

EMPOWERMENT FOR THE FUTURE

Identity Theft

Industry Canada

www.cmcweb.ca/idtheft

427

427113

Resources

Identity Theft Statement:

The Identity Theft Statement (ITS) is a form created by the Government of Canada, to create written documentation of an identity theft incident. The ITS can be used to help you notify financial institutions, credit card issuers and other companies that you have been a victim of identity theft, and give them the information they need to begin an investigation of the incident. Not all companies accept the statement; some still require that their own forms be used. Contact the company before sending the statement to find out what is required. Available in PDF form at www.cmcweb.ca.

Check your credit report:

Once a year, or if you think your personal information has been stolen, get a copy of your credit report from each of the major credit reporting agencies (credit bureaus). The report tells you what information the bureau has about your credit history, financial information, judgments, and any collection activity. It also shows who has asked for your information. You can receive a copy of your credit report from one of the following companies in the mail for free or online for a fee:

Equifax Canada Inc.: www.equifax.ca
(1-866-779-6440)

Trans Union Canada: www.tuc.ca
(1-866-525-02692 Quebec
1-877-713-3393)

By checking often, you can spot debts that are not yours and see who has been asking about you. You need to follow up if a lender or credit card issuer has asked for a report and you don't have an account with them and haven't applied for credit or a card from them. Someone else may have been using your name.

Key Government Contacts

If your government-issued documents are lost or stolen, it is important to report them right away, so that they can be cancelled and you can apply to have new documents issued.

As mentioned above, to replace any key government documents, contact the Government of Canada at 1 800 O-Canada (1-800-622-6232 TTY 1-800-465-7735). They will direct you to the appropriate organization. You can also contact them directly at the following coordinates:

Newfoundland and Labrador

Tel.: (709) 729-2600
Web Site: www.gov.nl.ca

Prince Edward Island

Telephone: (902) 368-4000
Web site: www.gov.pe.ca

Nova Scotia

Toll Free: 1-800-670-4357
Web site: www.gov.ns.ca

New Brunswick

Toll Free: 1-888-762-8600
Web site: www.snb.ca

Source: Industry Canada. Reproduced with the permission of the Minister of Public Works and Government Services Canada 2008.

What is identity theft?

Identity theft occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud, theft or forgery.

What is personal information?

Any factual or subjective information recorded or not, about an identifiable individual is personal information. This includes such things as your name, address, age, gender, identification numbers, credit card numbers, income, employment, assets, liabilities, payment records, personal references and health records. It can also include information about your purchasing preferences, family (such as mother's maiden name), interests, or attitudes.

How can I tell the information was stolen?

- A bank or credit card company contacts you about suspicious transactions
- Bills and bank or credit card statements arrive late or not at all (someone may have had your mail forwarded to another address)
- A creditor or collection agency contacts you about unknown debts
- Purchases and/or withdrawals not made by you appear on your monthly bills or bank statements
- You are denied credit for reasons that do not match your understanding of your financial position
- Your credit report shows credit issued that you didn't request
- Your property has a lien on it that you didn't know about
- Bills arrive for accounts that you do not own

How would this affect my life?

Identity thieves steal key pieces of personal information and use it to impersonate you and commit crimes in your name. If you are a victim, you could end up spending many hours trying to clear your name and may suffer emotional anguish throughout the process. In extreme cases, you could also suffer a loss of reputation, as court judgments for bad debts could be registered against you and your credit rating could tumble. This, in turn, could make it difficult for you to find employment or get access to credit when you need it.

How do they steal it?

Stealing mail from your mailbox or recycling bin, or fraudulently redirecting your mail by forging your signature on a "change of address" form.

- Stealing personal and private information from lost or stolen wallets or purses, from your home, your vehicle, or your computer.
- Stealing personal information from lost or stolen personal electronic devices such as, personal digital assistants (PDAs), digital audio players, cell phones and laptops.
- Posing as a trusted official of a company or of law enforcement, in person or online, and requesting your personal information such as your credit reports or bank account password.
- Tampering with automated banking machines (ABMs) and point of sale terminals, so that your debit or credit card number and personal identification number (PIN) can be recorded.
- Taking information from within organizations, such as employees who accept bribes or who steal your personal information on behalf of others. Organizations may also unwittingly release your personal information to criminals who pose as legitimate businesses.
- Searching public sources, such as newspapers (obituaries), phone books, and records open to the public (professional certifications).
- Using "spoof" emails and fraudulent websites ("brand spoofing") to fool customers into divulging their personal and financial information in a practice known as "phishing".
- Using "spyware" to steal information from your computer.

What can I do if this happens? Report it!

If you are the victim of identity theft, there are steps you can take to minimize damage and help prevent any further fraud or theft. As soon as you discover the fraud or theft, take the following steps to report it.

- Call your financial institutions – have them cancel your cards and re-issue new ones. If you do not report a lost or stolen card immediately you could be liable for any losses.
- Contact your local police. If a report is filed, be sure to include the police report number they give you in all correspondence you have relating to the theft.
- Contact Canada's main credit reporting agencies: Trans Union Canada at www.tuc.ca (1-866-525-0262 Québec 1-877-713-3393) Equifax Canada at www.equifax.ca (1-866-779-6440) Ask each agency to send you a copy of your credit report, and discuss with them whether you should have a fraud alert placed on your file.
- Replace your ID cards like health, driver's license, or SIN by calling 1 800 O-Canada. An agent will be able to direct you to the appropriate federal and provincial organization to replace each of your cards.

- If your mail is missing, contact Canada Post at www.canadapost.ca (1-800-267-1177).
- Contact each organization that provided the identity thief with unauthorized credit, money, information, goods or services in your name, and ask them to investigate the occurrence as well as cancel and close all fraudulent or affected cards or accounts. Find out the following: What information does the company need to begin an investigation? Has the company begun a criminal investigation? If so, what is the police report number? What do you need to do to have your losses reimbursed?
- For advice on privacy issues related to the identity theft (PIPEDA) contact the Privacy Commissioner of Canada (1-800-282-1376 or www.privcom.gc.ca).
- To help stop fraud, be sure to report the incident to Phonebusters, Canada's national anti-fraud call centre. Phonebusters gathers information and intelligence about identity theft and provides advice and assistance to victims. www.phonbusters.com (1-888-495-8501)

How can I prevent this from happening?

Prevention of identity theft is a shared responsibility between a consumer and the entities that have possession of their personal and financial information. Both consumers and business must take steps to safeguard the security of their data. While you may not be able to prevent identity theft entirely, the following are important steps that you can take to reduce your risk.

Guard your Personal Information & Documents

- Carry only the ID that you need. Keep all other identification (i.e. SIN, birth certificate, passport) locked in a safe place.
- Be careful about sharing personal information and don't give out more than you need to. If someone asks you for information that is not relevant to the transaction you are making, ask them why.
- When disclosing personal and financial information talk in a discreet manner and always shield your PIN when using your debit card. Please note that consumers have certain rights and responsibilities under the Canadian Code of Practice for Consumer Debit Card Services. For more information contact the Financial Consumer Agency of Canada (www.fcac-acfc.gc.ca).
- Ask about the security of your information at work and with businesses and charities.
- Don't leave personal information lying around at home, in your vehicle or at the office. Don't put more than your name and address on your personal cheques.
- Lock your household mailbox, if possible. If you are going to be away, arrange for a trusted neighbour to pick up your mail. You can also go to your local post office (with identification) and ask for Canada Post's hold mail service. There will be a charge for this service.
- Never give personal information by phone, Internet or mail unless you initiate the contact and you know the company very well. Identity thieves may use phony offers or pose as representatives of financial institutions, Internet service providers or even government agencies to trick you into revealing identifying information.



- Shred or destroy sensitive personal documents before tossing them into the garbage or recycling. This will help defeat dumpster divers looking for transaction records, copies of credit applications, insurance forms, cheques, financial statements and old income tax returns. Cut up expired and unused credit and debit cards. The card may have expired but the number may still be valid and could be used to make purchases.

