South African Journal
of Information Management
[DoE accredited]

Secure notes Vol.5(4) December 2003

Safeguarding that personal bit

S. Berner
sberner@ecognus.com

'*[T]hings are seldom what they seem: skim milk masquerades as cream*' (Gilbert & Sullivan in HMS Pinafore 1878)

1 When bad things happen to your good name

The supposed mutability of identity in the digital era – on the Internet no one knows that you are a dog – and the pervasiveness of payment systems that do not require fact to face contact (or much authentication) have been reflected in concern about 'identity theft' and 'identity fraud'.

Identity *theft* may be characterized as assuming the identity of someone else. As such it has a long and often colourful history. The advent of the information age has created new challenges to the ability of individuals to protect the privacy and security of their personal information. One such challenge is that of identity theft, which has imposed countless hardships upon its victims. Perpetrators of this fraud use the identities of others to steal money, obtain loans and generally violate the law.

Identity theft occurs when someone uses your personal information such as your name, credit card number or other identifying information, without your permission, to commit fraud or other crimes. Economically significant ID theft today does not involve supposed heirs of the Russian tsar or the wife of the former president of the Philippines. Instead it involves misuse of your credit card or cheque book, your medical insurance or telephone line. In our digital era, a person’s identity is embodied in information rather than flesh. Identity theft is a serious crime. People whose identities have been stolen can spend months or years – and their hard-earned money – cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they did not commit.

There is also an increase in 'spoofing': e-mail or even sites that purport to emanate from a public figure or private individual. That misuse of someone else's name and e-mail address may be used to defeat restrictions on spam. It may also be used to damage a reputation, with the supposed author being incorrectly assigned responsibility for racist or other offensive comments.

Identity fraud, an associated offence, has attracted less media attention. It involves an individual manipulating personal data: adding a degree or two, deleting a conviction or a divorce, adding a few years of age (popular among teenagers facing age-based access restrictions) or taking a few years off once the individual reaches a certain age. As such it is popular among all classes, from high school students enhancing ID passes to get into nightclubs through to company directors and members of parliament buffing their profiles.

South African banks have been suffering from a spate of identity thefts for almost a year (Vecchiatto 2003). These crimes fall under the jurisdiction of the *Identification Act No. 68 of 1997*. The incidents prompted the SA Banking Council to come up with a unified strategy in July 2003 (SA Banking Council 2003) to investigate the issue and share information between the various financial organizations. Because fraudsters have been unable to breach bank security systems, they are now targeting the home computers of account holders by stealing their electronic identity, principally their PIN and access account numbers.

On the other side of the ocean, Australia is not immune to the problem either. In 2002, the Australian Bankers' Association issued a statement explaining how to protect one's financial identity (ABA 2002).

2 I know who I am – but I am not THIS person

'Who steals my purse, steals trash;
'tis something, nothing
T'was mine, tis his, and has been slave to thousands
But he that filches from me my good name
Robs me of that which not enriches him
And makes me poor indeed'
(Shakespeare, Othello, Act III Scene ii).

Typically, these crimes go unprosecuted or under-punished, making them a haven for career criminals who want a decent payoff without the prospect of jail-time. Compared to equally profitable crimes involving drug or gun trafficking, the sentencing for identity fraud is much lighter – and these folks are tough to catch. These crimes are mostly committed by a cottage industry of professionals who dive into dumpsters; steal mail or wallets; pose as prospective employers and ask for information; or tap into the Net to get information on the unsuspecting. As if that were not enough, there is also the presence of unscrupulous information brokers that sell data to anybody without asking too many meaningful questions (Bielski 2001).

Since everyone's societal identity is built on pieces of interlocking data that fit together like a puzzle, deft ID con artists can take one element, say an address, as a starting point and link it fairly rapidly to the rest to get a more complete picture of a person's financial history. Identity-related crimes can be one-hit wonders or subtly complex orchestrations of deceit, depending on the quality of information obtained and the skill of the thief.

Scanning devices (which have legitimate purposes, and therefore continue to get openly sold on the Net and off) get into the hands of criminals who work as waiters or clerks at retail outlets, while also on the payroll for organized crime. Legitimate customer information is then taken on-line, where new accounts can be opened or counterfeit cards created.

The US Federal Trade Commission, in its white paper explaining identity theft, states that there are a few indicators that a person is being subject to identity theft:

- Unexplained charges or withdrawals on financial accounts;
- failing to receive bills or other mail signalling an address change by the identity thief;
- receiving credit cards for which the victim did not apply;
- denial of credit for no apparent reason; or
- receiving calls from debt collectors or companies about merchandise or services the victim did not purchase.

The document also enumerates the ways in which identity thieves can obtain someone's

personal information which is then used (FTC 2003).

While identity theft probably cannot be prevented entirely, you can minimize your risk. As such, managing personal information wisely, cautiously and with an awareness of the issue, can help guard against identity theft.

The following are things one could do to safeguard hardcopy information (ARMA 2003):

- *Order a copy of your monthly credit report from your bank.* The credit report contains information on the credit accounts that have been opened in your name, how you pay your bills and whether you have been in default of payment. By checking your report on a regular basis you can catch mistakes and fraud before they wreak havoc on your personal finances. Do not underestimate the importance of this step.
- *Place passwords on your credit card, bank and phone accounts*. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your passport or your phone number, or a series of consecutive numbers.
- *Do not give out personal information on the phone, through the mail or over the Internet* unless you have initiated the contact or are sure you know who you are dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your mother's maiden name, account numbers, passwords and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. You can check the organization's Web site as many companies post scam alerts when their name is used improperly, or you can call customer service using the number listed on your account statement or in the telephone book.
- *Secure personal information in your home*, especially if you have roommates, employ outside help or are having service work done in your home.
- *Ask about information security procedures in your workplace*. Find out who has access to your personal information and verify that records are kept in a secure location. Ask about the disposal procedures for those records as well.
- *Guard your mail and trash from theft*. Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you are discarding and credit offers you get in the mail.
- *Before revealing any personally identifying information* (e.g. on an application), find out how it will be used and secured, and whether it will be shared with others. Ask if you have a choice about the use of your information. Can you choose to have it kept confidential? Ask for a copy of the company's privacy policy.
- *Do not carry your ID card; leave it in a secure place.* Carry only the identification information and the credit and debit cards that you will actually need.
- *Give your ID number only when absolutely necessary*. Ask to use other types of identifiers when possible.
- *Pay attention to your billing cycles*. Follow up with creditors if your bills fail to arrive on time. A missing credit card bill could mean an identity thief has taken over your account and changed your billing address to cover his or her tracks.
- *Be wary of promotional scams*. Identity thieves may use phony offers to get you to give them your personal information.
- *Keep your purse or wallet in a safe place at work*. Information stored on your computer, whether at work or at home, can be a gold-mine for identity thieves who hack into your system. The following are steps you can take to safeguard your digital information

- *Update your virus protection software regularly*, or when a new virus alert is announced. Computer viruses can have a variety of damaging effects, including introducing program code that causes your computer to send out files or other stored information. Be on the alert for security repairs and patches that you can download from your operating system's Web site. Update your operating system and browser with the latest Microsoft patches to protect your PC from exploitation. These can be downloaded from the Microsoft Web site http://www.microsoft.com.
- Make sure that no-one has *unauthorized* access to your PC.
- Make sure that the software that is loaded onto your PC via a third party is *licensed*.
- *Do not download files sent to you by strangers* or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem. Do not open suspicious or unfamiliar e-mails.
- *Ensure that you have control over the shared folders* (folders that you and others have joint access to) on your PC as a shared folder could make your PC vulnerable to unauthorized installation of suspicious software. A shared folder can be identified by a blue icon shaped in the form of a hand.
- *Use a firewall program*, especially if you use a high-speed Internet connection like cable or ADSL, which leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited guests from accessing your computer. Without it, hackers can take over your computer and access your personal information stored on it or use it to commit other crimes.
- *Use secure browser software that encrypts or scrambles information* you send over the Internet, to guard the security of your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You also can download some browsers for free over the Internet. When submitting information, look for the 'lock' icon on the browser's status bar to be sure your information is secure during transmission.
- *Try not to store financial information on your laptop unless absolutely necessary*. If you do, use a strong password: a combination of letters (upper and lowers case), numbers and symbols. Do not use an automatic log-in feature which saves your user name and password so you do not have to enter them each time you log-in or enter a site. And always log off when you are finished. That way, if your laptop gets stolen, it is harder for the thief to access your personal information.
- *Before you dispose of a computer, delete personal information*. Deleting files using the keyboard or mouse commands may not be enough because the files may stay on the computer's hard drive, where they may be easily retrieved. Use a wipe utility program to overwrite the entire hard drive. It makes the files unrecoverable. For more information, see *Clearing Information From Your Computer's Hard Drive* (www.hq.nasa.gov/office/oig/hq/harddrive.pdf) from the National Aeronautics and Space Administration (NASA).
- *Look for Web site privacy policies*. They answer questions about maintaining accuracy, access, security and control of personal information collected by the site, as well as how information will be used, and whether it will be provided to third parties. If you do not see a privacy policy, consider surfing elsewhere. For more information, see *Site-seeing on the Internet: a traveler's guide to cyberspace* from the FTC at www.ftc.gov.

3 Books to read

There are a few excellent articles on identity fraud available for download from Amazon, however, they are extremely expensive:

Yankee Group. 2001. *Identity theft, fraud, and the future of biometrics for wireless* – this is a PDF report available for download at http://www.amazon.com/exec/obidos/tg/detail/-

/B00005V7WT/qid=1069129589/sr=1-5/ref=sr_1_5/103-8706480-6183844?v=glance&s=books. The price (US$995.00) is prohibitive for cash starved academics.

Jupitermedia Corporation. 2003. *Identity management reducing fraud costs and securely managing personal customer information*. Also available for download (at US$793.00) at http://www.amazon.com/exec/obidos/tg/detail/-/B000092PYR/qid=1069129589/sr=1-7/ref=sr_1_7/103-8706480-6183844?v=glance&s=books

C. Charrett's rather dubious book *Modern identity changer: how to create and use a new identity for privacy and personal freedo*', explains how to obtain a new identity, produce supporting documents for it and use it safely in today's society. It has a disclaimer stating it is for 'academic perusal only.'
Other interesting titles to read are:

Hammond, R. 2003. *Identity theft: how to protect your most valuable assets*. Career Press, Franklin Lakes (NJ). This guide shows you how to keep your identity protected, safe, and ready to be used by only one person – you! The author explains how identity theft occurs, who the likely victims are, and what you can do if your identity has been stolen.

May, J. 2001. *The guide to identity theft prevention*. 1st Books Library, Bloomington (IN). A basic, easy to understand book, it covers the spectrum of identity theft issues from a 'real people' perspective. Both personal and business protection is covered and it outlines what to do if you are a victim of this rapidly-growing crime. From victim survey data to template letters of dispute, this provides an important guide for any consumer.

Newman, J. 1999. *Identity theft the cybercrime of the millennium*. Loompanics Unlimited, Port Townsend, (WA) – discusses the state of events in the USA.

4 References

ABA. 2002. *Identity fraud: protect your financial identity*. [On-line]. Available WWW: http://www.bankers.asn.au/ABA/adminpages/AdminViewAnArticle.asp?ArticleID=313

ARMA International. 2003. *11 Ways to protect yourself from identity theft*. [Online]. Available WWW: http://www.arma.org/pip/eleven_steps.cfm

Bielski, L. 2001. Identity theft. *ABA Banking Journal* 93(1):27-30

FTC. 2003. *ID theft: what IS it all about?* [Online]. Available WWW: http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.pdf

SA Banking Council. 2003. *Banks unite to combat fraud* [Online]. Available WWW: http://www.banking.org.za/Public/moreres.cfm?id=227&section=1

Vecchiatto, P. 2003. *Combating identity theft*. [Online]. Available WWW: http://www.itweb.co.za/sections/internet/2003/0310171012.asp?A=BUS&O=F

About the author

Sam Berner (B.Ed., Dipl. LIS, Postgraduate Diploma in Information Management) is a principal of the company ECognus (Brisbane, Australia). She is a knowledge management consultant, assisting small to medium enterprizes to benefit the most from their intellectual assets. ECognus also provides services in the area of tailored software applications and the digitization of business processes.

Disclaimer

Articles published in SAJIM are the opinions of the authors and do not necessarily reflect the opinion of the Editor, Board, Publisher, Webmaster or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special, incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user's use of the Website.

ISSN 1560-683X

Published by InterWord Communications for Department of Information Studies, Rand Afrikaans University