

Identity Theft: Are You a Victim?



What is identity theft?

Identity theft occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud, theft or forgery.

What is personal information?

Any factual or subjective information recorded or not, about an identifiable individual is personal information. This includes such things as your name, address, age, gender, identification numbers, credit card numbers, income, employment, assets, liabilities, payment records, personal references and health records.

It can also include information about your purchasing preferences, family (such as mother's maiden name), interests, or attitudes.

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

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

Why should you be concerned about identity theft?

Identity thieves steal key pieces of personal information and use it to impersonate you and commit crimes in your name. If you are a victim, you could end up spending many hours trying to clear your name and may suffer emotional anguish throughout the process. In extreme cases, you could also suffer a loss of reputation, as court judgements for bad debts could be registered against you and your credit rating could tumble. This, in turn, could make it difficult for you to find employment or get access to credit when you need it.

Signs your identity might have been stolen

- A bank or credit card company contacts you about suspicious transactions
- Bills and bank or credit card statements arrive late or not at all (someone may have had your mail forwarded to another address)
- A creditor or collection agency contacts you about unknown debts
- Purchases and/or withdrawals not made by you appear on your monthly bills or bank statements
- You are denied credit for reasons that do not match your understanding of your financial position
- Your credit report shows credit issued that you didn't request
- Your property has a lien on it that you didn't know about
- Bills arrive for accounts that you do not own

How identity thieves get your personal information

- Stealing mail from your mailbox or recycling bin, or fraudulently redirecting your mail by forging your signature on a "change of address" form.
- Stealing personal and private information from lost or stolen wallets or purses, from your home, your vehicle, or your computer.
- Stealing personal information from lost or stolen personal electronic devices such as, personal digital assistants (PDAs), digital audio players, cellphones and laptops.
- Posing as a trusted official of a company or of law enforcement, in person or online, and requesting your personal information such as your credit reports or bank account password.
- Tampering with automated banking machines (ABMs) and point of sale terminals, so that your debit or credit card number and personal identification number (PIN) can be recorded.
- Taking information from within organizations, such as employees who accept bribes or who steal your personal information on behalf of others. Organizations may also unwittingly release your personal information to criminals who pose as legitimate businesses.
- Searching public sources, such as newspapers (obituaries), phone books, and records open to the public (professional certifications).
- Using "spoof" emails and fraudulent websites ("brand spoofing") to fool customers into divulging their personal and financial information in a practice known as "phishing".
- Using "spyware" to steal information from your computer.