



Protect Your Personal Information

Tips and tools to help
safeguard you against identity theft



WHAT IS IDENTITY THEFT?

Recent developments in telecommunications and computer processing have made it easier for companies and consumers to reach one another. However, these developments can also make your personal information more widely accessible, not only to legitimate companies, but also to fraudsters.

Identity thieves do not need a lot of information to carry out criminal activity. Your name, date of birth, address, credit card number, Social Insurance Number (SIN), and other personal identification numbers can be used by thieves to assume your identity. Once an identity thief has assumed your identity they could conduct numerous activities under your name including:

- Opening new bank accounts and writing bad cheques;
- Establishing new credit card accounts and defaulting on bill payments;
- Obtaining mortgages, personal loans or car loans;
- Getting cash advances;
- Establishing a cellular phone or utility service and running up bills;
- Changing your credit card mailing address, obtaining supplementary credit cards on your accounts and charging purchases on your existing accounts;
- Obtaining employment; and
- Renting an apartment.

If this happens, you could be left with the bills, charges, bad cheques, and taxes. More importantly, since bills are often sent to a different address, victims of identity theft are often not aware that debt is mounting in their name until a collection department tracks them down. As a result, it can take months before the victim is aware of any wrongdoing, and once they realize they have been a victim of identity theft, it can take months to correct the damage.

HOW SERIOUS IS THE IDENTITY THEFT PROBLEM?

Identity theft has become one of the fastest growing crimes in Canada. In 2004, PhoneBusters National Call Centre, the national call centre dedicated to the prevention of deceptive telemarketing, received 11,001 identity theft complaints by Canadians, amounting to more than \$18.3 million in fraud losses. PhoneBusters is

operated by the Ontario Provincial Police in conjunction with the Royal Canadian Mounted Police (RCMP) and the Canadian Competition Bureau.

From a global Visa perspective, identity theft has not increased significantly in Canada and represents a small portion of our overall fraud. However, with the growing complexity of identity theft crimes, victims face more challenges when it comes to clearing up the issues associated with identity theft. As a result, it is important that Canadians take greater precaution in protecting their personal information.

HOW DO CRIMINALS STEAL AN IDENTITY?

Here are just a few examples of how identity theft is committed:

- 1. "Dumpster Diving"** - Thieves rummage through trash cans, or garbage dumpsters, searching for pieces of unshredded personal information that they can use to assume your identity, or to sell to others.
- 2. Mail Theft** - Fraudsters seek out unattended or unlocked mailboxes to steal newly issued credit cards, bank statements, and tax forms. Letters that contain "pre-approved credit card" offers, if not shredded or destroyed, can be sent back to the issuing bank requesting that the card be re-sent to the recipient (i.e. you), but at a new address of the identity thief's choosing.
- 3. Inside Sources** - A dishonest employee with access to personal records, payroll information, insurance files, account numbers and/or sales records can cause a great deal of damage to your personal finances.
- 4. Imposters** - Many identity theft victims have been taken in by an individual who fraudulently posed as someone who had a legitimate reason to access the victim's personal information (e.g., landlord asking for background information, an employer, etc.).
- 5. Online Data** - On the simplest level, thieves access public databases that consumers share through phone listings, directories, memberships, etc.
- 6. "Phishing"** - More sophisticated criminals, who want to get data from people online, use a technique known as phishing. This involves creating e-mails and Web sites that appear to belong to legitimate businesses, such as financial institutions or auction sites. Consumers who receive e-mails claiming to be from a legitimate business are often directed to a Web site, appearing to be from that business. Once on this fraudulent site, consumers are directed to enter personal data.

Identity theft has become one of the fastest growing crimes in Canada. In 2004, PhoneBusters National Call Centre, the national call centre dedicated to the prevention of deceptive telemarketing, received 11,001 identity theft complaints by Canadians, amounting to more than \$18.3 million in fraud losses.

Criminals who create these e-mails and Web sites have no connection whatsoever with these businesses, and their sole purpose is to get consumers' personal data to engage in fraudulent activity. For more information on phishing, refer to "Cut the Line on Phishing Scams," a brochure provided by Visa, and available at: www.visa.ca/securewithvisa.

7. Direct Access to Personal Documents in the Home

- Unfortunately, there are identity thieves who can gain legitimate access into someone's home and personal information through household work, babysitting, healthcare, friends, or roommates.

8. Purse/Wallet Theft - Stolen purses and wallets usually contain bank cards and personal identification. A thief could use this information to obtain credit under the victim's name or sell the information to criminal groups.

9. Hacking - Some criminals have the ability to break into computer databases at e-commerce merchants, credit card processors, or payment gateway service providers to gather personal information which they can then use to assume someone's identity.

WHAT CAN I DO TO GUARD AGAINST IDENTITY THEFT?

There are measures you can take to protect your personal information and minimize the risk of falling victim to identity theft:

Do...

- Sign all your credit cards as soon as you receive them, and never lend them to anyone.
- Shred all personal and financial information (e.g., bank statements, credit/ATM receipts, credit card offers, credit card bills, etc.) before you recycle them.
- Be careful about sharing or disclosing your personal information. Do not give personal information out over the phone, through the mail, or over the Internet unless you are the one who initiated the contact, and know the person or organization with whom you are dealing.
- Before you share any personal information, find out how it will be used and if it will be shared.
- Pay attention to billing cycles, or to a lack of mail being delivered to your address, it is possible the mail is being intercepted by a fraudster.
- Carefully check each of your monthly credit card and bank statements and look for unauthorized purchases and withdrawals.

- Use technologies, such as digital signatures, data encryption, and passwords through programs like *Verified by the Visa*® service to give you added security and privacy protection when you use the Internet.
- Minimize the amount of identification and credit cards that you carry.
- Report lost or stolen cards immediately. To report a lost or stolen *Visa* card, call 1-800-847-2911.
- Cancel all inactive credit card accounts. Even though you do not use them, those accounts could be used by thieves.
- Guard your mail. Deposit outgoing mail in post office collection boxes or at your local post office.
- Choose difficult passwords. Avoid using ones that may be easy to figure out such as your mother's maiden name, your birth date, or telephone number.
- Review your credit bureau report annually and immediately question any unknown credit inquiries or unauthorized accounts.
- Be aware of others nearby when entering your Personal Identification Number (PIN) at an ATM and shield the PIN entry with your body or your free hand.

WHAT IS VERIFIED BY VISA?

The *Verified by Visa* (VbV) service is an online authentication technology designed to verify a cardholder's identity during an online transaction. The *Verified by Visa* service verifies your identity through your use of a password that only you know, preventing thieves from using your *Visa* card online. To sign up for VbV, visit www.visa.ca/verified.

Don't...

- Lend your credit cards to anyone, ever.
- Record or keep an ATM card PIN, password, or SIN in your wallet.
- Volunteer any personal information when you use your credit card.
- Give any personal information such as birth date or credit card information over the phone, through the mail, or over the Internet, unless you have initiated the call and know that the business you are dealing with is reputable.



- Give out your SIN, or any bank account details, unless you are dealing with the government, your employer, or your bank directly, and you initiated the contact. Your employer will need your SIN for income tax reporting purposes, and your bank account number for payroll purposes.
- Leave your mail unattended.
- Leave your receipts at ATMs, bank counters, or unattended gasoline pumps.
- Leave your purse or wallet unattended at work, restaurants, health clubs, in a shopping cart, or at social gatherings.

What Are Some of the Signs That Your Identity May Have Been Stolen?

- Bills and statements do not arrive when they are supposed to because they may have been stolen from the mailbox, or someone has redirected your mail to another mailing address.
- You receive calls from collection agencies or creditors for an account you don't have or one that is up to date:
- Financial account statements show withdrawals or transfers you didn't make.
- A creditor informs you that you've been approved or denied credit that you haven't applied for. Or, you get credit card statements for accounts you don't have.
- You apply for credit and are turned down, for reasons that do not match your understanding of your financial position.

AM I LIABLE FOR UNAUTHORIZED VISA® CARD CHARGES MADE UNDER MY NAME?

Under the Visa Cardholder Zero Liability Program, you will not be liable for unauthorized use of your card if your card is lost, stolen, or if your card number is used fraudulently*.

*Visa cardholder must establish, to the satisfaction of the financial institution, that the transaction is not the responsibility of the cardholder in accordance with the financial institution's cardholder agreement. Zero Liability does not apply to PIN-initiated transactions (e.g. ATM transactions) or commercial cards.

WHAT SHOULD I DO IF I BECOME A VICTIM OF IDENTITY THEFT?

1. File a report with the police immediately:

- Ask for a copy of the police report so that you can provide the evidence to the various companies you have to contact.

2. Report your identity theft case immediately to the appropriate government organizations listed below.

- PhoneBusters National Call Centre at 1-888-495-8501. PhoneBusters has a mandate to gather information and intelligence about identity theft, and will provide advice and assistance to identity theft victims.
- 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

- If you suspect that someone has been diverting your mail, contact Canada Post at www.canadapost.ca or by telephone at 1 800-267-1177.
- In the case of passport theft, advise the passport office at <http://www.ppt.gc.ca> or by telephone at 1 800-567-6868.
- Advise the Ministry of Transportation in your province (Driver's License, Vehicle License).
- Advise the RCMP of your situation by reporting the crime online through RECOL – Report Economic Crime Online (www.recol.ca)

3. Fill out the Identity Theft Statement.

- The Identity Theft Statement is a form developed by the federal government that you can use to notify financial institutions, credit card issuers and other companies that you have been a victim of identity theft. This statement gives them information they need to begin an investigation of the incident.
- You can get a copy of the Identity Theft Statement at www.consumerinformation.ca.

4. Contact all creditors that you deal with, to review your financial information.

- Describe your identity theft problem and follow up with a letter or affidavit, as required.
- Creditors that should be contacted include: credit card issuers, phone companies, cable companies, utilities, banks, and other lenders.

5. Cancel your credit cards and get new ones issued:

- Ask creditors about accounts that have been tampered with, or opened fraudulently in your name. Work with your financial institution to get fraudulent accounts cancelled immediately.

6. Close your bank accounts, open new ones, obtain a new bank card and change your bank card PIN.

7. Contact the two national credit bureaus to:

- Report identity theft and request a “fraud alert.” This ensures that you will be contacted before any new account is opened and/or an existing account is changed.
- Request copies of your credit report. Review the report carefully and identify any new accounts that may have been opened. Pay particular attention to the section of the report that lists “inquiries” from new companies that you do not recognize. Contact these companies immediately and have them remove any pending or new accounts from the system.

Equifax Canada

(800) 465-7166

Web: www.equifax.com/EFX_Canada

Trans Union Canada

(877) 525-0262

Web: www.tuc.ca/TUCorp/consumer/personalsolutions.htm

8. Chart your course of action

Use this form to record the steps you've taken to report the fraudulent use of your identity. Keep this list in a safe place for reference.

Banks, Credit Card Issuers and Other Companies

Company	Phone Number	Date Contacted	Contact Person
Visa	1-800-847-2911		

Comments:

Company	Phone Number	Date Contacted	Contact Person

Comments:

Company	Phone Number	Date Contacted	Contact Person

Comments:

Company	Phone Number	Date Contacted	Contact Person

Comments:



Credit Reporting Agencies

Company	Phone Number	Date Contacted	Contact Person
Equifax Canada	1-800-465-7166		

Comments:

Company	Phone Number	Date Contacted	Contact Person
Trans Union Canada	1-800-525-0262 Quebec residents: 1-877-713-3393		

Comments:

Company	Phone Number	Date Contacted	Contact Person

Comments:

Company	Phone Number	Date Contacted	Contact Person

Comments:

Law Enforcement

Company	Phone Number	Date Contacted	Contact Person
---------	--------------	----------------	----------------

Local Police			
--------------	--	--	--

Comments:

Company	Phone Number	Date Contacted	Contact Person
---------	--------------	----------------	----------------

Phone Busters	1-888-495-8501		
---------------	----------------	--	--

Comments:

Company	Phone Number	Date Contacted	Contact Person
---------	--------------	----------------	----------------

--	--	--	--

Comments:

For Further information on Identity Theft and how you can protect your personal information, visit:

- Phonebusters: www.phonebusters.com
- Privacy Commissioner of Canada: www.privcom.gc.ca
- Consumer Measures Committee: www.cmcweb.ca
- Visa Canada: www.visa.ca/securewithvisa
- Canadian Consumer Information Gateway:
www.consumerinformation.ca
- Royal Canadian Mounted Police: www.rcmp.gc.ca
- Ontario Provincial Police: www.opp.ca
- Competition Bureau: www.cb-bc.gc.ca



TM Trademark of Visa International Service Association;
Visa Canada Association is a licensed user.

[®] Registered trademark of Visa International; Visa Canada is a licensed user.