Ministry of
Justice and
Attorney General

Consumer Protection Branch

Consumer Tip

This tipsheet is intended to provide general information and is not a substitute for legal advice.

Tips for Reducing the Risk of Identity Theft

Identity theft (ID theft) is on the increase. It's one of the fastest growing crimes in the marketplace. This tip sheet identifies key ways to reduce your risk of becoming a victim of identity theft.

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 or theft.

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. In addition to names, addresses and phone numbers, thieves look for social insurance numbers, drivers licence numbers, credit card and banking information, bank cards, calling cards, birth certificates and passports.

They may physically steal important documents, or they may find out your personal information in other ways, without your knowledge.

Once they steal the information, identity thieves can manipulate it and invade your personal and financial life. They can use stolen identities to conduct spending sprees, open new bank accounts, divert mail, apply for loans, credit cards, and social benefits, rent apartments and even commit more serious crimes and, once arrested, they use their new identity.

What are some of the signs your identity might have been stolen?

- Bills and statements don't arrive when they are supposed to - they may have been stolen from the mailbox or someone has changed the mailing address.
- You receive calls from collection agencies or creditors for an account you don't have or that is up to date. Someone may have opened a new account in your name, or added charges to an account without your knowledge or permission.
- Financial account statements show withdrawals or transfers you didn't make.
- A creditor calls to say you've been approved or denied credit that you haven't applied for. Or, you get credit card statements for accounts you don't have.
- You apply for credit and are turned down, for reasons that do not match your understanding of your financial position.

Three key ways to reduce your risk

While you probably can't prevent identity theft entirely, there are important steps that you can take to minimize your risk, by managing your personal information wisely and cautiously.

1. Guard your personal information and documents.
2. Keep your computer and its contents safe.
3. Be vigilant.

Identity thieves get your personal information by:

- Buying the information from a dishonest employee working where personal and/or financial information is stored.
- Removing mail from your mailbox or fraudulently redirecting your mail.
- Stealing personal and private information from wallets, purses, mail, your home, vehicle, computer, and Web sites you've visited or e-mails you've sent.
- Retrieving personal information in your garbage or recycling bin by "dumpster diving".
- Posing as a creditor, landlord or employer to get a copy of your credit report or access to your personal information from other confidential sources.
- Tampering with automated banking machines (ABMs) and point of sale terminals,

enabling thieves to read your debit or credit card number and personal identification number (PIN).

- Searching public sources, such as newspapers (obituaries), phone books, and records open to the public (professional certifications).

1. Guard your personal information and documents

- If any of your key documents (such as your birth certificate, driver's licence, passport, bank card or credit card) are lost or stolen, notify the issuer immediately.

- Shred or destroy sensitive personal documents before tossing them into the garbage or recycling. This will defeat dumpster divers looking for transaction records, copies of credit applications, insurance forms, cheques, financial statements and old income tax returns.

- Beware of mail, phone or Internet promotions that ask for personal information. Identity thieves may use phony offers to get you to give them your information.

- Cut up expired and unused credit and debit cards. The card may have expired but the number may still be valid.

- 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.

- If you use ABMs or point-of-sale terminals, always shield the entry of your PIN, and never give your access code (PIN) to anyone. Choose a PIN that can't be figured out easily, 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.

- Don't leave personal information lying around at home, in your vehicle or at the office. Keep your birth certificate, passport and social insurance card in a safe place, such as a safety deposit box at your financial institution, when you're not actually using them. Other important papers, such as diplomas and degrees, marriage certificates, insurance policies, tax returns,wills, stocks, bonds and term deposits would also be safer in the safety deposit box, rather than in a file cabinet at home.

- Find out how your employer makes sure your personal information is private. How do they store and dispose of it? Who can see it?

- Don't give personal information to anyone who phones or e-mails you unless you know who they are or can confirm that the person is from a legitimate company. Identity thieves may pose as representatives of financial institutions, Internet service providers and even government agencies to get you to reveal identifying information.

- Don't put more than your name and address on your personal cheques.

- Carry only the documents and cards you will need that day. You rarely need to carry your birth certificate, SIN card or passport.

- When you receive a renewal or replacement for a document or certificate that contains identity information (such as your driver's licence or vehicle registration), make sure you return or destroy the old one.

2. Keep your computer and its contents safe

Computer technology makes it easier for criminals to find personal and financial information. If you keep credit card numbers, account numbers, and tax information in your system or use e-mail to do financial business, take steps to make sure that this information is safe from hackers and thieves. The following measures can help protect against identity theft on-line.

- Protect your computer, including laptops, with a startup password that is a combination of letters (upper and lower case), numbers and symbols. Don't use an automatic login feature that saves your user name and password.

- Use a personal firewall, especially if you use an "always connected/ always on" Internet connection, even if your computer is turned off. The firewall stops uninvited visitors from getting access to your information in the computer.

- Disable file-sharing software to prevent unauthorized access to your computer and its data.

- Install virus protection software and be sure to update it regularly. Viruses can damage your data and instruct your computer to send information to other systems without your knowledge.
- Be careful what you open. E-mails from strangers could contain viruses or programs to hijack your Internet connection or damage your computer.

- Don't send personal or confidential information over e-

mail. E-mail messages are not secure.

- Even though you've deleted files from folders, remnants may still be on the computer's hard drive, where they may be easily retrieved. Make sure personal information is really deleted before you sell, recycle or discard your computer. Use a secure hard drive overwrite utility to reduce the risk that others could recover your data.

Shop and bank safely online:

- Before giving your credit card number or other financial information to a business, make sure that 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 Web site is secure look for:

  - A Web site address that starts with https://, or

  - An icon, often a lock or an unbroken key, at the bottom right corner of the screen.

- Fake or "spoof" Web sites are designed to trick consumers and collect their personal information. Be cautious when clicking on a link or an unknown Web site or unfamiliar e-mail. The link may take you to a fraudulent site.

- After completing a financial transaction or on-line banking, make sure you sign out of the Web site and clear your internet file/caches (internet files are retained in your computer automatically and thus should be cleared so that hackers can not obtain the information). Most financial institutions provide instructions on how to clear the caches under their "security" section.

- Companies may also display a seal on their Web site to assure online customers that their business has the ability to maintain privacy and security for Internet transactions. Check to see which organization is awarding the seal and what requirements a merchant has to meet to display the seal.

- Prior to submitting any personal information to an Internet Web site, review the Web site privacy policy for an understanding of how your information may be used.

3. Be vigilant

Paying attention to details can make a difference.

- Once a year, get a copy of your credit report from the major credit reporting agencies (credit bureaus). The report tells you what information the bureau has about your credit history, financial information, any judgments, collection activity and who has asked for your information.

  You can call:
  Equifax Canada at
  1-800-465-7166
  Trans Union Canada at
  1-866-525-0262
  (Quebec Residents:
  1-877-713-3393)
  Northern Credit Bureau
  1-800-523-8784
  You may also visit their Web sites at
  www.equifax.ca
  www.tuc.ca
  www.creditbureau.ca

- By checking, you can spot debts that aren't 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.
- Know when your credit card and financial statements and utility bills are due. If they don't arrive when they are supposed to, call the company - an ID thief may have changed the billing address.

- Pay attention to credit card expiry dates. If the replacement card hasn't arrived call the company. Someone may have taken it from the mail or changed the mailing address.

- Keep credit card, debit card and automatic banking machine (ABM) transaction records so you can match them to your statements.

- Review your bank and credit card statements promptly and report any discrepancies to your financial institution right away.

- 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.

- A cardholder can be liable for losses associated with debit card transactions if they have contributed to the unauthorized use of the card. However, the loss will not exceed the established debit card transaction withdrawal limits. For more information, visit http://strategis.ic.gc.ca/debitcard

- Memorize all passwords and personal identification numbers. If you must write them down, ensure that they are well disguised, for example, by re-arranging the numerals or substituting other numerals or symbols and by keeping it within a record of other information, such as a telephone list.

Keeping Your Key Documents Secure

Documents that contain important personal information, such as your driver's license, birth certificate,

Social Insurance Card, passport, or citizenship and immigration documents can be resources for identity thieves. Criminals can use these documents to obtain others and to gain access to more of your personal and financial information. Keep these documents safe to ensure that they don't fall into the wrong hands. If one of these documents is lost or stolen, notify the issuing agency right away.

Driver's/operator's licence

A driver's/operator's licence has become the most universally accepted and trusted picture identification card issued by government. While its purpose is to show that you have the privilege to drive, society generally accepts the driver's/operator's licence as an identity document.

Because it's so well accepted, if your driver's licence is stolen, scanned, faked or obtained fraudulently, it can serve as a crucial tool for committing crime.

Motor vehicle and driver's licence issuing agencies across North America are working together to make it harder to forge driver's/ operator's licences and to tighten the controls used when issuing licences.

Birth certificate

The birth certificate is the primary government document issued to anyone born in Canada. The birth certificate is required when applying for a passport or Social Insurance Card as well as for other provincial or federal programs.

Birth certificates, unlike many identity documents, don't have an expiry date. You shouldn't carry your birth certificate in your wallet or purse. Keep it in a secure place such as a safety deposit box.

Social Insurance Number

Social Insurance Numbers (SINs) are used in a wide variety of databases as a primary identifier. Computer-savvy criminals can collect information about you by searching databases.

Although certain government departments and programs are authorized to collect and use the SIN, there is no legislation that prohibits other organizations asking for it. You can challenge a request for your SIN. The Office of the Privacy Commissioner of Canada has a fact sheet with more details. (1-800-282-1376 or http://www.privcom.gc.ca/)

You do not have to give your SIN to anyone who isn't authorized to collect the information. Also, don't carry your SIN in your wallet, purse or car. Keep it in a secure place like a safety deposit box.
Other important government-issued documents include the Passport, issued by the Canadian Passport Office, and the Permanent Resident Card and Certificate of Canadian Citizenship, issued by Citizenship and Immigration Canada. If you have any of these documents, carry them only when needed, keep them in a safe place and report them if lost or stolen. For further information on Identity Theft visit:
http://ConsumerInformation.ca

Key Government Documents: Contact Information

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

Federal Government

Key documents issued by the federal government include your Social Insurance Card, Passport, Citizenship and Immigration Documents and the Certificate of Indian Status.
For information on Government of Canada programs and services,

Call **1 800 O-Canada** (1 800 622-6232).

If you use a TTY call 1 800 465-7735.

Visit: www.canada.gc.ca

Privacy Commissioner of Canada

Toll Free: 1-800-282-1376
TTY: (613) 992-9190
Web site: www.privcom.gc.ca
E-mail: info@privcom.gc.ca

Provincial and Territorial Governments

Key documents issued by Provincial and Territorial governments include your birth certificate, driver's licence, and health card, among others.

For more information contact:

Ministry of Justice
and Attorney General
Consumer Protection Branch
Suite 500
1919 Saskatchewan Dr.
Regina, SK S4P 4H2
Phone (306) 787-5550
Toll free: 1-888-374-4636
(Within Saskatchewan)
Fax: (306) 787-9779

Email: consumerprotection@justice.gov.sk.ca

http://www.justice.gov.sk.ca/cpb

A current version of this Consumer Tip and other Consumer Tips are available at the Consumer Protection Branch Web site at http://www.justice.gov.sk.ca/cpb
Most public libraries have Internet access available if you do not have Internet at home.

If you need more copies of this tipsheet, you have permission to photocopy. Please check the Web site or contact our office to make sure you have the most up-to-date copy.

January 2008
G:\FA\CP\Common\Computer\Justice Web Site\Licensing and Investigation\Consumer Tips\2008\Tip Identity Theft Jan 2008.doc

Identity Theft – What to do if it happens to you

Identity theft occurs when someone uses your personal information to commit fraud or theft – such as opening accounts or incurring debt in your name, or taking money from your account. If you believe that you have been a 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 identity theft, take the following steps:

- ☐ Contact each financial institution, credit card issuer or other company that provided the identity thief with unauthorized credit, money, goods or services. Tell them what happened, and ask them to investigate the occurrence, cancel and re-issue any cards that were affected, and close any fraudulent or affected accounts. Also find out:

  - Does the company require written documentation to begin investigating your claim of identity theft?
  - Do they accept the **Identity Theft Statement**?
  - Do they require any additional information?

  Complete the identity theft statement and/or any other required documentation and provide it to the company as soon as possible.

- ☐ Contact both of Canada's national credit reporting agencies, Trans Union Canada and Equifax Canada. 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, asking that creditors call you before opening any new accounts or changing your existing accounts. The credit report may reveal whether there are other companies where the identity thief has opened accounts or incurred debt in your name.

  You can call Equifax Canada at 1-800-465-7166, and Trans Union Canada at 1-866-525-0262 (Quebec Residents: 1-877-713-3393), toll free. You may also visit their Web sites at www.equifax.ca and www.tuc.ca.

- ☐ Report the incident to your local police department. Ask the police to take a report, if possible, and to give you the report number. If the police report is available, include it in all correspondence with financial institutions, credit issuers, other companies and credit reporting agencies.

- ☐ Report the incident to PhoneBusters National Call Centre, which has a mandate to gather information and intelligence about identity theft, and will provide advice and assistance to identity theft victims. You can call PhoneBusters toll-free at 1-888-495-8501.

- ☐ If your government-issued documents were lost or stolen, report them to the responsible ministry or department and request new documents.

IDENTITY THEFT STATEMENT

To: _____
(Name of financial institution, credit card issuer, or other company)

Part One: Information about You and the Incident

I, _____, state as follows:
(name)

Personal Information

(1) My full legal name is:

_____
(first) (middle) (last)

(2) My commonly-used name (if different from above) is:

_____
(first) (middle) (last)

(3) My date of birth is (y/m/d): _____/_____/_____

(4) My Address is:

_____

City: _____ Province/Territory: _____ Postal Code: _____

(5) My home phone number is: _____

(6) My business phone number is: _____

(7) I prefer to be contacted at:

__ Home

__ Business

__ Alternate number:_____

Name _____

Information about the Incident

Please check all that apply

8) I became aware of the incident through: _____
_____
_____
_____

9) I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this document.

10) I did not receive any benefit, money, goods or services as a result of the events described in this document.

11) My identification document(s), (for example, credit card, debit card, birth certificate, driver's licence, etc.), were:

____ lost on or about (y/m/d) _____/_____/_____
____ stolen on or about (y/m/d) _____/_____/_____
____ never received

Additional information (e.g. which cards, circumstances):
_____

_____

12) Additional Comments (for example, a description of the incident, what information was used or how a possible identity thief gained access to your information):

_____

_____

_____

Attach additional pages as necessary

This information notifies companies that an incident has occurred and it allows them to investigate your claim. Depending on the details of your case, each company may need to contact you with further questions.

Investigation and Enforcement Information

13) I have reported the events described in this document to the police or other law enforcement agency.

The Police ____ did ____ did not complete a report.

In the event that you have contacted the police or other law enforcement agency, please complete the following:

_____ Agency	_____ Officer
_____ Phone Number	_____ Badge Number
_____ Date of Report	_____ Report number, if any

Documentation

Please indicate the supporting documentation you are able to provide. Attach legible copies (not originals) to this document.

14) A copy of the report completed by the Police or law enforcement agency. *(if available)*

15) Other supporting documentation: (Describe):

Part Two: Statement of Unauthorized Account Activity

Complete this section separately for each company you are notifying.

As a result of the events described in the Identity Theft Statement (*check all that apply)*:

The account(s) described in the following table (e.g. deposit account, investment account, credit card account, etc.) was/were opened at your company in my name without my knowledge, authorization or consent, using my personal information or identifying documents.

My account(s) described in the following table (e.g. deposit account, investment account, credit card account, etc.) was/were accessed, used or debited without my knowledge, authorization or consent, using my personal information or identifying documents.

The unauthorized activity took place through *(if known):*

An in-person transaction

An automated banking machine

A point of sale purchase

An Internet transaction

A telephone transaction

A cheque

Other _____

Don’t know

The credit product(s) described in the following table (e.g. loan, mortgage, line of credit) as/were obtained from your company in my name without my knowledge, authorization or consent, using my personal information or identifying documents.

Name _____

Description of Unauthorized Account Activity

Company Name/Address	**Type of Account/**	**Description of unauthorized activity (if known)**	**Date (if known)**	**Amount (if known)**
Example: ABC Bank	Deposit Account 1234567-890	Withdrawal	01/02/02 or: All activity since 01/02/02	$500

Attach additional pages as necessary

If the incident involved a **mortgage**, please indicate

Lender's Name/Address	**Date of Registration (if known)**	**Legal description of the property**	**Municipal Address of The property**	**Registration Number of mortgage(if known)**

Attach additional pages as necessary

During the time of the incident(s) described above, I had the following account(s) opened with your company (*please list any account not mentioned above)*:

Billing Name _____

Billing Address _____

Account/Card Number

_____

Attach additional pages as required.

Protecting Your Privacy

I agree that companies to whom I provide the Identity Theft Statement may use the personal information in it only 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 (for example, police departments) for these purposes. The companies to whom I provide the Identity Theft Statement agree that this information may not be used or disclosed for any other purposes except as authorized by law. If this document or information contained in it is requested in a law enforcement proceeding (e.g. before a court or tribunal), the company may have to provide it or disclose it.

Signature

All statements made by me in this form are true and complete in every respect to the best of my knowledge and belief.

_____
Signature

_____
Printed name

_____
Date

Knowingly submitting false information in this Statement could subject you to criminal prosecution.