BC Crime Prevention
Association

A recognized province-wide team of citizens, businesses and police dedicated to preventing crime through community partnerships.

131 – 8th Street
New Westminster,BC
Canada V3M 3P6
Tel: 604=529-1552
Fax: 604-529-1550
E-mail: info@bccpa.org
www.bccpa.org

Do You Know Where Your Identity Is?
Identity Theft Issues for Practitioners and Their Clients

By Jeff Burton

The phenomenon labelled "identity theft" was first used in the United States in the mid 1990s as a catchy and appealing umbrella term for the practice of stealing personal, biographical and financial information for fraudulent purposes. As such, it has been popularized in the media worldwide, yet the brush is so broad that it embraces any fraudulent conduct that involves stealing information to the financial detriment of the true owner. Examples of identity theft include: applying for a credit card in another's name; cloning a debit card to withdraw cash at an ATM; forging legal documents to show property ownership and applying for fraudulent mortgages; stealing then using another's Social Insurance Number (SIN) to gain tax advantages; using basic name, address, birthdate and SIN to obtain cellular phone service in the owner's name; assuming another's name to evade criminal warrants or even child support.

The reality is that in Canada there is no criminal offence of identity theft per se. You will not find it in the Criminal Code of Canada, and yet, the offence of impersonating another has been on the statute book for over 125 years! In the absence of a specific criminal offence known as identity theft, the prevalence of stealing personal data in Canada is hard to accurately measure. The various forms of identity theft described above fall under a range of fraud and consumer crimes. Compounding the problems of an accurate assessment is the fact that, due to the nature of the crime, victims underreport all types of fraud.

Nevertheless, identity theft statistics have been gathered by PhoneBusters, the Canadian Anti-fraud Call Centre, which is jointly operated by the RCMP, Industry Canada Competition Bureau and the Ontario Provincial Police. In this context and with Benjamin Disraeli's classic quotation "There are three kinds of lies: lies, damned lies and statistics" in mind, it is safe to conclude from Phonebusters' first two complete years of statistical analysis, namely 2002 and 2003, that identity theft has shown a marked increase. This increase relates to both the number of complaints and the dollar value of losses. The Canadian numbers pale in comparison with those recorded by the Federal Trade Commission for the United States but we should not seek comfort from this. There is no room for complacency!

Public practitioners, in the course of their work, will have come across many aspects of identity theft that have touched their clients, some experiencing considerable financial loss, not to speak of stress and time consumed straightening out the mess that usually ensues. This article is primarily

addressed to those clients, but public practitioners themselves will also find valuable tips to help them in their professional and personal lives.

Identity theft manifests itself in many forms, but there is a convenient way to describe its face in Canada. This can be done by examining three general groups that reflect the way we handle our personal information, the exposure risks and the degree of control (or lack of) we have over the misuse of this information. These groups are not finite as there is some overlap.

A. **Protecting Information at Home: Low Risk/Most Control**

This is where we have the most control over the custody and control of personal information. For home-based businesses, employees who take work home or the public at large there are many potential risks but in the home environment we are in the best position to manage what happens to our information. Some examples are:

1. Computers:

Risks:

- Sensitive data (financial, business records, genealogical databases and personal information) stored on a hard drive can be accessed by hackers if protective hardware and software are not used. Theft of the computer also results in the permanent loss of data.
- Internet and email transactions are highly vulnerable to abuse of personal information unless precautions are taken.

Recommendations:

- Store sensitive information on external media and in a location away from the computer workstation.
- Install a firewall (either hardware or software) and use updated anti-virus software and other software to detect and quarantine or remove Trojan horses, pop-up ads and other spyware.
- Use email addresses that do not include the user's actual name or indicate gender.
- Select passwords that are difficult to guess and change them often.
- Watch for Website security indicators that ensure transmitted information is encrypted and shielded from unauthorized access.
- Consider subscribing to a recovery service that uses chip transmitters to locate stolen laptop computers.

2. Paper records/documents:

Risks:

- Carelessly discarded papers containing personal information can be retrieved by fraudsters and used for fraudulent purposes.
- Disorganized filing systems may result in the inadvertent disposal of valuable documents.

Recommendations:

- Use a good quality crosscut shredder to properly dispose of unwanted papers so that they are rendered unreadable or arrange for an on-site or off-site shredding service for larger quantities.
- Store valuable personal documents (wills, insurance policies, mortgages, deeds, etc.) in a safety deposit box.

3. Telephone conversations:

Risks:

- Callers purporting to represent a bank or credit card company may use social engineering to trick subscribers into disclosing information usable in frauds.
- Seniors are especially vulnerable to disclosing banking information to fraudulent telemarketers.

Recommendations:

- Record the caller's information and phone number to call the bank or credit card company referenced. Their contact phone numbers are published in telephone directories.

B. **Interacting With Others: High Risk/Some Control**

In the normal course of our daily lives we have to interact with other agencies to which we send sensitive information. They, in turn, send us information of equal sensitivity. Although there are new ways of communicating, the use of surface mail remains the principal medium for communicating information. Identity thieves know this all too well and therefore look upon surface mail in transit to and from homes to businesses as a rich resource for harvesting information for fraudulent use. While there are some measures we can take to reduce the risks, we entrust such information to the carrier – the postal service – in the expectation that mail will not be intercepted prior to reaching its destination.

There are other activities that expose us to identity theft, especially in banking where we may unwittingly and sometimes unavoidably lower our guard to our detriment.

1. Surface mail:

Risks:

- Sensitive outgoing mail left overnight in street collection boxes could be removed by fraudsters, as could mail stored in common mailbox banks in apartment buildings.
- Unsecured external mail boxes with flags are a common target of thieves.

Recommendations:

- Try to reduce the volume of incoming and outgoing surface mail by considering alternatives. Elect to receive statements, such as Hydro, Terasen Gas and phone and credit card bills, on-line and request the utility or bank to stop sending hard copy statements.
- Where the sending of sensitive information by surface mail is unavoidable, select a street mailbox with an imminent collection time or take it to a sub-post office or shopping mall postal outlet where the risk of mail interception is reduced.

2. Banking activities:

Risks:

- Debit cards used at ATMs and gas stations and other Point of Sale locations can be compromised through "skimming" techniques.
- Internet "phishing" techniques might trick users into disclosing banking information to fraudsters who have imitated the Websites of banks, credit card companies, auction sites and other household corporate businesses.

Recommendations:

- Be vigilant whenever you use your debit or credit card. Watch for unauthorized changes to the appearance of ATM architecture, note suspicious behaviour of those around you and when surrendering payment cards, make note of any process that departs from normal procedure for processing payment.
- No matter how serious the tone and content of an email purporting to come from your bank, do not click on any links that request your banking information (account number, password or PIN). Notify your bank of the fraudulent email.

C. **External Custodians: High Risk/Least Control**

Consider the number and variety of agencies that maintain records about every Canadian, from governments to provincial bodies, public and private organizations and non-profit associations. In each case the quantity of information about us differs according to the agency's purpose for data collection. In most cases we are compelled to provide information in order to qualify for services, but once the information is submitted we never see it and entrust the custodians to protect it.

Risks:

- Computer databases, although password protected, can be accessed by unauthorized personnel who have been approached by organized crime and are rewarded for disclosing confidential information.
- Temporary employees or those with fabricated employment histories may seek to be placed in a sensitive position to access databases for the purpose of gleaning information for their own personal fraudulent aims or for passing on to others.

- Computer hard drives on which sensitive information is stored could be stolen or recycled as part of hardware infrastructure improvements but there may have been an omission to properly "clean" the hard drives prior to disposal.

Recommendations:

- Effective January 1, 2004, privacy legislation, whether federal or provincial, now applies to all agencies from governments down to not-for-profit organizations as well as for-profit entities. All custodians of personal information are mandated to protect data in their possession and control, and to put in place measures preventing unauthorized access and disclosure. This legislation provides for sanctions exercised by privacy commissioners for those agencies failing to comply. Each of us should question the reason for the collection of personal information and request an explanation of how the data will be used and protected.
- Organizations and agencies should practice the highest level of due diligence in the hiring of employees who have potential access to confidential information useful to identity thieves and limit database access to as few personnel as possible. Such restrictions must be in tandem with strict password protocols, log on procedures and regular and impromptu computer audits of employees accessing our information.
- Use professional utility software to completely sanitize hard drives prior to disposal.

It is well established that we cannot completely insulate ourselves from the threat of identity theft; however, we can certainly take steps to reduce and minimize that risk. Often identity thieves steal our information today but do not necessarily commit a fraud tomorrow. The information could be held for months or years before it resurfaces, making it very difficult, if not impossible, for victims to determine when and where their information was compromised. Where identity theft is concerned, the maxim "An ounce of prevention is worth a pound of cure." is very apt. If the recommendations in this article are followed, we could all save ourselves a lot of stress, time, money and the loss of our identity.

Jeff Burton has an extensive background in law enforcement, including 11 years as a member of the London, U.K. police force followed by more than 30 years' service with the Vancouver Police Department. Jeff completed his policing career with a seven-year stint as a detective with the Financial Crime Section. Since his retirement from policing, he has drawn on his investigative experience to develop identity theft material for use in presentations as well as television and radio appearances. Jeff contracts to the BC Crime Prevention Association as a resource person under the HeadsUp BC Fraud Program. Contact Jeff at ***jburton@dccnet.com*** *or (604) 831-1341.*

The BC Crime Prevention Association is located at 131 – 8th Street, New Westminster, BC and can be contacted at (604) 529-1552. The B.C. Crime Prevention Association Website is located at: ***http://www.bccpa.org/headsup/awareness.html****. Two of the articles available for downloading on this site are "Identity Theft and Fraud" and "Preventing Internet Identity Fraud."*