Identity Theft

CONSUMER IDENTITY THEFT KIT

IDENTITY THEFT:

Recognize it.
Report it.
Stop it.

For more advice and tools on identity theft, visit
www.cmcweb.ca/idtheft

PHONEBUSTERS
The Canadian Anti-fraud Call Centre

Canada Ontario Québec Nova Scotia New Nouveau Brunswick

Manitoba British Columbia Prince Edward Island Government of Saskatchewan Alberta Government

Newfoundland Labrador Yukon Government Northwest Territories Nunavut

Identity Theft: Are You a Victim?

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.

In general, data collected about you by businesses or your employer must be used only for the purpose for which it was collected, or for an additional purpose to which you have consented. Privacy legislation requires that government and businesses put systems in place to ensure that your client information is secure, accurate, gathered with your consent and not used beyond a stated purpose.

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and equivalent provincial legislation in British Columbia, Alberta and Quebec, apply to businesses collecting your personal information and give you the right to see and ask for corrections to any information a business may have collected about you. For more information about your rights under PIPEDA, download "Your Privacy Rights: A Guide for Individuals" from the Office of the Privacy Commissioner of Canada at www.privcom.gc.ca. You will also find information about the various provincial laws as well.

Why should you be concerned about identity theft?

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 judgements 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.

Signs your identity might have been 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

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

- Your property has a lien on it that you didn't know about
- Bills arrive for accounts that you do not own

How identity thieves get your personal information

- 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, cellphones 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.

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

Watch Your Identity: Tips for Reducing the Risk of Identity Theft

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 and 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.

Be Vigilant

Pay attention to financial details

Paying attention to financial details can help you watch for signs that you may be a victim of identity theft.

- When using your bank/debit card to withdraw cash or make a purchase, always shield the entry of your PIN. Never give your PIN to anyone, including anyone claiming to be a police officer or bank employee. Choose a PIN that can't be easily

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

guessed, as you could be liable if you use a PIN combination selected from your name, telephone number, date of birth, address or Social Insurance Number (SIN). Remember that no one from a financial institution or the police will ask you for your PIN.

- Keep credit card, debit card and automatic banking machine (ABM) transaction records so you can match them to your statements. If you choose to dispose of your records or statements, shred or destroy them, do not dispose of them in a public place.
- Report any discrepancies on your statements to your financial institution right away, whether it is transactions that appear which you have not made, or transactions that you know you have made, but do not appear.
- Know when your credit card, financial statements and utility bills are due. If they don't arrive when they are supposed to, call the financial institution or utility company – an identity thief may have changed the billing address. If you are missing mail from more than one business, contact the post office to inform them that you are concerned someone is redirecting your mail.
- Pay attention to credit card expiry dates. If your replacement hasn't arrived call the company. Someone may have taken it from your mail or changed the mailing address.
- Keep a list of the names, account numbers and the expiration dates of your cards in a secure place. This will help you when alerting your credit grantors about a lost or stolen card.

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)
Northern Credit Bureau: www.creditbureau.ca (1-800-532-8784)

By checking, 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.

For more information on understanding what a credit report is, take a look at, Understanding your Credit Report and Credit Score, available from the Financial Consumer Agency of Canada (www.fcac-acfc.gc.ca).

Guard your Computer and its Information

Online chats, shopping and banking add a lot of convenience to our lives but, if you don't have appropriate security for your computer, your personal and financial information could be at risk.

A common way for hackers to steal personal information is by using "spyware" which is software that gathers user information through the user's Internet connection without his or her knowledge. Spyware applications are typically bundled as a hidden component of freeware or shareware programs (such as music and video downloading software or online games) that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

The following measures can help protect you against identity theft while online:

- Always create passwords that include a combination of letters (upper and lower case), numbers and symbols. Do not use automatic login features that save your user name and password.
- Install fire-wall, anti-virus, anti-spyware and security software, and keep it up to date.
- Do not send personal or confidential information over email. Email messages are NOT secure.
- Don't try, don't buy and don't reply to spam (unsolicited emails) or phishing emails that ask for personal or financial information. Spam and phishing emails are often a source of scams, viruses and offensive content. *Delete!*
- Install security patches on your operating system and update regularly and frequently. Most software manufacturers regularly release updates and patches to their software to fix bugs that could allow attackers to harm your computer. However, it is up to you to find out.
- Check for suspicious activity online. Almost all firewalls and encryption programs include audit functions that record activities on the network. Check audit trails for unusual or suspicious activity, e.g., computer files in use when you are not aware.
- When disposing of, selling or giving away computer equipment, make sure that you permanently destroy the personal information on the hard drive. If you are disposing of the equipment you can physically destroy it, otherwise use overwrite software. If you don't know how, find out.
- If you use a laptop, physically lock it to prevent thieves from walking away with it and any personal information it contains.

Only shop and bank online with trusted merchants

- Make sure that the website is legitimate. Fraudsters can create a fake website ("brand spoofing") to trick consumers into revealing personal and financial information. Check that the URL is correct – including the domain (.com, .ca, etc.)
- Before submitting any personal information to a website, review its privacy policy for an understanding of how your information may be used.
- Before giving your credit card number or other financial information to a business, make sure the merchant has a secure transaction system. Most Internet browsers indicate when you are using a secure Internet link. To check to see if a website is secure look for a web site address that starts with http**s**://, a closed lock or an unbroken key icon at the bottom right corner of the screen.
- After completing a financial or online banking transaction, make sure you sign out of the website and clear your Internet file/caches and "cookies". Most financial institutions provide instructions on how to do so under their "security" section.
- If you receive an unsolicited email that asks for personal or financial information, do not reply. They are "phishing" for your information. Some fraudsters send email messages posing as a business or a bank that you normally deal with, sometimes even sending you to a site that looks exactly like the business's or bank's website, but is actually a fraudulent site. Reputable companies will never ask for your personal or financial information in this manner. Note that similar attempts to steal your identity can take place by telephone (sometimes referred to as "vishing"). If you're not sure who you are dealing with when someone calls claiming to be from your financial institution, hang up, and call to confirm using the telephone number that appears on your financial statements, not the telephone number given to you by the person calling you.

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

Personal Electronic Devices

Any electronic device with personal information could be used to steal your information if a thief were to gets their hands on it. Personal digital assistants (PDAs), cellphones, digital audio players or laptops can all carry your personal information. In order to protect your information, try to create passwords when possible. Most devices offer a way to “lock” the device so that the information can only be accessed with a password. Also, when carrying an electronic device, carry it in a manner that you cannot easily drop it or mistakenly leave it somewhere. If you plan to sell, give away or discard an electronic device, ensure you take measures to properly erase all of your personal information from the device. Most manufacturers can provide you with information on how to do so.

Keep your Key Documents Secure

Only carry the ID that you need:
If you drive, you will need to carry your driver’s license of course, and it is also a good idea to carry your provincial or territorial health card as well. However, your birth certificate, SIN (Social Insurance Number) card and passport/citizenship cards should be kept under lock and key, unless you need to bring them with you for a specific purpose. If the documents are stolen they can be used to commit a crime or to impersonate you, resulting in serious consequences. If you do need to carry an important ID card with you, be sure to keep a photocopy of it in a safe place.

Types of documents to keep secure:

- Birth certificate
- Social Insurance Number
- Passport

Note that your Social Insurance Number (SIN) is a confidential number that is only required, by law, for tax reporting if a customer is earning income (either employment or investment).While many companies may ask for you SIN for other purposes, you have the right to refuse under these circumstances. For more information visit the Office of the Privacy Commissioner of Canada at www.privcom.gc.ca.

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

Identity Theft: What to do if it Happens to You

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)
  Northern Credit Bureau at www.creditbureau.ca (1-800-532-8784)
  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). Note that Quebec, British Columbia, and Alberta have separate privacy laws that are similar to PIPEDA, so if you live in one of these provinces, contact the corresponding Provincial Commissioner.
- 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)

Keep Records

Be sure to record the steps you've taken to report the fraudulent use of your identity. Use the following chart to help you, make sure you keep it in a safe place for reference.

Banks, Credit Card Issuers and other Companies				
Company	**Address and Phone Number**	**Date Contacted**	**Contact Person**	**Comments**

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

Credit Reporting Agencies				
Agency	**Phone Number**	**Date Contacted**	**Contact Person**	**Comments**
Equifax Canada	1-866-779-6440			
Trans Union Canada	1-877-525-3823			
Trans Union Canada Québec residents	1-877-713-3393			
Northern Credit Bureau	1-800-465-7166			

Law Enforcement					
Agency	**Phone Number**	**Date Contacted**	**Contact Person**	**Report Number if available**	**Comments**
Local Police					
Phonebusters	1-888-495-8501				

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. Although **1 800 O-Canada** agents can direct you to your provincial or territorial government for key documents issued by provincial or territorial governments, you can also contact them directly at the following coordinates:

Newfoundland and Labrador Tel.: (709) 729-2600 Web Site: www.gov.nl.ca	**Nova Scotia** Toll Free: 1-800-670-4357 Web site: www.gov.ns.ca	**Prince Edward Island** Telephone: (902) 368-4000 Web site: www.gov.pe.ca
New Brunswick Toll Free: 1-888-762-8600 Web site: www.snb.ca	**Quebec** Toll Free: 1-800-363-1363 Web site: www.gouv.qc.ca	**Ontario** Toll Free: 1-800-267-8097 TTY Toll-free: 1-800-268-7095 Web site: www.gov.on.ca
Manitoba Toll free: 1-866-626-4862 TTY: 204-945-4796 Web site: www.gov.mb.ca	**Saskatchewan** Web site: www.gov.sk.ca	**Alberta** Toll Free: 310-0000 TTY Toll Free: 1-800-232-7215 Web site: www.servicealberta.ca

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

British Columbia Toll Free: 1-800-663-7867 TTY Toll-free: 1-800-661-8773 Web site: www.gov.bc.ca	**Yukon** Toll free: 1-800-661-0408 TTY: (867) 393-7460 Web site: www.gov.yk.ca	**Northwest Territories** Telephone: (867) 873-7817 Web site: www.gov.nt.ca
Nunavut Telephone: (867) 975-6000 Web site: www.gov.nu.ca		

For information on debit card fraud and credit reports, contact the Financial Consumer Agency of Canada at 1-866-461-FCAC (3222) (pour les services en français: 1-866-461-ACFC (2232)) or visit their website at www.fcac-acfc.gc.ca)

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

The Identity Theft Statement: Frequently Asked Questions

What is the Identity Theft Statement?

- The Identity Theft Statement is a form created by Government, which helps you create written documentation of an identity theft incident.
- The Identity Theft Statement is a form that you can use 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.

Why should I use the Identity Theft Statement?

- In order to investigate an incident and correct their records, companies (financial institutions, credit card issuers and other companies) often need to receive information from the victim. You may be able to provide the necessary information over the phone, but in some cases the company will require written documentation.
- Some companies will accept the Identity Theft Statement to provide them with the information they need to begin an investigation. Instead of having to obtain each company's unique form, and fill it out separately, you can complete one form and send a copy to each company, if they accept the statement. This can save you time and help streamline the process of putting a stop to the fraud and clearing your name.
- Even if a company does not accept the Identity Theft Statement, having all of the important information about the incident in one document can help you when filling out the company's forms.

How will companies use the Identity Theft Statement?

- Financial institutions, credit card issuers and other companies that accept the Identity Theft Statement will use the information in the form to begin an investigation into the incident. They may ask you for additional information to help with the investigation.
- Completing the Identity Theft Statement or any of the forms required by the company does not guarantee that the identity thief will be prosecuted or that the debt or charges will be cleared.

How do I complete the Identity Theft Statement?

- After you have made all the important phone calls, complete the Identity Theft Statement (and any other required documentation) as soon as you can after becoming aware of the incident. This will allow investigations to begin sooner and prevent further damage.
- Provide as much information as you can. This will help the company carry out its investigation and resolve your claim.
- Fill out both parts of the statement: Part One asks for general information about you and the identity theft**.** Part Two asks you for specific information about accounts and activities. ***Complete this section specifically for each company you're notifying, and send each company only the information that relates to accounts or activities with that company.***
- Once you have completed and signed the Statement, attach copies (not originals) of any supporting documents you have (for example, transaction records, receipts, a police report). Keep a copy of everything that you are submitting, for your records.

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

Where do I send the Identity Theft Statement?

- Provide a copy of the completed Identity Theft Statement and attached documents to each company that provided the identity thief with unauthorized credit, money, goods or services and that accepts the statement. Send it by registered mail. However, do not send the statement to government agencies.

How will I know that my personal information is safe when I submit the Identity Theft Statement?

- Companies that receive the Identity Theft Statement must ensure that the personal information you provide is safeguarded and is only used for the purposes of investigating the incident described in the Statement, prosecuting the person(s) responsible and preventing further fraud or theft. The companies may disclose the information to law enforcement institutions or agencies only for these purposes. The information may not be used or disclosed for any other purpose except as authorized by law.
- You may wish to take precautions when you submit the Identity Theft Statement. For example, if the company has a branch or office in your community, you may want to deliver the Identity Theft Statement personally. Alternatively, you should send it by courier or registered mail.
- You should keep a copy of all documentation that you provide, and store it in a secure place.

I've taken all the recommended steps. What can I expect now?

- By quickly taking the steps described here, you can help stop the imposter from doing any further harm, and start the process of clearing your name. Unfortunately, this process can require time and effort from you: writing letters, making phone calls, and providing documentation and other information. In addition, the problem may not be resolved right away.

The following measures can help in your effort to resolve the incident:

- Keep a log of all your phone calls – write down the name of anyone you talked to, what he or she told you, and the date your conversation occurred.
- In complex cases, you may want to follow up in writing with contacts you've made on the phone or in person.
- Keep the originals of supporting documentation, like police reports, and letters to and from companies; send copies only.
- Keep old files even if you believe the case has been resolved. Errors can reappear on your credit reports or your information can be re-circulated. Should this happen, you'll be glad you kept your files.

Cat. No. Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155