

Privacy and Information Protection Bulletin

March 2005

Fasken Martineau DuMoulin LLP

Identity Theft

Sara Levine and Joanna Erdman (student-at-Law), Toronto

February 2005 is designated *Fraud Awareness Month* by the Fraud Prevention Forum, chaired by the Competition Bureau in partnership with the Office of the Privacy Commissioner of Canada, law enforcement organizations, Canadian businesses and consumer advocacy organizations.

Throughout the month of February, many businesses are including messages about fraud prevention in their monthly bill statements, as well as, educating their employees and informing consumers about the dangers of fraud.

Identity theft is one of the fastest growing types of fraud in Canada. To facilitate fraud prevention and awareness among our clients and friends, we have updated and expanded our Identity Theft Bulletin, first issued in September 2003.

We hope that the information and resources provided in this bulletin will help you to protect yourself and your families.¹

¹ All contact information (phone numbers, web site addresses) is current as at date of this bulletin but could be subject to change.

What is identity theft?

Identity theft:

- is the theft and fraudulent use of another person's identity or personal information;
- is the fastest growing fraud crime in Canada; and
- is estimated by the Canadian Council of Better Business Bureaus to cost Canadian consumers \$2.5 billion a year. The two major Canadian credit bureaus, Equifax and Trans Union, reportedly receive 1400 to 1800 identity theft complaints per month. Statistics gathered by PhoneBusters indicate that the largest number of identity theft complaints relate to the false use and application for credit cards and cellular phones. According to Canada's Social Insurance Registry, there are 1.4 million more Social Insurance cards in circulation than people.

Today, with easily available software, "identity thieves" can:

- use just one piece of stolen information to create full identification sets;

Vancouver

Calgary

Toronto

Montréal

Québec City

New York

London

Johannesburg

- forge SIN cards, driver's licences and passports;
- use an individual's personal information to redirect mail, establish cellular phone service, get jobs, open fraudulent credit card and bank accounts, and incur large debt and other liabilities, all in the victim's name; and
- do all of this before an individual even discovers that a piece of their personal information has been stolen.

Stolen identities can even be used to facilitate organized crime, money laundering and terrorism.

What information is useful to a thief?

A thief can use any *one* of the following pieces of personal information to commit fraud:

- date of birth
- mother's maiden name
- ATM receipts
- financial records and tax returns
- identification: passport, driver's licence, SIN card, health card
- pre-approved credit applications
- utility and phone bills
- home and work addresses
- credit card and bank account numbers
- phone numbers

How do identity thieves get your personal information?

- They steal your wallet or purse.
- They retrieve pre-approved credit card offers from your trash or a mailbox and return them to the bank, requesting that the card be sent to an alternative address where they are waiting to receive it.
- They change your mailing address, so they can receive your mail.
- They read your personal identification number ("PIN") over your shoulder at an ATM or debit card machine, then distract you, steal your card and use it to access your accounts.
- They swipe your card through an inexpensive electronic device (known as a "skimmer") when they are serving you in a legitimate transaction, such as at a restaurant or retail store. The information from the magnetic strip is stored in the "skimmer" and later used to create a duplicate credit card or other identification.
- They send you unsolicited e-mail messages ("spam") that appear to come from legitimate businesses with whom you regularly do business. These authentic-looking messages falsely indicate there is a problem with your account, and ask you to provide account numbers and passwords to fix the error.
- They call to congratulate you on being a contest winner or to conduct a survey, and then ask you apparently innocent questions. When you answer, you give them your personal information.

A January 2005 survey, commissioned by EDS Canada Inc. and conducted by Ipsos-Reid, revealed that Canadians willingly provide significant amounts

of personal information to organizations over the phone and the Internet, even when the contact is unsolicited. For example, 61% of those surveyed were willing to provide their postal code to an organization that contacted them by phone. 54% of respondents were willing to provide their address over the Internet. On a positive note, most individuals do recognize the importance of protecting their SIN, credit card and debit card numbers. Only 4% of respondents indicated that they would provide their SIN to an organization that contacted them by phone.

What are the ten habits of highly protective people?

1. Sign credit cards immediately upon receipt.
2. Carry only a minimal amount of ID, credit cards and the like and keep all non-essential identification in a safe place.
3. Choose passwords that are difficult for others to guess – *not* your mother's maiden name. Change your passwords frequently and memorize them – don't write them down.
4. Carefully review each monthly credit card statement and pay attention to billing cycles. If your statement shows unexpected charges, immediately contact the credit card company. If a statement does not arrive when expected, contact the sender and the post office to ensure your mail has not been fraudulently re-directed.
5. Ensure that paper documents containing personal information are shredded or destroyed before you throw them away. This includes receipts from electronic and credit card purchases, ATM receipts, utility bills, preapproved credit card applications and other paper documents and forms containing personal information. Insist that businesses that you deal with do the same.
6. Never provide:
 - your personal information unless it is legally required;
 - your address or phone number when using a credit card; or
 - your personal information over the phone, through the mail or over the Internet unless it was you who contacted the organization requesting the information.
7. When online:
 - check the organization's web site for fraud alert notices as to improper uses of its name, or call its customer service number listed on an account statement or in the phone book; and
 - keep in mind that unless the web site is reputable and has secure encryption, the security of business transactions may be at risk.
 - to protect yourself from spam, shield your computer with anti-spam programs and use separate e-mail addresses for different online activities. For other tips from Canada's Task Force on Spam, visit: www.stopspamhere.ca.
8. Order your credit reports from major credit bureaus (see below) at least once every year to ensure they are accurate. Report any error to the credit bureau to ensure immediate detection and correction.
9. Take a photocopy of the contents of your wallet and keep it in a very safe place, such as your safety deposit box, a locked safe or a secret place in your home.

10. Keep a written record of all important numbers for reference in case you are a victim of identity theft. Again, keep that record in a very safe place. *Do not keep such information in your wallet or on your computer, where it can be vulnerable to thieves or hackers.*

In addition, you may wish to use the information protection services offered, for a fee, by some private companies and major banks. These services keep a record of the information on your credit and debit cards, driver's licences, health cards, passports, cellular phones and other important cards and documents. If these items are lost or stolen, you only need to make one telephone call to the service, and it will notify every company that you have cards with, any entities you pay by way of pre-authorized credit card payments, and your cellphone service provider. They may also request replacement cards and phones. Some of these companies offer additional travel assistance, such as emergency airline tickets and emergency funds. Call your bank for further information.

What if your personal information is lost or stolen?

1. Call the police immediately.
2. Call your bank and credit card companies.
 - Toll-free phone numbers can be found in the phone book, on your issuing bank's web site or on your credit card monthly statement.
 - Cancel or replace all existing credit and debit cards, close all bank accounts and open new ones that have password-only access. Ensure that no other accounts have been opened in your name. Confirm all recent activity on the accounts.
3. Call all credit bureaus.
 - Advise the phone, cable and utility companies that someone using your name could open new accounts fraudulently.
 - Cancel or replace all of your passwords and PINs.
 - Credit bureaus are private companies that provide credit grantors (such as banks or car leasing companies) with information about an individual's credit records. These companies use the information to verify and assess creditworthiness.
 - Generally speaking, a financial institution will not extend credit or debt to a new customer without first checking with a credit bureau.
 - If advised of a loss or theft, the credit bureau should attach a "lost or stolen identification flag" or a "potential fraud alert" to your credit file, making it more difficult for a thief to use stolen personal information.
 - Do a follow-up check with the credit bureaus three months later to ensure that the appropriate "flag" or "alert" is on your record.

The three Canadian credit bureaus are:

Equifax Canada

Phone: 514 493 2314 or 1 800 465 7166

Fax: 514 355 8502

E-mail: consumer.relations@equifax.com

Web: www.equifax.ca

TransUnion of Canada

For residents of all provinces except Quebec: 905 525 0262 or 1 866 525 0262

For residents of Quebec: 514 335 0374 or 1 877 713 3393

Fax: 905 527 0401

Web: www.tuc.ca

Northern Credit Bureaus

Phone: 1 800 532 8784

Fax: 1 800 646 5876

E-mail: bcn@bcn.qc.ca

Web: www.creditbureau.ca

4. Report the loss or theft of government-issued documents to the issuing authority.

Documents issued by the federal government include your:

- *Passport* - contact the Passport Office at 416 973 3251 or 1 800 567 6868. If you are outside of Canada, contact the nearest Canadian government office.
- *Social Insurance Card* - contact Human Resources and Skills Development Canada (HRSDC) at 1 800 206 7218 or go to: www.sdc.gc.ca/en/cs/sin/130.shtml.

Documents issued by provincial and territorial governments include your:

- *Birth certificate* – if you hold an Ontario birth certificate, contact the Office of the Register General at 416 325 8305 or 1 800 461 2156, or go to www.cbs.gov.on.ca for information about the local Registry Offices. If you were born in another province or country, you will need to contact that province or country.

- *Driver's licence* – to replace an Ontario driver's licence, you must visit a Driver & Vehicle Licence Issuing Office. Two pieces of photo identification required. For more information go to: www.mto.gov.on.ca/english/dandv/driver/replace.htm.
- *Health card* – during business hours call the Ministry INFOLine at 1 800 268 1154. In Toronto, call 416 314 5518. After business hours call 1 800 664 8988.

5. Contact Canada Post.

- To ensure that your mailing address has not been changed, or to correct any fraudulent changes, contact Canada Post at 1 800 267 1177 or by e-mail at service@canadapost.ca.

What if your personal information is fraudulently used?

1. Contact all the resources listed above, AND
2. Contact *PhoneBusters*.

- PhoneBusters, established by the Ontario Provincial Police, is a central agency that collects information on identity theft incidents and will contact the appropriate credit card companies and your local police.

PhoneBusters National Call Centre

Phone: 1 888 495 8501

Web: www.phonebusters.com

E-mail: info@phonebusters.com

- Keep a copy of the police report. A creditor or credit bureau that mistakenly believes the victim is the person

responsible for a fraudulent transaction may insist upon proof of a police report.

3. Alert the credit bureaus to the fraudulent use.
 - Once alerted, the credit bureaus should attach a “fraud alert” to your credit file.
 - Corrections on your credit report should be forwarded to any credit grantor who has received your credit report within the past two years. Credit history and banking information remains on a credit file for six or seven years from the date of delinquency or the date of last activity.

Important: When reporting a theft or fraud keep a record of the steps you’ve taken, the contact name and a copy of all documents. These are necessary if you become involved in any criminal or civil proceeding resulting from the theft and fraud. They will also assist in showing that you should not be liable for debts or liabilities incurred in your name by the thief.

For more information please contact:

Sara Levine
416 865 5162
slevine@tor.fasken.com

This publication is intended to provide information to clients on recent developments in provincial, national and international law. Articles in this bulletin are not legal opinions and readers should not act on the basis of these articles without first consulting a lawyer who will provide analysis and advice on a specific matter. Fasken Martineau DuMoulin LLP is a limited liability partnership under the laws of Ontario and includes law corporations.

© 2005 Fasken Martineau DuMoulin LLP

Vancouver

604 631 3131
info@van.fasken.com

Québec City

418 640 2000
info@qc.fasken.com

Calgary

403 261 5350
info@cg.fasken.com

New York

212 935 32 03
info@nyc.fasken.com

Toronto

416 366 8381
info@tor.fasken.com

London

44 20 7929 2894
info@lon.fasken.com

Montréal

514 397 7400
info@mtl.fasken.com

Johannesburg

27 11 685 0800
info@jnb.fasken.com