



# Identity Theft

## Info for Victims and Prevention Tips



Identity theft is an intrusive crime resulting in the violation of one's privacy. For many victims, identity theft can lead to devastating emotional, social and financial consequences.

Identity theft occurs when an individual steals another person's identity and impersonates that individual. By using the victim's basic personal information like name, address and social insurance number, identity thieves can open credit card accounts, lease or buy cars, rent apartments or even engage in criminal activity using the stolen name.

Identity theft can start with the loss or theft of one's wallet or identification, stolen mail, a data breach, a computer virus, or a phishing scam.

### Warning signs of Identity Theft

- You have been notified of an application for credit or the opening of an account in your name with your Social Insurance Number.
- You receive calls or letters stating that you have been approved or denied by a creditor to which you never applied.
- You receive credit card, utility or telephone statements in your name to your address which you never applied.
- You are no longer receiving credit card statements, or you notice that not all of your mail is being delivered.
- Your credit card statement includes purchases you do not recognize.
- A collection agency contacts you advising they are collecting for a defaulted account established with your identity.

### Minimizing your risk

- Sign all credit cards when you receive them and never lend them to anyone. Cancel and destroy credit cards you no longer use. Keep a list of the ones you use regularly.
- Immediately report lost or stolen credit or bank cards.
- Carry only the identification and credit cards that you actually need. Do not carry your social insurance card, leave it in a secure place. This applies also to your passport unless you need it for travel.
- Pay attention to your billing cycles and follow up with your creditors and utility companies if bills do not arrive on time.
- Review your monthly credit card statements, immediately report any discrepancies to the issuing credit card company.
- Shred or destroy paperwork no longer needed such as bank machine receipts, receipts from electronic and credit card purchases, utility bills, and any document that contains personal and/or financial information.
- Shred or destroy pre-approved credit card applications you do not want before putting them in the trash.
- Do not give personal information over the phone, through the mail, or over the Internet unless you are the one who initiated the contact.
- Know the person or organization with whom you are dealing. Before you share information, ensure that the organization is legitimate by checking its website to see if it has posted any fraud or scam alert when its name has been used improperly, or by calling its customer service number listed on your account statement or in the phone book. Review the company's privacy policy to verify how personal information will be protected.
- Password-protect credit cards, bank, and phone accounts. Keep passwords and PINs in a secure location.
- Obtain a copy of your credit report from the major credit reporting agencies at least once every year. Make sure your credit report is accurate and includes only those activities authorized.

### What to do if you Become a Victim

If you are a victim of identity theft, the following steps should be taken immediately:

- Contact your bank and/or credit card providers if you had your debit/credit card or cheques stolen. If replacement accounts or credit cards require passwords or PINs to access, do not use the same passwords or PINs as on original accounts.
- Keep copies of all documentation and correspondence exchanged with each creditor.
- Report the incident to your local police. A creditor or collection agency may want to see a copy of a police report or file number before correcting your credit account or credit report.
- Report your identity theft case to the Canadian Anti-Fraud Centre (CAFC). The CAFC works on compiling information on identity theft to identity theft trends and patterns. They, use the information to assist law enforcement agencies in possible investigations.
- Contact both of the credit reporting bureaus to have a "fraud alert" placed on your file. A fraud alert will make it harder for someone to open new accounts in your name.
  - Equifax: 1-800- 465-7166 [www.equifax.ca](http://www.equifax.ca)
  - TransUnion: 1-800-663-9980 [www.transunion.ca](http://www.transunion.ca)

### Additional Information

- Canadian Anti-Fraud Centre: [www.antifraudcentre.ca/index.shtm](http://www.antifraudcentre.ca/index.shtm)
- Competition Bureau - Fraud Prevention: [www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/h\\_00122.html](http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/h_00122.html)
- Canadian Identity Theft Support Centre: [www.idtheftsupportcentre.org/](http://www.idtheftsupportcentre.org/)