IDENTITY THEFT and YOU

Office of the
Privacy Commissioner
of Canada

IDENTITY THEFT

The Criminal Code was amended in 2010 to make identity fraud and identity theft criminal offences.

With today's proliferation of technology, stealing innocent people's identities in order to commit fraud has become a very lucrative business.

Cloaked in your stolen identity, a fraudster can cash your cheques, raid your bank accounts, bilk your credit card company and even load a big mortgage on your house.

The term identity theft can be used for everything from cheque forgery and the use of stolen credit cards to sophisticated scams in which an impostor adopts other people's identity to gain access to their assets.

Identity thieves have many ways to get their hands on your personal information. Some simply steal old bills or preprinted credit card offers discarded in waste or recycling bins. Others exploit information lost or stolen from databases operated by retailers or other private-sector organizations and even government bodies.

You can, however, help protect yourself from unscrupulous criminals. One important way is to limit the amount of information you give out about yourself. This brochure describes some of the key steps you can take to safeguard your identity and better protect yourself from swindlers.

Incorporating these tips into your life doesn't take long, but will lessen the chances that your personal information winds up in the wrong hands.

Tips for reducing the risk of identity theft

- Be careful about sharing personal information or letting it circulate freely. When you are asked to provide personal information, ask how it will be used, why it is needed, who will be sharing it and how it will be safeguarded. Do not give out more than necessary.
- Be particularly careful about your SIN; it is an important key to your identity, especially in credit reports and computer databases. Don't share it unless absolutely necessary.
- Talk with your children about identity theft and how to minimize the risk.

CREDIT CARDS

- Keep track of when credit card bills are supposed to arrive, and call the company if they're late.
- Review credit card and bank statements to make sure there are no unauthorized purchases. If there are, contact the card issuer immediately.
- If you do online banking, consult your statement frequently to check for any anomalies.
- Check your credit report annually. Major credit reporting bureaus provide one free report each year.

MAIL

- Use a locked mailbox or one with a drop slot to prevent mail theft. If you use a regular box, pick up your mail as promptly as possible after it is delivered.
- Ensure your mail is forwarded if you move.
- Shred or destroy items with your name and address, such as preapproved credit card offers, insurance and loan applications, bills, and receipts. Don't discard them in recycling or waste bins.
- If you are going to be away from home, arrange for a trusted neighbor to pick up your mail. Canada Post also provides a mail-holding service for a fee.

PHONE

- Don't give out credit card numbers or other personal information over the phone unless it's to a trusted person or you initiated the call yourself.
- If someone calls unexpectedly and requests your personal or financial information, try calling the organization they are representing to verify that the request is legitimate. Reputable firms never ask for personal information without significant safeguards.

WALLET

- Carry only essential ID such as your driver's license and health card. Leave your Social Insurance Number card, passport and birth certificate in a safe place.
- Do not let private organizations make copies of your ID documents unless there is a legitimate need and you know that they will be protected adequately. The information on the copy is as valuable as on the original document.

ONLINE

- Make sure your computer and mobile device are protected with passwords. Mobile phones and tablets are small and easily lost or stolen. They are full of personal information that could be compromised if they fall into the wrong hands.
- Make sure your computer is equipped with online security and privacy safeguards including, but not limited to, firewalls and virus protection.
- Create unique, hard-to-guess passwords for each of your online accounts and change them often, particularly if you suspect they may have been compromised.
- Keep all software, especially security and privacy safeguards, up-to-date.
- Whenever possible, do not engage in sensitive activities—like online banking or online purchases—on your mobile device when you are in public. You never know who may be watching or filming you in order to capture your personal information.
- If you feel you need to log on to your e-mail or bank account from a library or other public computer, make sure no one can watch over your shoulder as you type in your password and other private information. Log out when you leave.

- When you shop or bank online, or fill out online forms, look for the padlock symbol at the lower right corner of your screen (also look for "https" in the site URL). This symbol means the link between your computer and the site is encrypted, helping to protect the information while it is in transit. And be sure to log off when your transaction is complete.
- Be careful about where and to whom you divulge or post any personal information online.
- Don't reply to suspicious e-mails, IM or text messages asking you to provide personal information online, even if they appear to come from financial institutions or government agencies. Call the bank or agency if you have doubts.
- Disable Wi-Fi and Bluetooth when you are not using it – when you leave your device open by default, you leave your data vulnerable to access by others without your knowledge or consent whenever you pass through cafés and other places offering open, public wireless networks.
- Delete all personal information from your electronic media devices before discarding, recycling or selling them. There are several ways to do this, for example by overwriting or destroying the media.

If you become a victim

If you think you have been targeted, there are some actions you should take to address the situation. Depending on the circumstances, you might need to:

- Report the incident to local police if the matter involved a theft/crime.
- Report the incident to the Canadian Anti-Fraud Centre (1-888-495-8501) if the matter involved a scam or fraud.
- Seek a copy of your credit report and review it.
- Advise your bank and credit card companies. Close any accounts and cancel any cards that may have been compromised.
- Report any missing identity documents or cards, such as a driver's licence, a health card or immigration documents to the appropriate organization.

The Office of the Privacy Commissioner of Canada

The Office of the Privacy Commissioner is working with you to safeguard your personal information and your privacy, which can help you protect yourself from fraudsters.

Organizations also play an important role. In the course of doing business they acquire personal information about employees, clients and customers, and they must ensure it is well managed and protected.

Canada's federal privacy laws - the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to private sector organizations, and the *Privacy Act*, which covers federal government departments and agencies – both require that personal information be safeguarded.

If you feel an organization or institution has not appropriately protected your personal information, you should raise your concerns directly with them. If the response is not satisfactory, you may wish to contact our Office.

We are empowered to investigate complaints and recommend that organizations and institutions adopt better personal information handling practices. Our Office has also developed a number of tools to help individuals to become more informed about how to protect their personal information. Our website (www.priv.gc.ca) offers other useful information about identity theft and related frauds. ***For more information, please contact:***

Office of the Privacy Commissioner
of Canada
30 Victoria Street, 1st floor
Gatineau, QC
K1A 1H3

Tel.: (819) 994-5444
Toll-free: 1-800-282-1376
Fax: (819) 994-5424

Cat. No. IP54-26/2014
ISBN 978-1-100-54693-3

www.priv.gc.ca
Follow us on Twitter: @privacyprivee