

Identity Theft: Could it happen to me?

Identity Theft is a growing crime in Canada as a result of technological advancements – especially over the last decade. Once thought to be found only in Hollywood movies, identity theft has become a serious problem for consumers and businesses alike.

Identity theft is the act of stealing or misrepresenting the identity of another individual or business. Once a new identity has been acquired it will provide the criminal with an effective means to commit other crimes.

Financial Fraud is the most common form of identity theft. This is an act where funds are stolen and used to fund a criminal activity. This can occur through banking transactions, fraudulent credit card purchases, tax refunds or mail fraud.

Personation is when a criminal takes on another identity to commit a crime, enter a country, obtain special permits, hide their own identity or commit other illegal acts.

How does it happen?

Tombstoning: Criminals will obtain names and dates of birth of deceased people from tombstones. In many cases the tombstone will also include a valuable piece of information – the names of the parents. This information can be used to create a new identity.

Stealing wallets and purses: Criminals can make use of personal identification including:

- Name, address, telephone number
- Birth certificate / Passport / Medical Health Card
- Mother's Maiden Name
- Social Insurance Number
- Driver's license number
- Bank and Credit cards and/or number
- Personal Identification Number (PIN)

Mail Theft: Criminals can pick up your mail before you retrieve it. "Pre-approved" credit applications are taken and filled out on your behalf.

ATM/Debit Card Use: ATM's can be fitted with "skimmers" which copy your card data and record your PIN for the criminals to use. The data is copied and transferred to the "real" ATM so the client isn't aware of the skimming. Clerks can also "double skim" your card and sell or use the data themselves. "Shoulder surfing" occurs when a person lurking around the machine looks over your shoulder and views you entering your PIN number.

Credit card receipts: Credit card receipts contain your card number and your signature on them. An identity thief can use this data. Protect this information.

Dumpster diving: Your trash can contain your name, address, date of birth, signature, etc and can be used to complete financial transactions in your name.

How can I protect myself?

It would be next to impossible to completely prevent the chance of identify theft happening to you. However you can significantly reduce your risk. Manage your personal information cautiously and be aware that identify theft exists.

Identification:

- Do not carry all of your identification. Bring only what you need for the purpose of your trip. Never keep your SIN, bank PIN's or passwords in your wallet or purse.
- When you change homes alert Canada Post, all your credit card companies, and other business and government agencies of your new address immediately. Ensure your bills are being properly redirected to your new address. Verify the changes have been completed.
- Shred unwanted mail, in particular credit card offers.

- If you have had your purse or wallet stolen - report it to police immediately. File a police report by calling 986-6222 or attending a police station.

Credit and Debit Cards:

- Do not use an ATM that looks unfamiliar or suspicious to you. Notify staff immediately of faulty or defective ATMs. NEVER write down your PIN. Ensure the keypad is protected from the view of others when you are using your card. Be aware of people lurking around the machine when you are entering your PIN. This is known as "shoulder surfing." NEVER accept help from someone in the vicinity if the machine appears to be broken. Contact your bank immediately if this occurs.
- When making online purchases, use a separate credit card with a small limit.
- Cancel credit cards that you do not use regularly.
- Immediately report lost/stolen credit cards and discrepancies in statements to credit card company
- Shred pre-approved credit card applications, credit card receipts, and bills
- NEVER write down your bank PIN number(s), social insurance number and computer passwords.
- If you lose a credit card, bankbook or bankcard, report it to the bank as soon as possible. Most banks will have a "1-800" number that operates around the clock. Keep this number somewhere safe, separate from your wallet/purse.

Personal Information:

- When asked for personal information, only provide the minimum amount. Never provide information such as SIN, date of birth, credit card numbers, over the phone unless you have initiated the call
- Do not leave or discard receipts at bank machines, in trashcans, or at gasoline pumps.
- Pick up your mail regularly to minimize the chance of someone stealing a pre-approved credit card offer, tax form, etc. Have someone pick up your mail daily when you cannot.
- Avoid solicitations disguised as promotions or surveys that offer prizes or awards designed to gain your personal information.
- Pay attention to your billing cycles. If your statements or bills do not arrive on time, contact the senders to ensure they have not been illicitly redirected.
- Review your credit report annually to ensure it is accurate and doesn't include debts or activities you haven't authorized.
- 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. Memorize them, change them often. *Don't* write them down and leave them in your wallet, or some equally obvious place.
- If you are denied credit, find out why.
- Never give out your PIN to anyone for any reason. No legitimate person or business will EVER ask you for your PIN.

How do I know if I am a victim?

Typical indicators that your identity has been stolen include:

- You are informed that a credit application was received which you did not apply for.
- Correspondence stating that you have been approved/denied credit you did not apply for.
- Reception of credit card statements or bills in your name, which you did not apply for.
- You are missing credit card statements or it seems you are missing mail.
- A collection agency contacts you to collect on an account you haven't opened.

What should I do if I am a victim?

- Immediately notify the following Canadian credit rating agencies. They will "flag" your account for further suspicious activity. Request that a "Fraud Alert" be placed in your files and order copies of your credit reports. Have the report annotated to identify the theft.

Equifax Canada: 1.877.323.2598
Trans Union: 1.800.663.9980

Keep a record of your conversations and correspondence with anyone you deal with in the coming months regarding your situation. Perform the following actions:

- Do not use "credit-repair" companies. It is unlikely they can help. Establishing credit under a new identity is NOT the solution.
- Contact the Winnipeg Police Service at 986-6222 and file a report. If you are not a Winnipeg resident, file a report with the Police in your community. Ask for a copy of the police report to provide proof of the theft to the organizations that you will be contacting.
- Start a log of dates and person(s) that you spoke with and what they said.
- Close any accounts that you know or believe have been tampered with or opened fraudulently.
- Replace ALL of your identification and advise the organizations as to the reason.
- Contact the fraud department of creditors for any accounts that have been opened or tampered with. This may include credit card companies, phone companies, banks or other lenders.
- Contact PhoneBusters National Call Centre. PhoneBusters manages information on these types of crimes to identity trends and patterns. The information is also used to assist law enforcement agencies in investigations.

Toll Free: 1-888-495-8501
Email: info@phonebusters.com

- Follow-up with the credit agencies three months later to ensure that someone has not tried to use your identity again.
- Contact Canada Post if you suspect that someone is diverting your mail.

Winnipeg Central P.O.
266 Graham Ave.
Winnipeg, MB R3C 0K0
Phone: 1-800-267-1177

- If your passport has been compromised, contact the Passport office:

Passport Canada
Foreign Affairs and International Trade Canada
Gatineau, QC, Canada
K1A 0G3
Toll free: 1 800 567-6868
Outside Canada and the United States: (819) 997-8338
TTY services: 1 866 255-7655

- Advise your telephone, cable, and utilities that someone using your name could try to open new accounts fraudulently.
- 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

Thank you to Mike Shaver, Information Systems Manager for Sport Manitoba for providing us with this valuable information. Should you have further questions on this topic, please feel free to contact Mike at shaver@sport.mb.ca

Publication of the PSO Unit

Contacts: Janet McMahon mcmahon@sport.mb.ca Fred Schneider schneider@sport.mb.ca
Brenda Wiwcharyk wiwchar@sport.mb.ca Kristin Albo albo@sport.mb.ca

For further information, please contact a member of the PSO Unit.