaced in the event someone's i-PIN number has been copied or misused.

Relation to fraud and other crimes[8]

In most cases, perpetrators involved in this illicit activity aim at engaging in a variety of other wrongs for different purposes including obtaining credit, money, goods, services, employment benefits, or anything else of value to be used in the name of the victim, without consent.

ID thieves may sometimes not use the victims' identity themselves to commit fraud. Instead, they will sell it to other parties who will themselves commit fraud, or generate new illegal forms of personal identity (such as a birth certificate, driver's license, or a passport).

According to a 2004 US victimisation survey conducted by the Identity Theft Resource Centre (ITRC), the most prevalent form of ID theft was mostly financial (66 %); financial and criminal (9%); and financial, criminal and cloning (6 %) (ITRC, 2005, p. 6). Economic and financial fraud committed by the use of credit cards has clearly profited from technological advances. Owing to the growing number of people using electronic payment systems, this kind of fraud could propagate further in the coming years.

The online environment

Over the past 10 years, business-to-consumer (B2C) electronic transactions have increased. Numerous factors can help explain the increase: most firms in the OECD area have now a presence on the Net; in particular,

financial institutions offer online banking services to their customers; finally, as consumers get more experienced in buying goods or services on line, they become more aware of how to avoid e-scams. As a consequence, hardly any business wanting to benefit from commercial opportunities can today afford to remain present solely in the offline world.

Despite its potential, the growth of the e-commerce market is somewhat restrained (OECD, 2006c).[9] This is particularly true in the European Union (EU). As noted in the *EU 2006 Special Eurobarometer* (EC, 2006, p. 12), only 27% of the EU population purchased goods and services on line over the past year, and mostly on a domestic basis. One of the main reasons explaining this limited popularity is a continuing lack of full consumer confidence in the E-marketplace. The new commercial opportunities offered by the Internet have proved to be prone to inherent risks. Those risks have taken the form of sophisticated frauds which may affect consumers and users very quickly and on a global scale, while allowing perpetrators to escape detection.

Other statistics also indicate a decline in consumer confidence in e-commerce. In a 2006 online survey conducted by the Business Software Alliance and Harris Interactive, nearly one in three adults said that security fears compelled them to shop on line less, or not at all, during the 2005-2006 holiday season (US IDTTF, 2007, Vol. I, p. 11). Similarly, a Cyber Security Industry Alliance survey in June 2005 found that 48% of consumers avoided making purchases on the Internet because they feared that their financial information might be stolen (US IDTTF, 2007, Vol. I, p. 11-12). Although the studies have not correlated these consumer attitudes with online habits, these surveys indicate that security concerns likely inhibit E-commerce.

ID theft is regarded by many as one of the major risks consumers and users are exposed to in today's digital environment. E-payment and e-banking services, on which this book will mainly focus, substantially suffer from such mistrust. In the United Kingdom, for example, an estimate of 3.4 million people were prepared to use the Internet but not willing to shop on line because of a lack of trust or fears about personal security (UK OFT, 2007, p. 6).

Many member countries have noted the problem and taken steps to help ensure that consumers and users are adequately protected against ID theft. These steps encompass various actions and measures, such as consumer and user awareness campaigns, new or adapted legislative frameworks, private-public partnerships, and industry-led initiatives aimed at putting in place technical prevention measures and responses to the threat.

Notwithstanding the initiatives outlined above, many member countries have not sufficiently addressed the problem of ID theft. As a result, its

scope, magnitude and impact may vary from one country to another, or even from one source to another within the same country. These differences reflect the need for a more co-ordinated response at both domestic and international levels.

Notes

1. "A Borderless World: Realising the Potential of Global Electronic Commerce," OECD Ministerial Conference on Electronic Commerce, 7-9 October 1998, Ottawa, Canada, at *www.ottawaoecdconference.org/english/homepage.html*.
2. See Chapter 4 for a description of the terminology used in various OECD member countries as well as in international and regional organisations.
3. The concept of "personal information" refers to identification or authentication data.
4. These attributes are contained in official documents such as passports, identity card, birth and death certificates, social security numbers or driving licences.
5. This last element is a crucial means to identify individuals in the United States. This was also the case in the United Kingdom until recently. However, in early 2007, a new system of ID cards was introduced in the country.
6. Reference to this new Korean identity verification means may be found at: *www.vnunet.com/articles/print/2165834*.
7. In early 2006, 1.2 million Korean citizens noticed that their citizen registration number was used without their knowledge or consent to sign up for accounts in *Lineage*, a series of online games.
8. Discussion on the various forms of ID theft is further developed in Chapter 2.
9. See also the OECD Policy Brief on *Protecting Consumers from Cyberfraud*, OECD, Paris, October 2006, at: www.oecd.org/dataoecd/4/9/37577658.pdf, (OECD, 2006d).

Chapter 2. Online Identity Theft: Tools of the Trade

ID theft is an illicit activity with a long history that predates the Internet. Typically, conventional ID theft was – and still is – committed through techniques such as dumpster diving (also known as "bin raiding");[1] payment cards' theft; pretexting,[2] shoulder surfing;[3] skimming;[4] or computer theft.

In recent years, these activities have been given a modern spin through the fast development of the Internet, which, as examined below, allows ID thieves to install malicous software (malware) on computers, and to use a luring method known as "phishing," which itself can be perpetrated through the use of malware and spam.

ID theft based solely on malware[5]

Malware, is 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. With the rise of stealthy malware programs, such as "keystroke loggers," viruses or "Trojans"[6] that hide on a computer system and capture information covertly, malware is increasingly used as a standalone technical tool to steal victims' personal information.

ID thieves use various malware threats, including blended and targeted attacks, to obtain consumers' personal information.

Blended attacks (hidden)

Most malicious activity now combines several malware applications to carry out attacks. This has resulted in a change in landscape as blended malware attacks use techniques such as social engineering to circumvent established defences. One type of blended attack occurs for instance when malicious actors embed malware into a website that is otherwise legitimate.

Targeted attacks (hidden and/or self announcing)

Most targeted attacks notably seek to steal an entity's intellectual property and proprietary data. Because users throughout the world have taken more proactive steps to protect their systems, attackers have moved away from large scale attacks that seek to exploit as many occurrences of vulnerability as possible, to smaller more focused attacks. Targeted attacks often allow attackers to remain undetected by security measures (anti-virus software and firewalls), and maintain privileged access to a user's system for longer periods of time.

Key drivers of online ID theft: Phishing and its variants

The concept of "phishing" is not clearly and consistently defined in OECD member countries. Some law enforcement authorities or industry often use it as a synonym of ID theft. Others distinguish the two notions. As stated in the *OECD Anti-Spam Toolkit of Recommended Policies and Measures* (OECD, 2006c, p. 25), phishing is considered as the main method enabling cyber crooks to commit ID theft.

Background

Phishing is a term that was coined in 1996 by US hackers who were stealing America Online ("AOL") accounts by scamming passwords from AOL users. The use of "ph" in the terminology traces back in the 1970s to early hackers who were involved in "phreaking," or the hacking of telephone systems.

Phishing is today generally described as a luring method that thieves use to fish for unsuspecting Internet users' personal identifying information through e-mails and mirror-websites, which look like those coming from legitimate businesses, including financial institutions, or government agencies. A well-known phishing e-mail is the one pretending to be from a bank to customers asking for their account details. In France, for instance, in 2005, a one-stop-shop phishing scam targeted four banks' customers.

Another well-known phishing e-mail is the so-called "419 scam"[7] (also known as the "Nigerian scam" or offline as the "Nigerian letter"), through which phishers try to commit advance fee fraud by requesting upfront payment or money transfer from their targets. Phishers usually offer their potential victims to share with them a large amount of money that they want to transfer out of their country. Victims are then asked to pay fees, charges or taxes to help release or transfer the money. Victim of its own success, this

scam is today very well known among Internet users and is not used as much anymore.

Other examples of phishing e-mails or fake websites are collected and stored by the Anti-Phishing Working Group ("APWG"), an industry association aimed at eliminating ID theft and fraud resulting from phishing. The consortium, which serves as a forum where industry, business and law enforcement agencies discuss the impact of phishing, maintains a public website allowing its members to share information and best practices for eliminating the problem.[8]

Scope

A social-engineering scheme

Phishing originally entailed deceptive attacks using deceptive or "spoofed"[9] e-mails and fraudulent websites hijacking brand names of banks, e-retailers and credit card companies, with a view to deceiving Internet users into revealing personal information (OECD, 2005, p. 23). Classic phishing attacks through e-mail can be typically described as follows:

Step 1. The phisher sends its potential victim an e-mail that appears to be from this person's bank, or some other organisation that would hold personal information. The phisher in his scam carefully uses the colours, graphics, logos and wording of an existing company.

Step 2. The potential victim reads the e-mail and takes the bait by providing 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 bank or organisation in question.

Step 3. Through this fake website or e-mail, the victim's personal information is directly transmitted to the scammer.

A technical subterfuge scheme

Like the Nigerian scam, the classic phishing attack described above is nowadays well known and fraudsters have developed more sophisticated phishing variants which are more difficult to detect, if at all possible. These variants rely on specific techniques such as malware or/and spam.

In light of the above preliminary findings, phishing may be generally described as follows:

Box 2.1 Phishing process

Phishing is perpetrated through the sending of spoofed e-mail or fake websites that trick users into disclosing their personal information and enable fraudsters to commit ID theft.

- Frequently, these messages, or the websites that they link to, try to install malicious code (OECD, 2006c, p. 25).
- Examples of the type of information sought by "phishers" include credit card and PIN numbers, account names, passwords, or other personal identification numbers.
- Phishers use victims' personal information to conduct unlawful activity, typically fraud.

Phishing techniques

Increasingly, ID theft is perpetrated using malware or "crimeware" (Radix Lab, 2006, p. 4). It is also propagated through spam messages, which often themselves contain malware.

Forms of automated phishing

Although malware is not the only means by which computers can be compromised, it provides the attacker convenience, ease of use, and automation to conduct attacks on a large scale that would not otherwise be possible due to lack of skill and/or capability. Some forms of automated phishing can be illustrated by the following attacks:

"Pharming"

Malware-based phishing attacks can take various forms. A typical malware-based phishing attack is often illustrated by the technique known as "pharming" (or "warkitting"[10]), which uses the same kind of spoofed identifiers as in a classic phishing attack, but which, in addition, redirects users from an authentic website (from a bank for instance) to a fraudulent site that replicates the original in appearance. When a user connects his/her computer to, for instance, a bank web server, a hostname lookup is performed to translate the bank's domain name (such as "bank.com") into an IP address containing several digits (such as 138.25.456.562). It is during that process that crooks will interfere and change the IP address.

"Man-in-the-middle attack"

Another example of malware-based phishing can be illustrated by the so-called "man-in-the-middle attack." This expression describes 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.

In today's convergent Internet, two other techniques, relying on non-computer devices, have been recently used by phishers to perpetrate ID theft.

"SMiShing"

Phishing continues to spread by reaching external devices such as mobile phones. Through this emerging technique, cell phone users receive text messages ("SMS") where a company confirms to them that they have signed 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 the unsuspected user's personal information.

As reported by McAfee Avert Labs in August 2006, SMiShing for the first time targeted two major mobile phone operators in Spain in 2006. The scam used the two companies' own system to send texts to customers offering free anti-virus software purporting to come from the phone operator. When customers followed the link to install the software onto their computers, these were infected with malicious programs.[11] McAfee predicts that although recent, the threat of SMiShing, which is now part of the "cybercrime toolkit," will increasingly be used by malware perpetrators in the coming months (McAfee, 2006, p. 20).

"Vishing"

Voice over Internet Protocol ("VoIP") is also a new technique using phones to steal individuals' personal information. Through this means, the phisher sends a classic spoofed e-mail, disguised so as to appear from legitimate businesses or institutions, which invites the recipient to call a telephone number. Victims feel usually safer in this way as they are not required to go to a website where they would transmit their personal information. When calling, the target reaches an automated attendant, prompting her to enter personal information such as account number, password or other information for pretended "security verification" purposes. In some cases, the phisher skips the e-mail altogether and cold calls consumers, fishing for financial information.

The above described techniques based on malware are evolving and transforming into new kinds of threats on a rapid basis. They can even be mixed, as noted in 2005 by the US Identity Theft Technology Council ("ITTC") report on *Online Identity Theft* (ITTC, 2005, p. 7). The ITTC reports that "the distinctions between [phishing] attack types are porous, as many [of them] are hybrid, employing multiple technologies." The report illustrates this with the example of a deceptive phishing e-mail, which could direct a user to a site that has been compromised via content injection, and which then installs malware that poisons the user's hosts file. As a result, subsequent attempts to reach legitimate websites would be rerouted to phishing sites, where confidential information is compromised using a man-in-the-middle attack. This hybrid attack includes a pharming and man-in-the-middle attack.

Phishing vehicled through spam

Spam is another vector used for sending massive phishing hits. As described in the OECD *Anti-Spam Toolkit* (OECD, 2006c, p. 7), spam began as electronic messages usually advertising commercial products or services. Over the past few years, spam has evolved from inoffensive advertising to potentially dangerous messages which can be deceptive and may result in ID theft.

While spam messages used to be mostly text-based, they increasingly contain images. The security company adds that while spammers 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; these lesser-known domain names are often not included in spam filters (McAfee, 2006, p. 15).

Spam, phishing and malware

Although the techniques are different, spam and malware are now increasingly combined as key underpinnings of the illicit techniques fraudsters use to commit ID theft. As shown in Box 2.2 below, spam often distributes malware or direct users to infected sites aimed at creating new infected computers (OECD, 2006b).

Box 2.2 The Haxdoor example

A series of identity theft Trojan attacks were directed against Internet users in Australia between March and August 2006. Attackers used spam that contained embedded links to malicious sites to conduct the attacks. When users clicked on the link provided in the spam e-mail, they were sent to a URL containing a commercial malware kit known as WebAttacker. WebAttacker then scanned the computer system to determine which exploit would be most effective in compromising the system. Once WebAttacker determined the proper exploit, the user was directed to another webpage within the same domain and a Trojan known as "Haxdoor" was downloaded. Haxdoor then disabled various security counter-measures so that when the users visited websites, Haxdoor began capturing passwords and other data. The data captured by Haxdoor were then sent to a domain registered to the attacker. The attacker used this domain to harvest the data on a periodic basis. In one case, a computer belonging to a company in Australia was compromised by Haxdoor for approximately 14 weeks and three days. During this time, the attacker was able to access the individual's personal data including credit card details, as well as personal information for other employees in the company.

Phishing evolution and trends

Today's ID theft perpetrators are viewed as professionals. They seem to increasingly belong to organised groups which use ID theft to commit other serious crimes such as drug trafficking, money laundering, vehicle theft and illegal immigration (McAfee, 2007, p. 10; UN IEG, 2007). Their illicit actions can remain unsuspected in many cases as they are more and more relying on the help of "innocent" intermediaries, such as students.[12] Moreover, they become ever more sophisticated.

More sophisticated and tailored attacks

At the origin of the phenomenon, ID theft messages were poorly designed. They included signs of weaknesses such as: rudimentary textual errors; English-language in messages addressed to non-English individuals.

In contrast, today's phishing scams contain well-designed logos and typical messages that appear to be from real companies or institutions. To fight against this threat, in the United States, the Intellectual Property Governance Task Force[13] has been created to encourage trademark owners to employ technical measures to prevent their brands from being abused by phishers.

More targeted attacks

While continuing to target high-profile banks and e-commerce sites, phishers now try to reach fewer victims, but in more personalised ways, thereby potentially becoming even more dangerous. McAfee's 2006 *Virtual Criminality* report (McAfee, 2006, p. 11) reveals that fraudsters are changing the content of their phishing mails away from "update your details now" scams to more tailor-made messages.

They can also send false personalised e-mails to other small groups such as employees through a technique known as "spear-phishing." In such a case, the sender impersonates a colleague or the employer to steal employees' passwords and username and to ultimately gain access to the employees' company's entire computer system.

Phishing trends

Phishing is considered as a serious threat that is on the rise. A large and diverse population of fraudsters ranging from expert hackers to inexperienced individuals who can even purchase phishing kits on line have exploited the Internet and other technological tools to wreak havoc on innocent victims.[14]

In 2006, the Netcraft toolbar, an anti-phishing tool developed by the Netcraft toolbar Community,[15] blocked more than 609 000 confirmed phishing URLs, a substantive jump from only 41 000 in 2005.[16] Netcraft views this dramatic surge, mainly concentrated in November – December 2006, as the result of recent techniques implemented by phishers to automate and propagate networks of spoof pages, enabling the rapid deployment of entire networks of phishing sites on cracked web servers.[17]

The Anti-Phishing Working Group's ("APWG") November 2006 *Phishing Activity Trends* report confirms a jump in cyber attacks from July to November 2006 (APWG, 2006a). In November 2006, 37 439 new phishing sites were detected, a 90% increase since September 2006. However, in its December 2006 report (APWG, 2006b), the APWG notes a decrease in the number of new phishing sites (which dropped to 28 531).

According to the APWG's April 2007 statistics (APWG, 2007), as shown in the pie chart below, phishing websites that host malicious code or have Trojan downloads are hosted in several different countries, with the most websites hosted in the United States (38.57%), followed closely by China (37.64%) and Russia (8.87%).

What online ID thieves do with the data: credit card fraud and other abuses

Once ID thieves obtain victims' personal information, they misuse it in a variety of ways. The US Federal Trade Commission (FTC) *2006 Identity Theft Survey Report* classifies ID theft victims in one of the three main following categories:

1. New Accounts (such as new credit card, bank accounts, or loans) and Other Frauds (such as obtaining medical care);
2. Misuse of Existing Non-Credit Card Accounts; or
3. Misuse of Existing Credit Cards Only (US FTC, 2007b, p. 12).18 The most commonly reported forms of misuse of both existing credit card and non-credit card accounts perpetrated by means of ID theft were as follows (US FTC, 2007b, p. 17):

   - Credit card fraud (61%)
   - Checking or savings accounts (33%)
   - Telephone service accounts (11%)
   - Internet payment accounts (5%)
   - E-mail and other Internet accounts (4%)
   - Medical insurance (3%)
   - Others (1%)

As reflected above, credit card fraud is the most common form of misuse of existing accounts. This form of ID theft occurs when the ID thief obtains the actual credit card, the numbers associated with the account, or the information derived from the magnetic strip on the back of the card. Since credit cards can be used remotely, for example via the Internet, ID thieves are often able to commit fraud without physically possessing the victims' credit card.

ID thieves also commit new account fraud by using the victims' personal information to open an account, incur excessive charges, and then disappear. Victims often do not discover the ID theft until they are contacted by a debt collector or denied a job, loan, car, or benefit because of a negative credit rating. In some instances, ID thieves deposit stolen or counterfeit cheques, or cheques drawn on insufficient funds, and withdraw cash, causing immediate financial harm that is typically in large amounts (US IDTTF, 2007, Vol. I, p. 19-20). Although this form of ID theft is less prevalent, it can cause more financial injury, is less likely to be discovered quickly, and requires the most time for victim recovery.

Indeed, the US FTC's *2006 ID Theft Survey Report* indicates that 24% of New Accounts and Other Fraud victims did not find out about the misuse of their information until at least six months after it started – compared to just 3% of Existing Credit Cards Only and Existing non-Credit Card Account victims. In the Existing Credit Cards Only and Existing Non-Credit Card Accounts categories, the median amount of time that elapsed before victims discovered that their personal information was being misused was between one week and one month. For the New Accounts & Other Frauds category, the median value was between one and two months (US FTC, 2007b, p. 24).

Some 17% of ID theft victims reported that the thief used the victim's personal information to open at least one new account. The most common type of accounts victims reported thieves opening were as follows (US FTC, 2007b, p.19):

- Telephone service accounts (8%)
- Credit card accounts (7%)
- Loans (3%)
- Cheque / savings (2%)
- Internet payment accounts (2%)
- Auto insurance (1%)
- Medical insurance (0.4%)
- Other accounts (2%)

Some 12% of victims reported that their personal information was misused in non-financial ways (US FTC, 2007b, p.21). The most common such use, which was reported by 5% of victims, was the use of the victim's name and identifying information when the ID thief was stopped by law enforcement authorities or charged with a crime.

Other increasingly popular forms of ID theft include the misuse of personal information to obtain passports or government ID numbers (social security numbers in the United States), particularly by illegal immigrants, fraudulent requests for taxpayer refunds, and health care fraud. In particular, health care fraud may put victims at risk of receiving improper medical care due to inaccurate entries in their medical records, or having their medical insurance coverage depleted by the ID thief (US IDTTF, 2007, Vol. I, p. 20).

ID thieves may also use victims' personal information to engage in data brokering. For example, certain websites, known as "carding sites," traffic stolen credit card data all over the world. The US Secret Service estimates that the two largest current carding sites collectively have nearly 20 000 member accounts (US IDTTF, 2007, Vol. I, p. 20).

Notes

1. 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.

2. Pretexting is another 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. (See US IDTTF, 2007, Vol. I, p. 17). The US FTC has brought three cases against financial pretexters and five cases against telephone pretexters. Information on these cases is available at: *www.ftc.gov/opa/2002/03/pretextingsettlements.htm* and *www.ftc.gov/opa/2006/05/phonerecords.shtm.*

3. 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.

4. Skimming is 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.

5. Malware-related information may also be found in OECD, 2008.

6. Technical terms are defined in the Glossary.

7. This scam, which was originally committed off line, has been called "Nigerian" as, since the beginning of the 1990s, it has come primarily from Nigeria. The "419" part of the name comes from the Nigerian Criminal Code section which outlaws the practice. According to Wikipedia, the free Internet encyclopedia, as the Nigerian letter has become well known to potential targets, gangs operating it have developed variants. The targets are now often told that they are the beneficiaries of an inheritance or are invited to impersonate the beneficiary of an unclaimed estate.

8. More details about the APWG may be found in Chapter 3.

9. The term "spoof" covers any falsification of an Internet identifier such as an e-mail address, domain name or an IP address (OECD, 2005, p. 23).

10. See reference to this term at: *www.technologynewsdaily.com/node/5151*.

11. Reference to this case may be found at: *www.avertlabs.com/research/blog/?p=75*.

12. Jeevan Vasagar, *Internet criminals signing up students as "sleepers," The Guardian*, 8 December 2006, at: *www.guardian.co.uk/crime/article/0,,1967227,00.html*.

13. *See: www.ipgovernance.com/About_Us.html.*

14. See press release at: *http://fr.news.yahoo.com/12012007/7/un-kit-de-phishing-pour-les-novices-circule-sur-le.htmlb*.

15. The Netcraft toolbar Community is a digital neighbourhood watch scheme in which expert members act to defend all Internet users against phishing frauds. Once the first recipients of a phishing e-mail have reported the target URL, it is blocked for toolbar users who subsequently access that same URL. See more details at: *http://toolbar.netcraft.com/*.

16. Netcraft Toolbar Community, 2007, at: *http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html*.

17. These packages, known broadly as Rockphish or R11, each included dozens of sites aimed at spoofing major banks.

18. In 2003, the US FTC sponsored a first similar telephone survey of US adults, as described in its *2003 Identity Theft Survey Report* (US FTC, 2003). The aim of the survey was to estimate the incidence of ID theft victimisation, measure the impacts of ID theft on the victims, identify actions taken by victims, and explore measures that may help them in future ID theft cases. Based on the knowledge gained from the 2003 survey, FTC staff changed certain elements of the survey methodology for the 2006 survey, to more accurately capture consumers' identity theft experiences. Because of these methodological changes, estimates of the losses from ID theft in the two surveys cannot be directly compared (US FTC, 2007b, p. 8). The 2006 survey may not capture all forms of ID theft and, in particular, situations where a fictitious identity was created by combining personal information from one or more consumers with invented information may not have been captured as this form of ID theft (called "synthetic ID theft") is not always detectable by the consumer(s) whose information was used.

Chapter 3. The Impact of Online Identity Theft

Determining the impact of online ID theft is a challenging exercise. As mentioned earlier, the absence of a common legal approach to criminalising ID theft complicates matters. As a result, data measuring the extent to which ID theft can be harmful present significant weaknesses which distort the way in which the problem may be perceived. They concern a limited number of OECD member countries (including Australia, Canada, Korea, the United States, and the United Kingdom,) and may not be indicative of the situation in other countries or regions, such as the EU.

Box 3.1 Limited data on ID theft's impact on victims

- Statistics do not provide a clear picture of the notion of "victims" which either covers individuals, governments, international organisations, business and/or industry, or the economy as a whole.
- Statistics do not measure the same types of frauds or crimes and are thus incomparable.
- Statistics gathered by public authorities for policy purposes vary from those collected by private businesses for commercial purposes.
- Direct and indirect losses data do not cover all victims and all types of ID theft cases.
- Statistics do not cover all OECD member countries.

Defining the victims

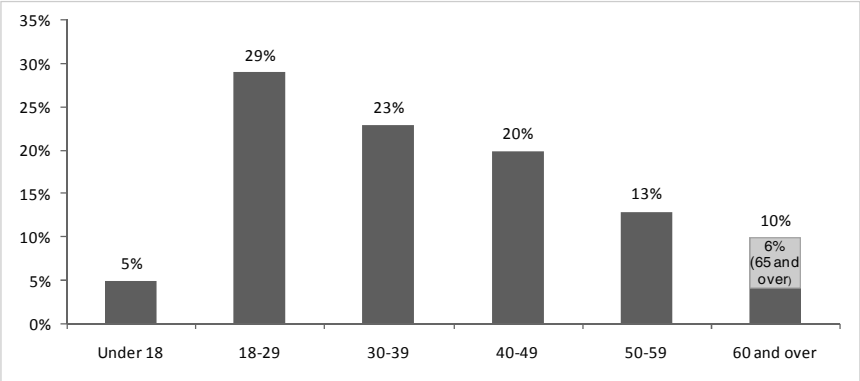
Complaint data

The category of ID theft victims could *a priori* be limited to those individuals whose personal information was misappropriated by a party, and who subsequently suffered from economic or other sorts of harms. Complaints data cover this type of victim.

According to research conducted by the Canadian Fraud Prevention Forum in 2003, the impact of ID theft in Canada extended to victims across all ages, regardless of income and levels of education (BWGCBMMF, 2004, p.4). In May 2006, over 20 000 individual phishing complaints were reported in Canada, an increase of over 34% from the previous year.

The US Federal Trade Commission's (FTC) *Consumer Sentinel*[1] 2007 report on *Consumer Fraud and Identity Theft Complaint Data* (US FTC, 2007a) confirms this finding. As illustrated in Figure 3.1 below, of the people who reported their age in their ID theft complaints, young people aged between 18-29 years experienced most ID theft (29%) in 2006, followed by persons aged 30-39 (23%).

Figure 3.1 Identity theft complaints by victim age



Note: Percentages are based on the total number of identity theft complains where victims reported their age (225 532). 94% of the victims who contacted the FTC directly reported their age.

Source: US FTC (2007a), Report on Consumer Fraud and Identity Theft Complaint Data.

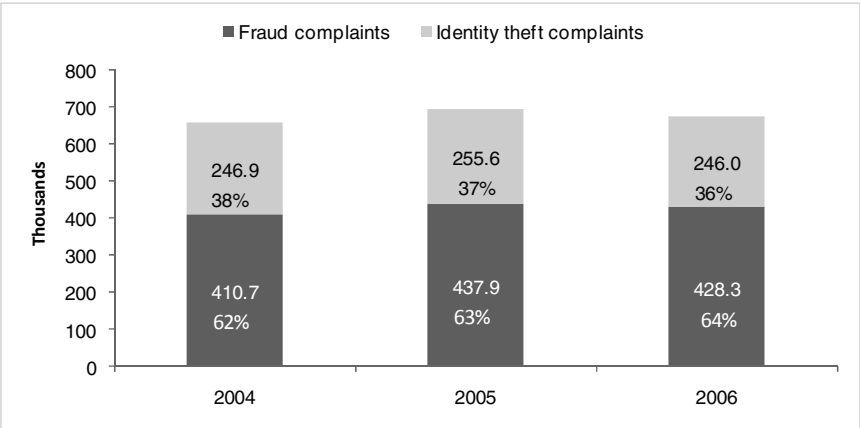
The above complaints data only reflect reported cases, and do not illustrate the fact that in reality, the concept of victim is more complex. For example, complaint data do not always reflect that businesses and institutions are also victims of ID theft. In some instances, ID thieves may misuse a customer's banking account, or may use a bank's brand name in a phishing cyber attack to steal money from one of its customers. In such a case, the bank will also be the victim of ID theft inasmuch as it would have to reimburse the sum lost to its customer.[2]

ID theft data covering certain types of fraud

Data based on the various legal formulations of ID theft are not indicative of all ID theft cases. Since ID theft sometimes refers to a crime or is absorbed in other types of frauds, data reflecting these different realities are incomplete and do not correspond from one country to another. Consequently, data are not easy to compare, if at all possible.

According to the FTC, in 2006, for the sixth year in a row, ID theft topped the list of consumer complaints, accounting for 246 035 of more than 674 354 fraud complaints filed with the agency (see Figure 3.2 below).

Figure 3.2 Sentinel complaints by calendar year



Note: Percentages are based on the total number of Sentinel complaints by calendar year. These figures exclude National Do Not Call Registry complaints.

Source: US FTC (2007a), Report on Consumer Fraud and Identity Theft Complaint Data.

The above *Consumer Sentinel* figure shows that complaints data can be classified in two categories: ID theft complaints and fraud complaints. Fraud complaints can be further broken down into Internet-related fraud complaints and other fraud complaints. However, the ID theft complaints, which are complaints involving the misuse of personal information to commit fraud, are not segregated based on whether the ID theft was perpetrated through the use of the Internet.

Divergent public and private data

There are substantial differences between statistical information gathered by public authorities for policy purposes and by private businesses for commercial purposes.

On the one hand, some security vendors state that the scale of the threat has gone down in the past years and that consumer confidence is now on the rise. Likewise, some financial institutions, which say that the costs are relatively modest, are not willing to reveal their own financial losses. On the other hand, other private bodies advance figures reflecting an increase in ID theft.

The US FTC's *2003 ID Theft Survey Report* (US FTC, 2003, p. 4) indicated that ID theft affects approximately 10 million Americans each year and that a total of 4.6% of survey participants experienced ID theft in 2002. The *2006 ID Theft Survey Report* (US FTC, 2007b, p. 4) found that approximately 8.3 million US adults discovered that they were victims of ID theft in 2005 (a total of 3.7% of survey participants).[3] In 2007, Javelin *Identity Fraud Survey Report* funded by Visa, Wells Fargo and CheckFree,[4] found that ID fraud had fallen about 12% over a year, translating into a total fraud reduction of USD 6.4 billion.

However, the Javelin report was criticised and regarded as trying to persuade the opinion that "business are doing an adequate job in protecting consumers' personal information and that the onus in on consumers to better protect themselves."[5] A 2007 McAfee survey noted this discrepancy, considering Javelin's percentages as "surprisingly low" (McAfee, 2007, p. 11) and comparing them to Gartner statistics, which, in contrast, in 2007, counted 15 million Americans as victims of ID theft.[6]

Adding to the confusion, some financial institutions even claim that none of their customers has ever been affected by a phishing attack, fearing damages to their reputation.[7]

Victims' direct and indirect losses

As mentioned above, ID theft is not a crime in itself under a vast majority of OECD member country legislation, the costs borne by victims are buried in statistics for various forms of frauds or crimes (UN IEG, 2007, p. 62). Moreover, data available alternatively refer to the costs borne by one country's economy, consumers, or consumers and business.

Victims' direct loss

In the United Kingdom, the Home Office estimates that ID fraud costs GBP 1.7 billion *to the UK economy*, compared to GBP 1.2 billion in 2002.[8] According to APACS, the UK payments association, online banking fraud continues to increase, costing the UK industry GBP 22.5 million in the first half of 2006, against GBP 14.5 million in the same period in 2005.

In the United States, according to Gartner 2007 statistics, the *average loss of funds in a case of ID theft* was USD 3 257 in 2006, up from USD 1 408 in 2005. In addition, the average loss in the opening of a fraudulent new account more than doubled over that time, from USD 2 678 to USD 5 962.[9] Based on the Javelin 2007 survey, ID theft is costing *the US industry and consumers* USD 49.3 billion annually.[10] According to a 2006 UK industry and law enforcement security report, in the United States, in 2005, 2.4 million consumers have reported losing money following a phishing attack (BT, 2006, p. 9).

In Australia, as reported by McAfee in 2007 (McAfee, 2007, p. 10), "[*estimates of the costs to the country's economy of ID fraud*] vary from less than USD 1 billion (from the Securities Industry Research Centre of Asia-Pacific) to more than USD 3 billion (Commonwealth Attorney-General's Department) per year."

According to a 2006 Computer Security Institute and FBI study surveying more than 600 US information technology ("IT") companies,[11] losses due to security incidents would have dropped by 18%, falling from USD 203 606 to USD 167 713. However, those incidents would still be significant, costing more than USD 52 billion to US IT companies.

The above variations in estimates raise the question of why data on direct losses attributed to victims of phishing vary so greatly. As observed in the *OECD Scoping Paper for the Measurement of Trust in the Online Environment*, "in part, this may be because financial institutions, while taking the threat seriously, are reluctant to publicly reveal their losses. In addition some firms may simply not know the scale of losses if they go unreported by their customers. Taken together, these factors may imply that it would be very difficult for the industry to determine a definitive figure for the direct financial losses attributable to phishing" (OECD, 2005, p. 25).

Victims' indirect loss

Victims' indirect loss can take many forms. Although there are not many statistics that clearly reflect the amount of indirect loss individual victims can suffer from ID theft, the US FTC and CIFAS have provided

some guidance on this issue. According to the US FTC's *2006 Identity Theft Survey Report* (US FTC, 2007b, p. 42), 16% of ID theft victims reported having difficulty obtaining or using a credit card, 10% reported being refused a cheque account or having cheques rejected. The survey reflects that a total of 37% of all ID theft victims reported having at least one of the aforementioned problems and that 21% of victims reported having more than one of these problems.

In addition, 33% of victims who had experienced one or more of these problems said that they had spent 40 hours or more resolving problems related to their ID theft. Similarly, CIFAS reports that, victims may need between 3 and 48 hours of work to sort through problems and clear their name. CIFAS adds that "in cases where a "total hijack" has occurred, perhaps involving 20-30 different organisations, it may take the victim over 200 hours and cost up to GBP 8 000 before things are back to normal."[12]

Moreover, law enforcement authorities report that consumers victimised by ID theft may lose out on job opportunities; be denied loans for education, housing, or cars as a result of negative information on their credit reports; or be arrested for crimes they did not commit. Victims also suffer indirect financial costs, including costs incurred in lawsuits initiated by creditors and in overcoming other obstacles they face in obtaining or retaining credit. In addition, they suffer the emotional toll of having their privacy violated and the frustration of attempting to restore their reputation and credit history.

The issue of liability

ID theft can occur as a result of personal, business, or government negligence. It can also take place in instances where there is no apparent negligence from any party. How ID theft occurs has implications for liability. Businesses, for example, often due to inadequate security practices, may be exposed to the theft of sensitive consumer data they hold. As a consequence, they may bear both direct and indirect losses in the form of liability suits, fines, and loss of clientele.[13]

Both legislation and voluntary business practices deal with the issue of liability. As provided in the *1999 E-commerce Guidelines* (OECD, 1999, Section V), "[L]imitations of liability for unauthorised or fraudulent use of payments systems, and chargeback mechanisms offer powerful tools to enhance consumer confidence and their development and use should be encouraged in the context of electronic commerce." Likewise, in its 2007 *Resolution on ID theft, phishing and consumer confidence,* the Transatlantic Consumer Dialogue ("TACD") recommends "the assignment of the liability for financial damages caused by ID theft or phishing to the respective companies or service providers involved and not to consumers, unless they

are proven to have acted negligently." [14] In most countries, business liability may be based on a duty for companies to provide reasonable security for all confidential data held and/or on a duty to disclose security breaches involving sensitive personal information. Such a duty, whether of a tort or contractual nature, is an important remedy tool for consumers falling victims of ID theft.[15]

In many member countries, legislation provides for ceilings of liability for the cost of fraudulent transactions by identity thieves.[16] In the United States, for example, consumer liability is limited to a maximum of USD 50 for unauthorised credit card charges; [17] for unauthorised electronic fund transfers, such liability is also limited, depending upon the timing of consumer notice to the applicable financial institution.[18] In the European Union, various instruments aim at protecting consumers from unauthorised payments. Under the 1997 European Commission's Recommendation on *transactions by electronic payment instruments and in particular the relationship between issuer and holder*,[19] consumers should bear the loss of unauthorised transactions up to a maximum of EUR 150, provided that they have not acted with extreme negligence. Under Directive 2002/65/EC *concerning the distance marketing of consumer financial services*,[20] consumers should be allowed to request cancellation of a payment where fraudulent use has been made of their payment card in connection with distance contracts, and in the event of such fraudulent use, to be re-credited with the sum paid or have it returned.[21] In the United Kingdom,[22] under the Banking Code, "[I]f someone else uses [someone's] card details without … permission for a transaction where the cardholder does not need to be present, [the cardholder] will not have to pay anything." In some countries, in addition to laws and regulations, industry practices provide consumers with "zero liability."[23]

Are there more victims off line than on line?[24]

In many instances, data does not clearly separate online ID theft cases from those occurring off line, making it difficult to assess which of the two activities is more prevalent. Whether ID theft is more dangerous on line than off line is actually a controversial issue.

Is ID theft more prevalent off line?

According to a 2006 survey by Javelin Strategy and Research ID theft is more prevalent off line than on line (JSR, 2006). Only 10% of US identity fraud cases occurred when the victim was on line, against 63% when the victim used more traditional channels. The report states that more than 90%

of identity fraud starts off conventionally by means of stolen bank statements, misplaced passwords, or bills stolen from the victim's mailbox. It concludes that if it is true that more attempts of ID theft are made on line, in only one out of 10 of those incidents did the actual successful theft of the personal data take place on the Internet. It goes on saying that this relatively low level of successful attacks is explained by the fact that a majority of leading US financial institutions have introduced adequate measures to detect and protect their customers against ID theft on line.

The conclusions of this book are however debatable. They are going against the opinion that ID theft is today more serious on line than off line.

Indeed, others have recognised the severity of the problem and noted that ID theft has a direct impact on e-commerce transactions.

According to a 2006 International Telecommunication Union online survey (ITU, 2006), more than 40% of users would refrain from transacting on line for fear that their personal information could be stolen.

Remediation tools for victims

In the United States, an important part of the multi-faceted approach to combating ID theft is developing adequate remediation tools for victims. Several federal and state laws offer victims of ID theft options to avoid or mitigate the damages caused by ID theft. Consumers are encouraged to report incidences of ID theft to the US FTC, which generates a report that may be used by law enforcement agencies to facilitate the extension of a fraud alert or to block fraudulent trade lines on a credit report.[25]

US victims of ID theft can also request one of the three Credit Reporting Agencies (Experian, Equifax, or TransUnion) to place an "initial fraud alert" on their credit report for a period of not less than 90 days, which requires creditors to confirm the consumer's identity before opening new accounts or making changes to existing accounts.[26] If a victim has an ID theft report documenting actual misuse of the consumer information, he is entitled to place a seven-year alert on his file.[27] In addition, victims may request a free copy of their credit report.[28] If the credit report contains fraudulent information as a result of the theft, the consumer may ask that the information be blocked from the credit report.[29]

ID theft victims in the United States are also advised to obtain records and application information from financial institutions that handled transactions conducted by the ID thieves in the victim's name (US IDTTF, 2007, Vol. II, p. 75).[30] In addition, US law enforcement authorities advise victims to close fraudulently opened or compromised accounts and send a

letter to debt collectors claiming a debt that the victim has not incurred (US IDTTF, 2007, Vol. II, p. 76). In some states, victims may request a "credit freeze" preventing their credit reports from being released without their express consent (US IDTTF, 2007, Vol. I, p. 46).

In Australia, people can ask credit reporting agencies to place an alert on their file if they suspect they are the victim of identity theft. The Australian Standing Committee of Attorney's General 2007 *Discussion Paper on Model Identity Crime Offences*[31] also canvases the issue of assistance that may be needed for victims of ID theft.

Notes

1. The *Consumer Sentinel* database, maintained by the US FTC, contains consumer fraud complaints that have been filed with federal, state, local, and foreign law enforcement agencies and private organisations. The *Consumer Sentinel* database also houses the Identity Theft Data Clearinghouse, the US's sole government national repository of consumer complaints about ID theft. The Clearinghouse provides investigative material for law enforcement agencies and reports that provide insight into how to combat ID theft. Access to this information via *Consumer Sentinel* enables domestic and international law enforcement partners to co-ordinate their law enforcement efforts more efficiently, although not all law enforcement agencies have access to ID theft data. The US FTC's 2007 statistics are based on information from over 115 data contributors to *Consumer Sentinel*. The statistics are based on self-reporting and, therefore, understate the number of occurrences of ID theft.
2. More discussion on liabilities may be found in the later sections of this chapter.
3. The difference between the 3.7% overall prevalence figure found in the 2006 survey and the 4.6% rate in the 2003 survey is not statistically significant using standard statistical analysis (US FTC, 2007c, p.4, footnote 3). In particular, given the sample sizes and the variances within the samples, one cannot conclude on a real decrease in ID theft.
4. See reference to this survey at: *www.networkworld.com/community/?q=node/11009* or at: *www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study/.*
5. See Annys Shin's article, *The Checkout*, press release, 6 February 2007, at: *http://blog.washingtonpost.com.*

6. See: *http://news.com.com/Study+Identity+theft+keeps+climbing/2100-1029_3-6164765.html*.

7. See Arnaud Devillard, *Le « phishing » en France, peu de victimes mais une menace grandissante*, press release, 10 April 2006: *www.01net.com/editorial/311785/cybercriminalite/le-phishing-en-france-peu-de-victimes-mais-une-menace-grandissante/*.

8. See: *www.identity-theft.org.uk/*.

9. See: *http://news.com.com/Study+Identity+theft+keeps+climbing/2100-1029_3-6164765.html*.

10. See: *www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study/*.

11. See reference to this study at: *http://solutions.journaldunet.com/0607/060726-etude-securite-csi-fbi.shtml*.

12. See CIFAS' website at: *www.cifas.org.uk/identity_fraud_is_theft_serious.asp*.

13. See this remark from the ITRC, at: *www.idtheftcenter.org/workplace.shtml*.

14. TACD's Resolution, 8th recommendation, at: *www.tacd.org/cgibin/db.cgi?page=view&config=admin/docs.cfg&id=306*.

15. See S. L. Wood and B. I. Schecter, *Identity Theft: Developments in Third Party Liability*, at: *www.jenner.com/files/tbl_s20Publications/RelatedDocumentsPDFs1252/380/Identity_Theft.pdf*.

16. For more details on this issue, see the OECD *Report on Consumer Protections for payments Cardholders*, DSTI/CP(2001)3/FINAL, (OECD, 2001).

17. 15 U.S.C. § 1643; 12 C.F.R. § 226.12(b).

18. 15 U.S.C. 1693g; 12 C.F.R § 205.6(b). For further discussion on this issue, see Annex 4.A2 to this book.

19. Commission Recommendation 97/489/EC of 30 July 1997 *concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder* (text with EEA relevance), at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997H0489:EN:NOT*.

20. Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 *concerning the distance marketing of consumer financial services*, Official Journal L 271, 09/10/2002 p. 16-24, at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0065:EN:HTML*. This Directive modifies Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC.

21. Article 8 of Directive 2002/65/EC.

22. See the UK *Banking Code*, p. 21, at: www.bba.org.uk/content/1/c4/52/27/Banking_Code_05.pdf.

23. For more details, see OECD, 2001, p. 17.

24. Philippa Lawson & John Lawford, Public Interest Advocacy Centre, Ontario, Canada, *Identity Theft: The Need for Better Consumer Protection*, November 2003, *www.travel-net.com/~piacca/IDTHEFT.pdf*.

25. US Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x.

26. 15 U.S.C. § 1681c-1 (a)(1).

27. Id. at § 1681 c-1(b)(1)(A).

28. 15 U.S.C. § 1691 (j)(d).

29. 15 U.S.C. § 1681c-2.

30. See also 15 U.S.C. § 1681(g)(e).

31. See *www.ag.gov.au/www/agd/agd.nsf/Page/Modelcriminalcode_IdentityCrimeDiscussionPaper*.

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