

Identity Theft Tip Sheet

What is identity theft?

Identity theft is when someone uses your name and personal information to commit fraud or theft.

Identity thieves may try and gain access to your information by stealing identification cards from your wallet or purse or taking your mail (e.g., bank and credit card statements or pre-approved credit applications). Another method is to obtain your credit report by pretending to be a landlord or employer. Some identity thieves are able to access personal information over the Internet or by paying employees of retailers, restaurants and hotels.

How do I know if my identity is being used without my knowledge?

- You receive bills for a credit card account you never opened.
- You get turned down for a credit card, mortgage or loan because your credit report includes debts you never knew you had.
- Telephone calls or letters state that you have been approved or denied by a creditor even though you did not apply.¹
- A billing period passes and you do not receive credit card statements or other expected mail.

What should I do if I think an identity theft has occurred?

- Take immediate action. Contact other companies or agencies that may have accounts in your name. For example, credit card companies, telephone companies, banks and other lenders.
- Contact the fraud departments of each of the two major credit bureaus and request that a 'Fraud Alert' be placed on your file:
 - Equifax: 1-800-465-716
 - TransUnion: 1-877-525-3823
- Once notified, these two agencies can provide you with copies of your credit reports
- File a report with your local police or the police in the community where the identity theft took place.
- Start a log of dates, person(s) contacted and what was said.

- Call Phonebusters National Call Centre at 1-888-495-8501. Phonebusters provides support and information to victims of identity theft. The information you provide can be used to identify trends and patterns that assist law enforcement agencies with possible investigations.

How can I protect myself?

- Before revealing personal information, find out how it will be used and whether it will be shared with others.
- Note billing cycles and follow-up if bills are not received on time.
- Be careful with your mail. Remove mail promptly from your mailbox and ensure that all mail is correctly forwarded and re-routed if you move or change your address. Only deposit letters in post collection boxes.
- Cut down on the number of cards you carry. Only carry your Social Insurance Number (SIN) when necessary.
- Only give out your personal information by phone, mail or e-mail if you initiated contact and are confident of the source.
- Shred or tear up receipts, credit card information, credit applications and related items before throwing them out. Cut up expired credit cards.
- Avoid tossing credit card receipts in public trash containers.
- Only give out your SIN when absolutely necessary and use other types of identification when possible.
- Avoid easily identifiable Personal Identification Numbers (PIN) such as mother's maiden name, birth date or telephone number.
- Memorize your PIN – **do not** write this number on your bank card or keep it on a piece of paper in your wallet or purse. Be aware of onlookers or video equipment that may be monitoring you when entering your PIN.
- Never leave your purse or wallet unattended.
- Do not let your credit card out of sight (e.g., when paying a restaurant bill).
- Check your credit rating at least once a year.

¹TransUnion Canada Website – www.tuc.ca/TUCorp/consumer/personalsolutions.htm