Victim Toolkit

Canadian
Identity Theft
Support Centre

1.866.436.5461
www.idtheftsupportcentre.org

identity theft

Canadian Identity Theft Support Centre

1.866.436.5461
idtheftsupportcentre.org

Suite 511, 475 Howe Street
Vancouver, B.C. V6C 2B3

Victim Toolkit

Table of Contents

- Introduction 1

- Glossary 2

- What to do if you become a victim 3
  1. Review your records 3
  2. Notify financial institutions 3
  3. Notify Canada Post 4
  4. Notify utilities and service providers 4
  5. Notify government agencies 4
  6. Put a Fraud Alert on your credit files 5
  7. Order a copy of your credit reports 6
  8. Review your credit report carefully and repeat previous steps as necessary 7
  9. Ask credit bureaus to block inaccurate information from your file 7
  10. Report the crime to the police and get copy of incident report 7
  11. Work with creditors to confirm the fraud and clear your name 8
  12. Report the crime to the CAFC 8
  13. Notify the Privacy Commissioner 9
  14. Monitor your accounts 9
  15. Keep track of your time and expenses 9

- Specific Issues 10
  - Making an Access to Information request 10
  - Fraudulent use of your SIN 10
  - Replacing your passport 11
  - Criminal records fraud 11

General Tips 13
  - Document everything 13
  - Be organized 14
  - Maintaining your Case Log 14
  - Tips for dealing with financial institutions and other large organizations 14
  - Dealing with debt collectors 14
  - Working with the police 14

Your Legal Rights 16
  - Privacy laws 16
  - Credit reporting laws 16
  - Debt collection laws 17
  - Land Title protection laws 17
  - Anti-spam laws 17
  - Other private rights of action 17
  - Criminal restitution 17
  - Victim rights in the criminal prosecution process 17

Key Contacts 18
  - Credit Bureaus 18
  - Credit Card Companies 18

Appendices:
  - CITSC Form 1: Identity Crime Victim Statement/Affidavit
  - CITSC Form 2: Contacts Log
  - CITSC Form 3: Case Log (sample)

CITSC Sample Letters:
  - CITSC SL 1: Information Request re: Fraudulent Transactions
  - CITSC SL 2: Demand Letter re: clearing your records
  - CITSC SL 3: Follow-up Request for Letter of Clearance

identity theft

Introduction

This toolkit is designed to help victims of identity theft restore their reputations.

You are a victim of "identity theft" if your personal information has been used by someone to access your bank account, credit card or other account without your authorization, to obtain loans or other benefits in your name, or to evade authorities.

The term "identity theft" is used by CITSC to mean not just the stealing of personal information, but also the fraudulent use of that information (i.e., identity fraud). Both "identity theft" and "identity fraud" are criminal offences in Canada. Related activities such as redirecting mail and selling fraudulent identity documents are also criminal offences.

The police cannot find and charge every identity thief. Many identity criminals are adept at hiding their location and identity from law enforcement. Many operate from abroad, making it difficult for police to investigate and prosecute the offence. Even if it is possible to identify the perpetrator, the police may have other priorities. For this reason, we suggest that you focus your energy on undoing the damage and preventing further damage. This toolkit is designed to help you do that.

Cases of identity theft vary widely in terms of the damage they cause to victims. In some cases, you may be quickly reimbursed (or never charged) for fraudulent transactions in your name and your credit may not be affected. Other cases can do serious damage to your credit, take months to unravel, involve many organizations, and require countless hours of your time in the process of clearing your name.

Once you know that your identity has been stolen and/or misused, you should be prepared to spend the time and effort it takes to restore your reputation. This toolkit explains what you need to do and provides tips on how to do it effectively. If you have questions about your case or need help, contact the Canadian Identity Theft Support Centre ("CITSC"). We are here to help you.

Glossary

Affidavit: A formal statement of fact sworn by the author and witnessed by a lawyer, Notary Public or Commissioner of Oaths who vouches for the authenticity of the author's signature and, by extension, the authenticity of the document.

Creditor: A company that lends money or extends credit to consumers. Creditors include financial institutions such as banks, trust companies and credit unions; standard credit card issuers such as VISA, Mastercard and American Express; retail and specialty credit card issuers such as Sears, The Bay and Diners Club; and service providers such as phone companies and utilities who bill for services provided in advance.

Credit Freeze (also known as "Security Freeze"): In the U.S. (but not Canada), consumers can have their credit reports "frozen". This prevents companies from viewing their credit reports except in specifically authorized situations (such as an existing loan). A credit freeze is an effective way to stop thieves from opening new accounts because most creditors will not approve applications without checking the applicant's credit. It is ineffective however if a creditor does not check the applicant's credit record before opening the new account. Nor does it stop identity criminals from stealing from existing accounts. Credit freezes are especially useful for older people who do not need to apply for credit; they can be cumbersome for people who need access to credit.

Credit Report: Also sometimes referred to as Credit History: A record of an individual's past history of borrowing and repaying money in any form for any purpose. It includes information about credit applications, bill payments, late payments and bankruptcies. The information is used primarily by lenders (including credit card companies and cell phone companies as well as banks) to assess an individual's credit worthiness or willingness/ability to repay debts before extending credit.

Fraud Alert: A notation on your credit file that you are or may be the victim of identity fraud. Fraud alerts signal to the credit issuer that extra vigilance should be used to verify an application for credit in your name. Fraud alerts do not affect your credit score but may slow down the regular credit process when using a credit card, for example. Fraud alerts are only reliable to the extent that creditors heed them by taking extra precautions to verify the identity of the individual purporting to be you.

SIN: Social Insurance Number: A unique number issued by the federal government to each individual wishing to work in Canada or to receive benefits and services from government programs. The SIN is required for purposes of employment, income tax, pensions, interest or income from financial savings, and certain government benefits and services. See http://www.servicecanada.gc.ca/eng/sin/info/yoursin.shtml for more information on how the SIN is used and when you can refuse to provide it.

What to do if you become a victim

As soon as you become aware that someone stolen your identity or account information, or has used your information fraudulently, you must take some immediate steps to prevent further damage. In particular, you must notify relevant creditors, credit bureaus and document issuers of the fraud or potential fraud and close affected accounts. DO NOT DELAY.

Keep track of all your communications and actions in a journal (your "Case Log" – see CITSC Form 3 for a sample). Use CITSC Form 2 ("Contacts Log") to keep track of key contacts you make with creditors and others. Tips on how to document your case and how to stay organized are provided later in this Toolkit. Contact information for key organizations is provided at the end of the Toolkit.

1. Review your records

Quickly identify all lost, stolen or compromised bank cards, payment cards, cheques, account information and/or identity documents. Review your bank, credit card, utility and/or other suspect account statements and identify any transactions that you did not authorize. Determine if you are missing any account statements normally received by mail. Make a list of all documents and accounts that you think have been compromised.

2. Notify the financial institutions involved

If your debit card, credit card, cheque or bank account has been used without your authorization, **contact the financial institution and report it immediately.** If you report lost, stolen or compromised credit cards immediately, the financial institution will cover the fraudulent transactions for you. They may do so for debit cards and cheques as well – it will depend in part on how quickly you act.

• Credit card loss or fraud: If you have the card, call the telephone number on the back of the card. If you don't have the card, call the number provided on your account statements or in the phone book. If your card has been compromised, the company will issue you a new one with a new number.

• Lost debit card: If there is any chance that the card could be used by someone else to access your account, call the bank or go to your branch in person. Close the account and open a new one with a new PIN/password.

> Secure passwords have at least eight characters and are a combination of at least three of the following: numbers, symbols, lower case letters and capital letters. They do not include names or words, especially those that could be guessed by an identity thief or someone you know.

• Stolen cheques: Call the bank or go in person. Put a "stop payment" on the stolen cheques if you know the cheque numbers. Close the account permanently and open a new one with a new PIN/password. Choose secure passwords and PINs and do not share them with anyone.

• Unauthorized transactions on your bank account: If someone has been accessing your bank account without your authorization, contact your bank branch or go in person. Ask to speak with a fraud investigator. Determine whether the account was accessed via your debit card, cheques or otherwise. Insist that the matter be thoroughly investigated. Close the account permanently and open a new one with a new PIN/password. If a new loan or other account has been fraudulently set up in your name, contact the company and close the account.

• Ask what address is on the account and note any addresses that are not yours. Contact Canada Post to correct any fraudulent addresses (see below).

• Have the financial institution note on the account that it was permanently closed at your request because of identity fraud.

• Ask that any new requests for service first be confirmed with you.

• If the financial institution provided the criminal with unauthorized credit, money, information, goods or services in your name, insist that the company investigate the occurrence. Find out:

• What information does the company need to start an investigation?

• Has the company already started a criminal investigation? If so, with which police force? What is the report number?

• What do you need to do to have your losses reimbursed?

3. Notify Canada Post

If you are missing mail and suspect that it has been redirected to another address, contact Canada Post at www.canadapost.ca (1-800-267-1177). Ask what address they have on record for you. If it is not your current address, instruct Canada Post to change it back and to have all mail addressed to you sent to your current address.

Note: If your mail is being stolen after it has been delivered (e.g., from an unsecured mailbox), it is considered theft of personal property and is a matter for the police.

For more information, see http://www.canadapost.ca/cpo/mc/aboutus/corporate/securitymailtheft.jsf

4. Notify utilities and service providers

Identity criminals sometimes open telephone or other utility accounts in their victims' names, then run up bills that they don't pay.

If this may have happened in your case, contact the service provider (e.g., local, long distance and cell phone, Internet, television, electricity and gas) and ask if any new accounts have been opened in your name recently. Close any accounts that were fraudulently opened. Have the company note on the account that it was permanently closed at your request because of identity fraud.

• Ask that any new requests for service first be confirmed with you.

• If the company provided the criminal with unauthorized services in your name, insist that the company investigate the occurrence. Find out:

• What information does the company need to start an investigation?

• Has the company already started a criminal investigation? If so, with which police force? What is the report number?

• What do you need to do to have your losses reimbursed?

If you have reason to suspect that the thief might try to open a(nother) utility account in your name, inform the company that attempts may be made to open new service using your identification information. Ask that any new request for service be confirmed with you before it is approved.

Do this in writing and keep a copy of each request. Your records will be useful if the company fails to confirm a fraudulent application made in your name.

Use **CITSC Form 1: Identity Crime Victim Statement/Affidavit** to provide financial institutions, creditors, service providers, document issuers, and others with the information they need to start an investigation, clear your record, issue replacement documents, or refund you for fraudulent transactions. Once you have completed the form, take it to a lawyer or notary public to have commissioned as a formal Affidavit. An Affidavit is much stronger than a Statement and may be required by some creditors before they will take action on your case.

5. Notify document issuers

If you have reason to suspect theft or fraudulent use of your government-issued identification (i.e., social insurance number, birth certificate, health card,

drivers licence, passport, immigration documents), immediately report the loss, theft or suspected fraud to the appropriate government agency (listed below). The agency will explain what steps you must take to have the document replaced.

• If your **passport** has been lost or stolen, contact Passport Canada at
1-800-567-6868 TTY services: 1-866-255-7655
Outside Canada and the United States:
819-997-8338
http://www.passport.gc.ca
See below under "Specific Issues" for instructions on obtaining a replacement passport.

• If your **immigration documents** have been lost or stolen or if you suspect that someone is using them fraudulently, contact Citizenship and Immigration Canada at 1-888-242-2100
TTY services: 1-888-576-8502
http://www.cic.gc.ca

• For all **other government-issued identity documents** (e.g., SIN, birth certificate, health card, drivers licence) contact Service Canada at
1-800-O-Canada (1 800 622-6232)
TTY: 1 800 926-9105.
You can also visit your local Service Canada Centre in person. An agent will direct you to the appropriate federal or provincial organization to replace each of your cards.

• To get a replacement SIN card or to talk to a government agent about replacing your Social Insurance Number due to fraud, call 1-800-206-7218. For more information on SIN fraud, see below under "Specific Issues".

• In order to replace your drivers' licence, you will likely be required to provide primary identification (e.g., a passport or citizenship card) and secondary identification (e.g., a debit or credit card). You will also have to pay a fee.

• Birth certificates are managed through the Registrar of Vital Statistics in your province or territory of birth. You will be required to complete a Declaration of Lost or Stolen Birth Certificate in order to cancel and replace the missing certificate. This can be done at the Vital Statistics office. If you have kept a photocopy of the certificate, showing the certificate number and issue date, the process of replacing your birth certificate will be faster.

6. Put a Fraud Alert on your credit files

If you are not yet sure whether a thief has been using your identity fraudulently (e.g., if you have simply lost your ID and have no evidence that it was used fraudulently), skip this step.

Every credit application made in your name, as well as your history of payment on every loan or credit account you set up, is reported to one or both of Canada's two credit reporting agencies (also known as "credit bureaus"): Equifax and TransUnion. These companies maintain credit files on Canadian consumers.

Once you know that you have been the victim of financial fraud, ask each credit bureau to put a "Fraud Alert" on your file. A Fraud Alert on your file will alert creditors to the fact that someone else may be pretending to be you, and requires creditors to take extra precautions to verify the identity of the person applying for credit. The alert will stay on your file for six years unless you file a written request for it to be lifted.

To request a Fraud Alert, call each credit bureau and follow the prompts:
Equifax Canada: 1-800-465-7166
TransUnion Canada: 1-800-663-9980
(Québec 1-877-713-3393)

When you place the Fraud Alert, ask the credit bureau to provide corrected information to any creditors who received inaccurate information about you because of the fraudulent transactions. If the credit bureau refuses to do this, you will have to determine who those creditors are yourself (by reviewing your credit report) and notify them of the fact that they received inaccurate information about your credit history. (You should do so in any case, as a cautionary measure.)

If you don't need to access credit, you can ask the credit bureau if it will "freeze" your credit file so that

creditors cannot access it unless you temporarily lift the freeze. A credit freeze will stop a thief from opening new accounts in your name as long as creditors require a credit check before extending credit to the imposter. (Note: Credit freezes do not stop creditors from improperly extending credit to imposters. Nor do they stop thieves from accessing your existing accounts.) Credit freezes are especially useful for older people who do not need to apply for credit. Credit bureaus in the U.S. offer credit freezes, but they are not required to do so in Canada.

7. Order a copy of your credit reports

In order to determine whether you have been the victim of financial identity theft or to find out what financial activities the thief has been conducting in your name, you will need to obtain a copy of your credit reports. Equifax and TransUnion are each required to provide you with a copy of your credit report upon request. If you have been a victim of identity theft, you should check your credit reports every few months.

> Even if you have not been victimized, it's a good idea to review your credit reports every year as a preventative measure.

These reports will show accounts that have been opened in your name, your payment history on every account, and the names of creditors who have made inquiries about you when you (or someone pretending to be you) applied for credit from them. You should order your report from both credit bureaus as there may be information on one that is not on the other.

The report is free of charge if ordered by phone or mail but there is a charge for online access. You will need to provide proof of your identity to the credit bureau in order to get a copy of the report. See below for how to order your credit reports.

How to order your credit report

• **By Phone:** Call each of the telephone numbers below and follow the instructions. Both Equifax and TransUnion use automated phone systems. Each system gives several options, including one for obtaining your credit report, and another for placing a Fraud Alert. Be patient and follow the automated instructions (see below for reporting fraud). If you need to speak to a customer service representative, call during office hours and follow the prompts until you get to one that is for speaking to a live agent. If you don't want to provide your Social Insurance Number, you may need to order your report by mail or fax.

Equifax: 1-800-465-7166
TransUnion: 1-800-663-9980

• **By Mail or Fax:** Each credit bureau has its own form that you must fill out to order your credit report by mail. The forms can be downloaded from their websites (see links below), or you can phone the telephone numbers above and request that the form be sent to you.

Equifax credit report request form:
http://www.equifax.com/ecm/canada/EFXCreditReportRequestForm.pdf (English)

http://www.equifax.com/ecm/canada/demandededossierdecredit.pdf (French)

TransUnion credit report request form:
http://www.transunion.ca/docs/personal/Consumer_Disclosure_Request_Form_en.pdf (English)

http://www.transunion.ca/docs/personal/Consumer%20Disclosure%20Request%20Form%20_fr.pdf (French)

Follow the instructions on each form. Along with the completed form, you will need to send photocopies of two pieces of identification and/or proof of residence (e.g., a copy of a utility bill with your current address).

• **In person:** If you happen to live close to one of TransUnion's offices, you can go there in person and obtain a copy of your credit report. Be sure to bring government-issued photo ID and a copy of a utility bill with your current address. As of April 2011, TransUnion had offices in the following

cities: Laval, Que; Burlington, ON; Halifax, NS; Charlottetown, PEI; St.John's NL. For a list of locations, see:
http://www.transunion.ca/sites/ca/personal/consumersupport/contactus_en.page

• **Online:** Each credit bureau offers online access to your credit report (credit monitoring services) for a fee. For more information on these options, see:
http://www.equifax.com/compare-products-ca/en_ca
http://www.creditprofile.transunion.ca/services/cmu/example.jsp?lang=en&loc=2059

8. Review your credit report and repeat previous steps as necessary

When you receive your credit reports, review them carefully. Note any accounts that appear to have been fraudulently opened in your name, and any inquiries by creditors to whom you did not apply for a service. Contact each of those creditors and notify them of the fraud (follow steps #2, 3, and 4 above as appropriate). Put a Fraud Alert on your credit files if you haven't already (step #6).

9. Ask credit bureaus to block inaccurate information from your file

If your credit reports show accounts that you didn't open or debts that you did not run up, this false information will be provided to companies to whom you apply for credit and you may be denied credit as a result. Until this information is removed from your credit record, it may create problems for you, even if you have put a Fraud Alert on your file.

At the same time that you are asking creditors for Letters of Clearance, ask the credit bureaus (Equifax and TransUnion) to block the inaccurate information from the credit report about you that they provide to businesses. Use CITSC Sample Letter 4 for this purpose.

10. Report the crime to your local police force

Once you are sure that you have been victimized, it is important to report the crime to the police. This is not so much to prompt a police investigation (police are unlikely to investigate your case unless it is unusually serious), but rather so that you can convince creditors, debt collectors and others that you have in fact been victimized. You may need to prove to creditors that you have reported the incident to the police in order for them to believe you and to take your case seriously.

• If possible, attend the police station in person with photo ID and all documentation that you have gathered about the theft and/or fraud. Keep copies of all documents that you give to the police.

• Provide the police with a concise summary of the theft/fraud and all relevant documentation. Use CITSC Form 1: Identity Crime Victim Statement/Affidavit for this purpose.

• **Get a copy of the police incident report.** Creditors, debt collectors and document issuers may require this before they will believe that you are a victim of identity crime. Explain to the police that you need a copy of the incident report to prove to creditors that you are a victim and to clear your name. **If you can't get a copy of the police report, get the report number.** You can then at least provide the report number to creditors who ask for it (and they can request a copy from the police directly).

• Have a police officer sign your Identity Crime Victim Statement/Affidavit as a witness with the date and his/her badge number. This will provide further legitimacy to your Statement/Affidavit and may allow it to serve as a police incident report for some purposes.

See below under "Filing an incident report with the police" for more tips on reporting the crime to police.

Use CITSC Form 1: Identity Crime Victim Statement/Affidavit to provide financial institutions, creditors, service providers, document issuers, and police with the information they need to clear your record, issue replacement documents, refund you for fraudulent transactions, or start an investigation.

11. Work with creditors to confirm the fraud and clear your name

If you have lost money or become indebted as a result of identity fraud, you will need to work with financial institutions and any other creditors to confirm that the transactions were indeed fraudulent and to clear your records of the fraud. You should do the following (in writing as well as verbally):

- Insist that the company (bank, service provider, etc.) investigate the matter. Speak with the company investigator and provide him/her with all relevant details.

- Demand that the company immediately stop all collection activity on the account.

- If the company has taken any further actions such as reporting you to the police for passing bad cheques or otherwise engaging in criminal activity, demand that all such reports be withdrawn.

- Provide the company investigator with:
  - your signed and witnessed Identity Crime Victim Statement/Affidavit. If possible, have your Statement notarized as an Affidavit (i.e., a sworn statement). A sworn statement is stronger than a statement that is merely witnessed.
  - a copy of the police report (if you were able to get a copy) or the report number, the police force, and the name/badge number/contact information of the police officer/detective to contact.
  - your written consent to disclosure of all information regarding the fraud to the police.

- Ask that the company provide you (or the police detective/officer, at a minimum) with copies of all documents regarding the fraudulent transaction(s), including:
  - account applications made in your name
  - transaction records on the accounts in question
  - cheques written on the accounts in question
  - relevant portions of video surveillance tapes
  - any other relevant documentation that will help to confirm that the transactions were conducted by someone other than you

If the company refuses to provide you with information about applications or transactions made in your name, you can make a formal access to information request – see under "Specific Issues" below.

Ask the company to clear your records of the fraudulent transactions and cease reporting the fraudulent debts to credit bureaus as if they were your debts. Ask also that they notify organizations (including credit bureaus) that any incorrect information sent by them was the result of identity fraud and is incorrect. Use **CITSC Sample Letter 2** for this purpose.

Advise the company that failure to correct their records accordingly would violate the provision of Canadian privacy law requiring that the records they have about you are accurate, complete and up-to-date.[1]

Ask for a "Letter of Clearance", confirming that your records have been cleared of the fraud. Use **CITSC Sample Letter 1** for this purpose.

12. Report the theft or fraud to the Canadian Anti-Fraud Centre

The Canadian Anti-Fraud Center ("CAFC") compiles statistics on identity crime and other fraud in Canada. You can report your case to the CAFC by going to their website or by calling **1-888-495-8501.** The CAFC provides valuable assistance to law enforcement agencies all over the

1. Specific provisions of privacy laws requiring data accuracy are: Personal Information Protection and Electronic Documents Act, s.5, Principle 4.6; Alberta Personal Information Protection Act, s.33; B.C. Personal Information Protection Act, s.33; Quebec Act respecting the protection of personal information in the private sector, s.11.

world by identifying connections among seemingly unrelated cases. Your information may provide the piece that completes the puzzle.

13. Report security breaches to the Privacy Commissioner

Under Canadian privacy laws, organizations must ensure that personal information they hold is secure against unauthorized access. If you have reason to suspect that your information was wrongly acquired from a corporation or government, you can hold that organization accountable for its security breach by lodging a complaint with the Privacy Commissioner of Canada (or the Privacy Commissioner for your province or territory). Privacy Commissioners can investigate data breaches by corporations or governments. Some can issue binding orders; others are limited to recommendations, but those recommendations may form the basis of a lawsuit.

For advice on privacy issues related to the identity crime, or to lodge a complaint, contact the Privacy Commissioner of Canada at 1-800-282-1376 or www.priv.gc.ca.

If you live in Quebec, Alberta or British Columbia, your complaint or inquiry is more likely to fall within provincial jurisdiction since these provinces have adopted their own private-sector privacy laws, which are enforced by provincial privacy commissioners:

- Quebec http://www.cai.gouv.qc.ca
  1 888 528-7741
- Alberta http://www.oipc.ab.ca
  1-888-878-4044
- British Columbia http://www.oipc.bc.ca
  (250) 387-5629 (request toll-free access via Enquiry BC)

14. Monitor your accounts

An unfortunate aspect of identity theft is that the criminal may continue to use your information in fraudulent ways. You need to be vigilant even after you have cleared up the initial problem.

- Order copies of your credit reports regularly (every few months at first, then annually) and review them carefully.

- Monitor your bank statements and other service accounts closely, with a view to detecting any additional fraud.

- Monitor your mail - be alert to missing account statements – so that you can detect mail diversion early.

- Consider setting up an online alert to monitor any online activity in your name - see:
  http://www.google.com/alerts

15. Keep track of your time and expenses

There is a small chance that you will be able to recover compensation for the time and expense involved in recovering your reputation, either via a civil lawsuit or restitution if the offender is criminally convicted. In such cases, you must have evidence of your time and expenses in order to back up your claims.

- Get receipts for all of your expenses and keep them along with phone bills and other related expenses.

- Document the time you spend working on your case, daily. Don't wait to do this as you will forget how much time you spent.

Specific Issues

Making a formal "access to information" request

Under privacy laws applicable to private organizations in Canada, you are entitled to access "personal information" about you held by the organization. (The same is true under separate privacy laws applicable to government.) "Personal information" is broadly defined and includes all information about you, including applications and transactions attributed to you. Relevant provisions are:

• In Quebec: ss.27-29 of the *Quebec Act respecting the protection of personal information in the private sector*

• In Alberta: s.24 of the *Personal Information Protection Act*

• In B.C.: s.23 of the *Personal Information Protection Act*

• Elsewhere in Canada and all federally-regulated companies: ss.8-10 and clause 4.9 of Schedule 1 to the federal *Personal Information Protection and Electronic Documents Act*

Formal requests to access your information must be made in writing (see CITSC Sample Letter 1) and should be sent by registered mail to ensure receipt. The company has 30 days to respond. If the company fails to respond or refuses to provide you with the information, you can complain to the Privacy Commissioner of the relevant jurisdiction (Quebec, Alberta, B.C., or Canada).

Social Insurance Number Fraud

Your SIN is especially valuable to identity thieves because it is unique to you. If an identity thief gets hold of your Social Insurance Number ("SIN"), they may use it to impersonate you when applying for credit, government benefits, tax refunds, employment or other services. If someone uses your SIN to work illegally, you could be assessed taxes for income you did not receive.

You cannot get a new SIN merely because your SIN card has been lost or stolen. In such cases, you can get a replacement card but the number won't change.

If another person uses your SIN for employment purposes or to receive other taxable income, you will receive a Notice of Reassessment from the Canada Revenue Agency concerning undeclared earnings. This is an indication that your SIN is being used fraudulently. In such cases, it is possible to get a new SIN but this may not be worth the effort.

Even if your SIN is being used fraudulently, replacing it may not resolve the problem since identity fraud can still occur using your old SIN (e.g., creditors may still accept your old SIN as proof of the thief's identity). Getting a new SIN is generally only worthwhile if the imposter is using your SIN to obtain employment or government services, and even then it may not be necessary if the criminal is caught or ceases the fraud. Moreover, if you get a new SIN, you must contact all of your financial institutions, creditors, employers, and pension providers, past and present, and update them with your new number. And getting a new SIN does not relieve you of the need to go through all the other relevant steps to clear your financial and other records. Before requesting a new SIN, you should therefore consider whether it the effort is worth it.

If you think that your SIN is being used fraudulently, you can call 1-800-206-7218 to speak with a government agent about whether it is worth getting a new number. If you want to get a new number, you will need to gather certain documentation (see below) and bring it with you to a Service Canada Centre, where an investigator will review your information and provide you with assistance and guidance.

Documentation required for issuance of a new SIN due to fraud:

1. An original identity document (your birth certificate, or immigration or citizenship document)

2. If you suspect that your SIN is being used by someone else to obtain employment:

• A printout from the Canada Revenue Agency showing each employer that issued a T4 tax form for your SIN over the past 3 years. Call 1.800.959.8281 to request this printout. Check for any employers for whom you have not worked. Service Canada will contact them on your behalf.

• A clear photograph of yourself for each employer for whom you did NOT work. Service Canada will use this photo to confirm with the employer that you did not work for them.

• A list of each address where you lived during the past 10 years.

3. If you suspect that your SIN is being used by someone to obtain credit:

• A copy of the application(s) for credit in question, showing both your name and your SIN.

• A letter of clearance from the creditor confirming that the application was fraudulent and that you are not responsible for any purchases that may have been made as a result of the fraud; this letter must include both your name and SIN. If you have difficulty getting a response to your request for a letter of clearance, use CITSC Sample Letter 2.

For more information regarding SIN fraud and related issues, see:
http://www.servicecanada.gc.ca/eng/sc/sin/index.shtml
http://www.servicecanada.gc.ca/fra/sc/nas/index.shtml

Replacing your passport

Once you report your Canadian passport as lost or stolen, it becomes invalid and can no longer be used for travel. You will therefore need to obtain a replacement passport. Before you can be issued with a replacement passport, the authorities will conduct an investigation which may delay processing a replacement.

To obtain a replacement passport, you must provide:

• a completed application form, signed by a guarantor.
• two up-to-date photographs
• documentary proof of Canadian citizenship
• a declaration about the lost passport
• a fee

Go in person to any Passport Canada office, call or write:

Toll free: 1.800.567.6868
TTY: 1.866.255.7655
Outside Canada and the U.S.: 819.997.8338
(M-F, 7.30 a.m. – 8.00 p.m., ET)

By mail:
Passport Canada
Foreign Affairs and International Trade Canada
Gatineau, QC, K1A 0G3

By courier:
Passport Canada
22 de Varennes Street
Gatineau, QC, J8T 8R1

http://www.ppt.gc.ca/planification/203.aspx?lang=eng
http://www.ppt.gc.ca/planification/203.aspx?lang=fra

Criminal Records Fraud

Sometimes criminals will use a stolen driver's licence (or other identity document) to identify themselves as someone else when stopped by police. If you are accused of a criminal offence that you did not commit, and suspect that the person who committed the offence was pretending to be you, you will need to do the following:

• Explain to the police that you are a victim of identity theft.

• Ask the police to compare identifying features of the imposter (scars, tattoos, height and weight) with you. Provide as much personal information about yourself as required in order to allow the police to distinguish you from the offender. The police may want your fingerprints, a photograph, and personal documents with a photograph, such as a drivers' licence or passport.

• Find out what information the police have about the imposter. If they have a photograph or fingerprints of the offender, it should be easy to prove that you are not that person. Descriptive remarks made during the original arrest can help if fingerprints or photographs were not taken.

• If you have already completed an Identity Crime Victim Statement/Affidavit (CITSC Form 1), provide it to the arresting police force. If the arresting police force is different from the police force to which you have already provided an identity theft incident report, ask the latter police force to forward your identity theft incident report to the arresting police force.

• Once you have established your innocence, ask the police to update all relevant databases with an “imposter alert” as appropriate, as well as with the corrected information so that your name is no longer associated with the crime.

General Tips

Identity theft cases can be complicated and time-consuming. There may be many instances of unauthorized use of your personal information, and you may have to correspond with many different organizations in order to clear your name. You need to be organized.

Document everything

It is important that you record each contact that you make, whether by phone, e-mail, text, or hand-written letter. In order to be an effective advocate for your case, you need to be able to provide evidence of who you talked to, what they told you, and what you did to pursue the matter. Small details that seem unimportant at the time can become important later.

Your papers may become evidence in a criminal case. They should be treated with care; never submit an original unless requested and then always keep a copy.

File immediately and safely all documents related to your case, even those that may not seem significant at the time – they may prove to be useful later on. Important documents that should be carefully filed include:

- The police incident report (ie: a description of the incident signed by a police officer with the officer's badge number). This is one of the most important documents in your case since it serves as a form of proof that you were indeed a victim. Creditors and debt collectors may require this document before they will believe that the debt was fraudulently incurred by someone else in your name. If you can't get a copy of the police report, (a) get the report number and (b) have a police officer sign your Identity Crime Victim Statement/Affidavit as a witness.

- Your credit reports from Equifax and TransUnion, showing the fraudulent activity.

- Copies of all correspondence (letters, emails, etc.) that you send and receive regarding the case.

- Any other records that you receive or are able to obtain regarding the fraudulent transactions (e.g., applications for credit that you did not make, credit cards that you did not order, transaction records...)

- If the matter goes to court, all court documents, including any subpoenas, probation reports, or transcripts of testimony.

Be organized

Use **CITSC Form 2: Contacts Log** to keep track of your contacts and the results of them. In simple cases, you may need only one page. In more complex cases involving several different organizations, you may need several pages – make as many copies of the blank form as you need.

You should also keep a **Case Log** – i.e., a diary in which you record everything you do on the case, chronologically by date (see sample CITSC Form 3: Sample Case Log). Together with the Contacts form, this will become an official record of your case. It will also help you remember what occurred, when you received documents, which documents are outstanding, as well as your personal costs and time used. See the tips on "Maintaining your Case Log", below.

Confirm agreements and discussions. Ask the person to send you written confirmation of your discussion and any agreement or undertaking they make. If they don't do so within 24 hours, send them a note entitled "confirmation of discussion," briefly summarizing your discussion and stating that if your description is in any way incorrect, they should contact you. This way, if they do not get back to you with a correction, your document may be considered confirmation of the discussion that took place. To confirm that they receive your letter or note, use registered mail or get them to acknowledge receipt by return email.

Do not allow papers to pile up in disarray in an unsecured area where they can easily be lost or unintentionally disposed of. Find a filing system that works for you - use regular file folders, accordian-style folders, binders with pocket/sleeve pages or other tools to organize your documents.

Maintaining your Case Log

Your case log should be a chronologically-ordered and detailed journal of events, best maintained in a bound booklet or ledger-style book. Keep it in a safe place. If you choose to keep it on a computer, make sure that your security systems are kept up-to-date and make back-up copies regularly.

- Date each entry. Any notes made on Post-its or scraps of paper should be transcribed into the log, by date.

- Keep track of each person you speak to, including their contact information (title, employee number, phone and fax numbers, e-mail address) as well as the method you used to reach them.

- Log all letters, emails and phone calls that you receive and send regarding the case. Keep copies of all written correspondence in a separate folder.

- Keep your Contacts Log together with your Case Log, and update it as appropriate.

Dealing with financial institutions and other large organizations:

- Request written verification that accounts have been closed on a specific date. Always get a confirmation number.

- Send important correspondence by registered mail so as to ensure that it is received. If you send important correspondence by email, get proof of receipt such as a return email message acknowledging receipt. Keep return receipts as proof that your letter or message was received.

- Whenever possible, speak to a "fraud investigator", not a "customer service representative". Customer service representatives deal with all sorts of different customer inquiries and are not as well-placed as fraud investigators to help you. If you are dissatisfied with the responses you receive, ask to speak to a supervisor or someone with greater decision-making authority.

- When you do contact the correct person, use the following strategy:
  - After introducing yourself, get straight to the point.
  - Keep your explanations BRIEF, especially for messages.
  - Always be polite.
  - Stick to the facts and do not become defensive.
  - Have all key information (eg, account numbers, dates) on hand.

- If you are asked to provide information, confirm exactly what is being requested. Write it down and read your notes back to the person making the request. Alternatively, have them send you a written list of the information they need from you.

- If you have left a message for someone to return, allow at least one full business day for a response before calling them again.

Dealing with Debt Collectors

If you are being pursued by a debt collector for a debt that you did not incur, explain to the debt collector that you have been the victim of identity fraud and that you had nothing to do with this debt. NB: Don't say that you "dispute" the debt – creditors treat "disputed debts" as debts that you incurred but over which you have some quarrel with the creditor.

Most debt collectors require a copy of a signed police incident report with the details of the identity theft/fraud before they will accept that you did not in fact incur the debt. A copy of your completed, signed ID Crime Victim Statement/Affidavit, signed by a police officer with badge number may suffice.

Working with the police

The primary purpose of filing a police report is to establish that you have been defrauded by an identity thief, not to initiate a police investigation of the alleged crime. If the police balk at taking a formal incident report from you, explain that you need it to clear your records. It is up to the police whether or not they wish to investigate the alleged crime further.

Before you contact the police, get your facts and evidence in order. Fill out the Identity Crime Victim Statement/Affidavit (CITSC Form 1) as best you can. Include:

- institutions and numbers of accounts that have been fraudulently accessed or opened

- a list of all fraudulent transactions of which you are aware;

- names of all companies and investigators or customer service representatives you have contacted about your case; include contact information for each. Briefly summarize the substance of any conversations you have had with each company.

- copies of relevant letters, account statements, or other correspondence you have received regarding your case (*do not submit originals*).

Call the non-emergency police phone number to make an appointment with an officer to file your incident report. It's best to meet with a police officer in person so that you can provide documentation to the police and have them witness your Statement.

Whether you are filing a report by phone or in person, have all relevant information ready and be succinct: the police have large caseloads to manage and will have a limited amount of time to spend with you.

Ensure that the police officer takes down all your information and treats your complaint as a formal criminal incident report.

Ask for a copy of the incident report once it is completed and signed by the police officer. If you can't get a copy, be sure at least to get the report number. You will need to give this information to creditors, debt collectors and others.

Get the name and contact information for the police officer taking the report (or the investigator to whom it is assigned), so that you can follow up with any additional information about the crime as it comes to light.

If the crime occurred in a different province or territory, report it to the police force in that jurisdiction as well.

If the police open an investigation into your case:

• Provide the officer/investigator with copies of all relevant documentation.

• Take down the name and title of the police officer or investigator for you to contact with any additional information about the crime or to get updates on the crime investigation.

• If the crime involves another country, your local police force should report the incident either to the law enforcement in the other country or to Interpol who will forward the request for assistance or information to the relevant foreign law enforcement agency.

• You may wish to ask questions such as the following:

  • What procedures will be followed from this point forward?
  • Is there anything you can do to move things along faster?
  • When will you next be contacted by the police?
  • Will they always have the same investigator on the case?
  • What should you do if you find out more information that may help them?
  • Is there any action that you might take that would harm the case?

Your Legal Rights

Privacy laws

The personal information of Canadians (i.e., name, address and any other information associated with you) is protected by two sets of laws: one applicable to governments (e.g., the federal Privacy Act and provincial/territorial legislation typically called the *Freedom of Information and Protection of Privacy Act* or *Access to Information and Protection of Privacy Act*), and the other applicable to the private sector (e.g., the federal Personal Information *Protection and Electronic Documents Act* ("PIPEDA") and similar legislation in Alberta, B.C. and Quebec). In each case, the legislation places obligations on organizations that collect, use or disclose your personal information to protect that information from misuse, to ensure that it is accurate, and to allow you to access information about you held by the organization and have it corrected as appropriate.

Federal legislation is overseen by the Privacy Commissioner of Canada, and provincial/territorial legislation is overseen by the Information and Privacy Commissioner of that province/territory.

Your rights under these laws can be useful in cases of identity theft. In particular,

- If your personal information was stolen from an organization because of inadequate security, you can lodge a formal complaint with the Privacy Commissioner about the organization's failure to properly protect your information. The Privacy Commissioner may investigate the matter and issue a report with recommendations, or in some jurisdictions, may order the organization to take certain measures. Depending on the jurisdiction, you may be able to sue the organization for damages in court either on your own or as part of a class action if others were similarly affected.

- If an organization refuses to correct inaccurate information about you in its files, you can lodge a formal complaint with the Privacy Commissioner.

- If you need to get information from an organization about a fraudulent transaction conducted in your name, but the organization refuses to give you the information, you can try to get it by making a formal "access to information" request under the relevant privacy legislation. If the organization refuses to provide you with the requested information, you can lodge a formal complaint with the Privacy Commissioner.

To learn more about your rights under these laws, contact the Privacy Commissioner of Canada or your provincial/territorial Privacy Commissioner

Office of the Privacy Commissioner of Canada
1.800.282.1376 (toll-free)
613.992.9190 (TTY)
www.priv.gc.ca

Credit Reporting Laws

Every time you apply for credit, obtain a loan or engage in other credit-related transactions, that information is collected by one or both of Canada's national credit bureaus (also known as "consumer reporting agencies" or "CRAs"), Equifax and TransUnion. These two companies have a file on virtually every adult Canadian consumer, showing the consumer's credit history and rating their credit-worthiness. Businesses rely on this information to decide whether or not to grant credit to a consumer, or on what terms to do so. When identity criminals get credit in your name and then don't pay, your credit rating suffers and you may find yourself unable to get loans, credit cards, or other services.

Credit bureaus are governed by consumer reporting laws in every province except New Brunswick, as well as by the privacy legislation outlined above. This legislation typically requires, among other things, that credit bureaus:

- take reasonable measures to ensure that the information they hold about consumers is accurate;

- corroborate unfavourable information about you;

- allow you to dispute an alleged transaction or debt on your file, note that dispute on the file, correct records where appropriate, and notify businesses to whom your report was given of the dispute or correction;

- inform you, upon request, of the source of information in your report; and

- provide you with a copy of your credit report upon

request, free of charge (or for a nominal change) once a year.

In Ontario and Manitoba, credit bureaus must place a "Fraud Alert" on your file if you request it (they may charge a nominal fee such as $5). In other provinces and territories, credit bureaus do so voluntarily upon request. A "Fraud Alert" alerts creditors to the fact that someone may be pretending to be you when applying for credit. The creditor must then take extra precautions to ensure that the applicant is indeed you. In Ontario, credit alerts expire six years after being place on the consumer's file unless removed earlier at the request of the consumer.

Credit reporting laws also place obligations on other companies in respect of the information they provide to credit bureaus and the reports they obtain from credit bureaus. Specifically, a company obtaining an individual's credit report must notify the individual if the report results in, or plays a significant role in, the denial of a benefit or service or an increase in the cost of a benefit or service. Companies must also notify individuals if information from a source other than a credit bureau results in, or plays a significant role in, the denial of a benefit or service, or an increase in the cost of a benefit or service. In either case, individuals are entitled to be informed of the source of the information.

Debt Collection Laws

Most provinces also have legislation governing the practices of debt collectors and outlawing certain overly aggressive tactics of debt collectors. Some provinces prohibit collection agencies from continuing to attempt collection where the consumer claims that they are not the debtor or states that they would prefer for the matter to be taken to court.

Land Title Protection Laws

Some provinces, including Ontario and Alberta, have passed legislation to protect property owners from real estate or mortgage fraud. Some provinces and/or professional associations operate special funds from which victims of real estate fraud may be compensated.

Anti-Spam laws

Canada now has a federal law prohibiting deceptive email and other deceptive online practices, many of which are used by identity criminals to gather personal information. The Canadian Radio-Television and Telecommunications Commission ("CRTC") can fine violators under this law. In addition, affected individuals can apply to court for compensation of $200 per violation on top of any losses actually sustained.

Other Private Rights of Action

As noted above, some privacy laws in Canada give victims the right to apply to court for compensation from the organization or person who violated the law. The same is true of some provincial consumer protection and credit reporting laws.

Criminal Restitution

In cases that are prosecuted under the Criminal Code and that result in convictions, victims of identity theft can request that the court make a restitution order, requiring the convicted criminal to compensate the victim for losses and expenses incurred "to re-establish their identity, including expenses to replace their identity documents and to correct their credit history and credit rating". Unfortunately, many convicted criminals do not have the means to pay restitution, so victims should not rely on this right for compensation.

Victim Rights in the Criminal Prosecution Process

In the event that the offender is prosecuted, identity theft victims have the same rights as other victims of crime to information about and participation in criminal proceedings. These rights are set out in provincial and territorial victims' rights legislation, as well as in the Criminal Code. For example,

- victims are entitled to file and read a Victim Impact Statement at the time of sentencing an offender

- victims are entitled to disclosure of certain information about the offender

- the Policy Centre for Victim Issues (Justice Canada) provides funding to victims to attend Parole Board hearings involving their offenders.

Key Contacts

Credit Bureaus

Equifax Canada Inc.
P.O. Box 190
Jean Talon Station
Montreal, QC, H1S 2Z2
1.800.465.7166
www.consumer.equifax.ca

Trans Union
P.O. Box 338, LCD1
Hamilton, ON, L8L 7W2
1.800.663.9980 (8 a.m. - 8 p.m. ET)
www.transunion.ca

For Quebec residents:
Trans Union
370 – 1 Place Laval Ouest
Laval, QC, H7N 1A1
1.877.713.3393 (toll free long distance) or 514.335.0374 (local) (M-Th 8.30 a.m. - 5.00 p.m.; F 8.30 a.m. - 4.30 p.m. ET)

Credit Card Companies

Visa Canada: 1.800.847.2911 (toll-free)
Visa instructs you to contact the institution that issued your card. If you don't have the card, look on your bill statements for the phone number to call for lost/stolen cards or suspected fraud.

Mastercard1.800.622.7747 (toll-free)
1.636.722.3725 (TTY/TTD)
Mastercard requires that you contact the financial institution that issued your Mastercard. If you don't have the card, look on your bill statements for the number to call for lost/stolen cards or suspected fraud. You can also find a listing of relevant telephone numbers for each financial institution that issues Mastercards at www.mastercard.com (click on the "Personal Services" tab, then "Cardholder Services", then "Emergency Contacts", then "Lost or Stolen Emergency Help" or"Suspected Fraud Emergency Help")

American Express
North America: 1.800.869.3016
(toll-free); 1.866.529.6426 (TTY/TTD)
Toronto: 905.474.0870; 905.940.7702 (TTY/TTD)
International: 905.474.0870 (collect)
www.americanexpress.com