



## protect yourself from fraud

the WISE network

Your risk of becoming a victim of fraud is not linked to your age, race, income or geographic location. One in six Canadians have reported being a victim of identity theft. Over 4.2 million people in Canada have had some type of identity theft crime committed against them. Research that has been done by the Canadian Anti-Fraud Centre shows that Canadians between the ages of 50 and 59 are the most targeted, with Ontario being the most-targeted province. Canadians between the ages of 40 and 49 reported the highest dollar loss. Victims spend a minimum of \$1,000 in out-of-pocket expenses and hundreds of hours resolving the numerous problems caused by the identity thieves. Desirable victims are more likely to be educated, relatively affluent and actively involved in their community.

Identity theft occurs when an imposter uses your name or personal information such as a driver's license, date of birth, or social insurance number to obtain a job, housing, money, goods or other services.

Having your personal identity stolen can have a devastating impact on your entire life; destroying your credit rating and your reputation, and it can take months or even years to repair the damage. Staying informed and taking preventative measures is key to reducing your risk of becoming a victim. Today's criminals and scam artists are very sophisticated and well organized with the latest trends and techniques to steal your money.

### THERE ARE THREE MAIN REASONS IDENTITY THIEVES STEAL YOUR PERSONAL INFORMATION:

- 1. Personal Financial Gain** – The number one reason identity thieves steal your identity is for personal financial gain. Identity thieves will use your personal information to obtain money, goods or services, leaving you with the bill. They can purchase real estate, use credit cards and even go on vacation for you. The two major credit bureaus in Canada receive 1,400 to 1,800 complaints a month, mainly in Ontario. Should this happen to you, it's your responsibility to correct the situation.
- 2. To Secure Employment** – In Canada there are tens of thousands of people working illegally, especially in Ontario because we are so diverse. Most illegals are working under the table or working under a false name and social insurance number. On the streets a social insurance number sells for minimum of \$100, and passports can go for as low as \$300 and as high as \$2,000. Most people do not become aware that someone is using their social insurance number until they file their income tax and are required to pay additional taxes because their supposed "second job" has placed them in a higher tax bracket. Should this happen to you, the onus is on you to correct the problem not the government.
- 3. To obtain Medical Treatment** – Identity thieves will also use your personal information to obtain prescriptions or a medical procedure in your name. Again, it goes back to illegals not having medical insurance. When you're visiting an emergency department in a hospital, do not throw your hospital armband in the garbage; it has your name, your doctor's name and sometimes other personal information. Identity thieves go through the garbage for this valuable information, making hospitals very popular sites for dumpster diving.

### SMARTSTEPS TO PROTECT YOU FROM BECOMING A VICTIM:

- The prime information targeted by today's criminals is your Social Insurance Number, birth certificate, passport, health card and driver's license. Leave your SIN, birth certificate, passport and health card at home in a locked drawer and only carry it when needed. In the event your wallet is lost or stolen, save valuable time and money by keeping a photocopy of everything you keep in your wallet at home in a locked drawer. Keep financial records, cheques, investment statements and credit/debit card information in a locked drawer. Your paystub has a wealth of information on it; do not leave it out on your desk at work. 50% of criminals convicted of identity theft stole the personal information from the victim's home or office. Lost and stolen wallets account for 30% of all identity theft cases.

- Credit card fraud is the most common form of identity theft. When paying for a purchase or a meal with a credit card, always check that your name appears on the credit card when it is returned to you with your receipt. Another popular method used by waiters in restaurants is to use the camera on their cell phone to take a picture of the front and back of your credit card and then sell the picture.
- Criminals will break into your car or gym locker, leaving your wallet behind fully intact. What you don't know is that they have switched your credit cards, buying themselves valuable purchasing time. Consider asking your credit card company to issue two credit cards with two different limits. Keep the card with the smaller limit in your wallet for everyday or online purchases and the card with the larger limit at home locked up for vacation or big ticket items.
- Limit the number of ATM/debit cards you keep in your wallet. Each financial institution sets a daily withdrawal limit for ATMs and Point of Sale terminals (Interac). Inquire as to your daily limits and consider lowering the withdrawal limit on your ATM and Interac debit card if needed. Always use your hand to cover the keypad when entering your PIN (even when you are alone) at ATMs and Interac machines; criminals use special equipment to capture your PIN and duplicate your card. In the event your card has been captured by an ATM at home or while on vacation, contact your financial institution immediately.
- Social network websites – While most adults are careful about the information they post on sites like Facebook, MySpace and LinkedIn, some people unknowingly have put themselves at risk of identity theft. Think twice when you post personal information such as your birthday, your employer, job title and your address. For today's criminals having this information at their finger tips makes it so much easier when taking out a loan, or applying for a credit card or services in your name.
- Buy a mailbox with a lock, the cost is about \$150 for a good quality one. Stealing mail from your mailbox is the number one method used by thieves with a preference for bank statements and income tax returns. While on vacation have a neighbor pick up your mail. If you notice missing statements, contact Canada Post to ensure your mail is not being redirected.
- Check all bank and credit card statements and immediately report any irregularity.
- Identity thieves use numerous phoney telephone techniques to obtain your personal information, pretending to be utility companies or other service providers. If you did not initiate the call, do not give out any personal or credit card information over the telephone. Be on alert for companies that offer to repair or fix your computer remotely. What they're really doing is downloading software to capture sensitive data such as your banking and password information. Scam artists will manipulate the call display on your telephone to trick you into thinking the company is legitimate. You have the right to check out any caller by requesting written information, a call back number, and time to think over an offer.
- Fake sweepstakes, online or telephone surveys are another method used by criminals to obtain personal information about you and your family. Criminals offer great fake prizes to lure you into doing their survey(s) and will have you do several surveys over several months to capture information so that you will not become suspicious. Do not give out your banking information for identity thieves to deposit your "winnings". Working in your home is one of the best ways for identity thieves to gain access to your personal information. If you have contractors or other workers in your home, don't leave out personal information, statements or bills. The same precautions should be taken if you have people coming in to help look after your elderly parents.
- Keep your passwords, access codes and PINs confidential. Do not store passwords on your computer, especially online banking/ investment passwords. Choose complicated passwords, combining letters and numbers.
- If you need to obtain your banking information while on holidays, it is safer to use a telephone (landline) than a public computer due to tracking software that criminals place on public computers to steal your passwords and personal information. .

- Safety precautions should be adhered to when using a wireless connection; update your anti-virus and anti-spyware programs regularly with your service provider. Think twice about downloading FREE anti-virus and anti-spyware programs, criminals use this method as the perfect platform to obtain your passwords, personal information and hijack your computer without your knowledge. Financial institutions may not cover the cost of your losses if you are found negligent in protecting your banking or investment passwords
- If you receive an e-mail (phishing scam) requesting your personal information or that prompts you to click a link and enter your personal information, call the company instead, even if the website looks legitimate.
- If you receive an e-mail greeting card do not open it; scammers use this method to transfer viruses and infect your computer.
- If you receive a call from your financial institution or credit card company about a problem with your payment, to respond only use the telephone number on your financial statement or on the back of your credit card. Today's criminals are hoping you'll call them back on the telephone number they have provided you, and thereby, you're using their automated system to enter your PIN and credit or bank account card number.
- A shredder is an essential tool in preventing fraud – shred all documents, bills and promotional offers with your name on it.

#### Checklist In the event of a lost or stolen wallet

Despite all the efforts you take to protect yourself from becoming a victim of fraud, it can still happen. If it does happen to you, the following contact information will save you time. Cut and paste this to the back of your telephone book in the event your wallet is lost or stolen. Include a copy of this list with your vacation itinerary:





the WISE network

COMPANY	PHONE # & WEBSITE	CALL DATE	NAME OF PERSON/FILE	FOLLOW-UP
Comtech Credit Union	1-800-209-7444 www.comtechcu.com			
Lost or Stolen Comtech ATM/Debit card	416-614-4466 www.comtechcu.com			
Lost or Stolen Comtech MasterCard	1-800-387-1949 www.mastercard.ca			
File a Police Report				
Contact Equifax Credit Bureau and ask to be contacted if someone does an inquiry on your account	1-800-465-7166 www.equifax.ca			
Contact Trans Union Credit Bureau and ask to be contacted if someone does an inquiry on your account	1-877-525-3823 www.tuc.ca			
Ontario Drivers License www.mto.gov.on.ca	1-800-387-3445			
Ministry Health Card www.gov.on.ca	1-800-268-1154			
Government Birth Certificate	1-800-461-2156 www.cbs.gov.on.ca			
Old Age Security	1-800-277-9914 www.cbs.gov.on.ca			
Phone Busters	1-888-495-8501 www.phonebusters.com			
RCMP	519-640-7267 www.rcmp.ca			
Better Business Bureau	1-800-459-8875 www.bbbmwo.ca			
Contact other banking services providers				
Contact department store card issuers				
Contact other credit card issuers				
Canada Post	1-800-267-1177 www.canadapost.ca			