
This document, Identity Theft, is taken from the website of the Office of the Privacy Commissioner of Canada (www.privcom.gc.ca)

Identity Theft: What it is and what you can do about it

Every year, thousands of people are victims of identity theft.

While recent developments in telecommunications and computer processing make it easier for companies and consumers to reach each other, they can also scatter your personal information more widely, making life easier for criminals.

Identity theft is the unauthorized collection and use of your personal information, usually for criminal purposes.

Your name, date of birth, address, credit card, [Social Insurance Number](#) (SIN) and other personal identification numbers can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment, or accommodation, and even secure employment.

If this happens, you could be left with the bills, charges, bad cheques, and taxes.

How to fight identity theft

- Minimize the risk. Be careful about sharing personal information or letting it circulate freely.
- When you are asked to provide personal information, ask how it will be used, why it is needed, who will be sharing it and how it will be safeguarded.
- Give out no more than the minimum, and carry the least possible with you.
- Be particularly careful about your SIN; it is an important key to your identity, especially in credit reports and computer databases.
- Don't give your credit card number on the telephone, by electronic mail, or to a voice mailbox, unless you know the person with whom you're communicating or you initiated the communication yourself, and you know that the communication channel is secure.
- Take advantage of technologies that enhance your security and privacy when you use the Internet, such as digital signatures, data encryption, and "anonymizing" services.
- Pay attention to your billing cycle. If credit card or utility bills fail to arrive, contact the companies to ensure that they have not been illicitly redirected.
- Notify creditors immediately if your identification or credit cards are lost or stolen.
- Access your credit report from a credit reporting agency once a year to ensure it's accurate and doesn't include debts or activities you haven't authorized or incurred.
- Ask that your accounts require passwords before any inquiries or changes can be made, whenever possible.

- Choose difficult passwords — *not* your mother's maiden name. Memorise them, change them often. *Don't* write them down and leave them in your wallet, or some equally obvious place.
- Key in personal identification numbers privately when you use direct purchase terminals, bank machines, or telephones.
- Find out if your cardholder agreement offers protection from credit card fraud; you may be able to avoid taking on the identity thief's debts.
- Be careful what you throw out. Burn or shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc. Insist that businesses you deal with do the same.

Are you a victim of identity theft?

- Report the crime to the police *immediately*. Ask for a copy of the police report so that you can provide proof of the theft to the organizations that you will have to contact later.
- Take steps to undo the damage. Avoid "credit-repair" companies: there is usually nothing they can do, and some have been known to propose a solution — establishing credit under a new identity — that is itself fraudulent.
- Document the steps you take and the expenses you incur to clear your name and re-establish your credit.
- Cancel your credit cards and get new ones issued. Ask the creditors about accounts tampered with or opened fraudulently in your name.
- Have your credit report annotated to reflect the identity theft. Do a follow-up check three months after to ensure that someone has not tried to use your identity again.
- Close your bank accounts and open new ones. Insist on password-only access to them.
- Get new bank machine and telephone calling cards, with new passwords or personal identification numbers.
- In the case of passport theft, advise the [Passport Office](#).
- Contact [Canada Post](#) if you suspect that someone is diverting your mail.
- Advise your telephone, cable, and utilities that someone using your name could try to open new accounts fraudulently.
- Get a new driver's licence.

If you suspect that someone has been using your SIN to get a job, or that your SIN has been compromised in some other way, contact [Human Resources Development Canada](#) at:

*Social Insurance Registration
P.O. Box 7000
Bathurst, NB E2A 4T1
E-mail: sin-nas@hrdc-drhc.gc.ca*

To find out more about your privacy rights, call the Office of the Privacy Commissioner of Canada toll-free at 1-800-282-1376, or write:

*The Office of the Privacy Commissioner
112 Kent Street
Ottawa, ON K1A 1H3
E-mail: info@privcom.gc.ca*