STRATEGIES

THIS IS ONE OF A SERIES OF ARTICLES PREPARED FOR CIBC PRIVATE WEALTH MANAGEMENT. THE SERIES IS WRITTEN BY PROFESSIONALS IN SUCH FIELDS AS TAXATION, TRUSTS, AND ESTATES.

Protecting yourself from identity theft

By Norman D. Inkster, BA, LLD, President, INKSTER Inc.

Ten years ago, identity theft was practically unheard of. Today, there are provisions in the Criminal Code of Canada that address numerous aspects of identity theft. During 2008, this crime cost Canadians more than $9.5 million, according to statistics kept by PhoneBusters, a national fraud-watch agency operated by the Ontario Provincial Police.

Identity theft is unusual in that victims don't even realize they've been targeted until well after the fact. A survey conducted by the Federal Trade Commission in the United States reported that 9% of identity theft victims didn't discover the theft for at least five years. An additional 23% were unaware of the theft for more than a year. By the time you become aware of the theft, your credit rating may be ruined and it can take years to remedy the situation.

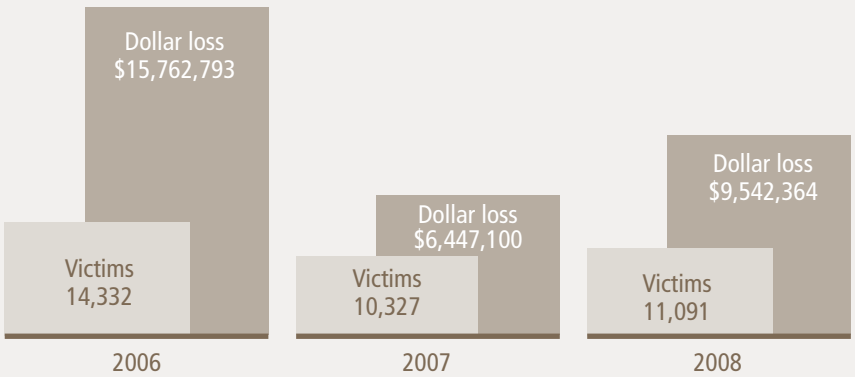
Fortunately, there are a number of steps you can take to protect your good name and credit rating from misuse by criminals. Safeguarding your personal information, making computer and Internet security a priority, and carefully reviewing all your bank and credit card statements are essential.

What the thief wants

An identity thief steals personal information about you so that he or she can impersonate you. Identity thieves are

The high cost of fraud

Despite heightened awareness, the number of victims and the dollar losses attributable to identity theft remain quite high.



Source: PhoneBusters, January 13, 2009 (www.phonebusters.com)

Norman D. Inkster is the President of INKSTER Inc., a specialized independent consulting firm. Mr. Inkster is a recognized international expert on law enforcement with over 35 years of experience with the Royal Canadian Mounted Police and is Past President of INTERPOL. He has managed large, complex investigations relating to fraud, money laundering and embezzlement including the recovery of stolen assets.

interested in your Social Insurance Number (SIN) and your driver's licence, as well as your bank account and credit card information. You may not even notice that anything has been taken, because unlike an ordinary thief, the identity thief wants the information on the documents rather than the documents themselves.

With this information in hand, the thief can use your credit card and bank account information to charge purchases to your credit cards and make withdrawals from your bank accounts, possibly emptying out all your savings. Some criminals go even further, using your identification not only to access your existing accounts, but also to open up new credit card accounts in your name. In one instance, the criminal used the information to place a mortgage on the victim's own house (see Case Study #1).

Although identity theft can affect anyone, more affluent individuals make more attractive targets. People with a high net worth typically have higher lines of credit and are more likely to own property mortgage-free, including real estate. They may also be less likely to notice fraudulent charges, particularly if their money is managed by others. And the more affluent someone is, the greater the potential loss he or she can suffer at the hands of an identity thief.

Case study #1 — Mortgage mavens

Bill and Mary Smith* had been happily mortgage-free for many years — or so they thought. When they decided to sell their home, they were shocked to discover that someone had mortgaged it without their knowledge.

The wily impostors had presented false identification, including Social Insurance Numbers, to the bank, and then forged Bill's and Mary's signatures on the mortgage documents. By the time Bill and Mary became aware of the situation, the thieves were long gone.

*Names are fictitious.

Criminal behaviour

Understanding how identity theft is committed is the first step in protecting yourself. Here are some of the practices favoured by scam artists.

Skimming. When you pay at a restaurant or store with your credit card or bank card, the card is quickly run through a machine called a "skimmer" before being processed legitimately. The skimmer records the personal information from the stripe on the back of the card. The skimmed information may be used to buy products or services on the Internet or over the telephone, or is encoded onto fake bank or credit cards to be used for illegal purchases (see Case Study #2).

Theft of payment cards or documents. Identity thieves steal newly issued credit cards or pre-approved credit card applications from your mailbox. "Dumpster divers" go through the garbage looking for bank or credit card statements. The thief contacts the issuing bank and requests a change of address, and then starts spending — at the victim's expense. The victim is often completely unaware of the charges accruing, since the bills are diverted to another address.

Shoulder surfing. This ploy is simple, but effective: The thief looks over your shoulder as you enter your Personal Identification Number (PIN) at an ATM or use your debit card to pay for a purchase, then uses your number to withdraw funds from your bank account using a stolen or counterfeit card.

Email and website spoofing (also called "phishing"). In this electronic scam, the target receives an email, seemingly from a legitimate business, which directs him or her to a website where personal information is requested. There is in fact no legitimate business and the real purpose of the website is to obtain the victim's SIN and personal financial data. A recent improvement on the theme of phishing is "spear phishing" where the same methods are used, but is much more targeted. For example, thieves may target a specific group of people within an organization, using "inside" language in the emails; alternatively, spear phishers will target a certain element of personal information, such as a bank account number or the three digit security code on the back of your credit card; they're looking for that one missing piece of data to complete their fraudulent scheme.

Social networking. Social networking sites like Facebook and MySpace create huge opportunities for identity thieves. Often, too much personal, identifying information is posted about users, including address, telephone number, email address, employment history, date of birth, and so on. And since these sites are so popular with young people, information is unwittingly revealed about users' parents as well. While these individuals believe they are corresponding with others their own age, these sites can be used by identity thieves (and sexual predators) to access profiling information with the intention to engage in fraudulent activities. Note also that because many young people carry credit cards, some with significant credit allowances, identity thieves can use the personal information they find on these sites, apply for new cards, and ultimately the parents pay. Furthermore, it is an accepted practice for those on social networks to adopt a nickname or pseudonym, guaranteeing anonymity that can protect the fraudster, often without any concern being raised.

Case study #2 — The southern skimmer

While vacationing in Florida, Frank Jones* used his credit card to pay his bill at a restaurant. The server took the card away from the table to obtain a credit card authorization. Unbeknownst to Frank, she also ran the card through a skimmer before returning it to him, and then went on a spending spree. Frank was unaware his card was being used fraudulently until he got back to Canada and received his credit card statement.

*Name is fictitious.

How to protect yourself

The average victim of identity theft spends more than 600 hours and $1,500 trying to undo the damage, according to PhoneBusters. As with many crimes, prevention is the best (and cheapest) protection.

Safeguard your personal information. Keep your personal information safe — particularly your SIN, but also your date of birth and credit card and bank account numbers. Your employer, the Canada Revenue Agency, and your financial institutions are legally entitled to know your SIN, but there are very few other situations where you are legally required to provide it. Don't give personal information to anyone unless you're absolutely sure you're dealing with a reputable company, and never give out personal information over a cordless phone, a cell phone or a laptop computer because of the risk of interception.

Protect your passwords. Use different passwords for your credit card, bank, and phone accounts. Choose passwords and PINs that can't be easily guessed (not your birthday, for example) and change them regularly, as often as once a month. Don't write them down or share them with anyone. When paying by debit card or making an ATM withdrawal, look around to make sure no one can see you enter your PIN.

Be credit card smart. Carry only the personal information and credit cards you actually need. Cancel credit cards you don't use and keep a separate list of the cards you use regularly.

Secure your mail. Always deposit your outgoing mail directly into a mail box, so it's not easily intercepted. Shred or destroy pre-approved credit card applications you don't want, as well as credit card receipts, utility bills, and any documents containing personal or account information. A personal shredder costs less than $50, and protects you against dumpster divers. Be sure to use a "cross-cut" shredder which reduces correspondence to confetti-like pieces — there is software available that can take the long strips of paper produced by old style shredders and reconstruct the original document.

Ensure computer and Internet security. You might want to equip your computer with a "firewall," which prevents outsiders from accessing the data on your computer. Deal only with reputable, established companies when using the Internet for credit card purchases or banking transactions, and be sure their sites are secure. Look for digital signatures, data encryption, and other technology that enhances user security.

Review your records regularly. Check your bank and credit card statements as soon as they arrive to discover and report any

discrepancies immediately. Pay attention to your billing cycles — if your bills don't arrive on time, it may mean your mail is being diverted to another address.

Check your credit rating. You may want to obtain a copy of your credit report and make sure it is accurate. Canada has two national credit bureaus: Equifax Canada (1-800-465-7166, www.equifax.ca) and TransUnion Canada (1-877-525-3823, www.tuc.ca).

What if it happens to you?

If you think that you've been a victim of identity theft, notify the police, your bank, and your creditors immediately. Obtain a copy of the police report, which your creditors may require as evidence that fraud has been committed. Then, take the following steps to clear your good name:

- Keep a record of every person you speak to and all the expenses you incur to clear your name and re-establish your credit.
- Cancel your credit cards and close your bank accounts and replace them with new ones. Use new passwords and PINs for each of these accounts.
- Get a new driver's licence.
- Call Equifax and TransUnion and request that a fraud alert be placed on your file, which lets credit grantors know you're a potential fraud victim. Both credit bureaus have fraud victim assistance specialists who will review your credit report with you on the telephone so that you have a complete list of your creditors.
- Do a follow-up check with the credit bureaus after three months and request an updated copy of your credit report to make sure that your identity has not been used again.
- Contact Canada Post if you think the identity thief has filed a change of address form for your name and is diverting your mail to another address.
- Advise your telephone, cable, and utility companies that someone has been using your name fraudulently and may try to open new accounts.
- If you think someone has used your Social Insurance Number to get a job, contact Human Resources and Social Development Canada.

Fraud: A truly international crime

Frauds, scams, and identity theft are international in scope. In one incident, Spanish police uncovered a fraud ring that had cheated some 500 Canadians and Americans out of millions of dollars.

In most cases, victims received a letter saying that they had won a portion of "El Gordo," Spain's well-known Christmas sweepstakes. In order to collect their winnings, recipients were asked to forward money to cover the taxes and handling fees — in some cases, as much as $26,000.

Needless to say, the "lottery winnings" never materialized. Bottom line: Never send cash or give out your personal information in order to receive a supposed prize.

This article is intended to provide general information only and should not be construed as specific advice. Since a consideration of individual circumstances is critical, anyone wishing to act on information in this article should consult his or her professional advisors. This article reviews Canadian federal tax and other laws only, unless otherwise stated. Provincial tax and other laws may also apply and may differ.

CIBC

For what matters.

The Masters Series of articles is provided as an information service only, and the information is subject to change without notice. The information is believed to be accurate at the time of writing but CIBC does not represent or guarantee accuracy, completeness or suitability. The opinions expressed therein do not necessarily represent the views of CIBC. Please consult your own professional advisors for further advice concerning your particular situation.
CIBC Private Wealth Management consists of services provided by CIBC and its subsidiaries.
"CIBC For what matters." is a trade-mark of CIBC.

FSC Mixed Sources
Product group from well-managed forests, controlled sources and recycled wood or fiber
www.fsc.org Cert no. SW-COC-002047
© 1996 Forest Stewardship Council

172A498E 12/09