



Solicitor General Solliciteur général
Canada Canada

U.S. Department
of Justice



Public Advisory: Special Report for Consumers on IDENTITY THEFT

Summary

The United States Department of Justice and the Department of the Solicitor General of Canada are jointly issuing a Special Report to advise the public on current trends and developments in Identity Theft.

Identity theft refers to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. United States and Canadian law enforcement agencies are seeing a growing trend in both countries towards greater use of identity theft as a means of furthering or facilitating other types of crime, from fraud to organized crime to terrorism. This Public Advisory will highlight some of the most significant forms of identity theft in Canada and the United States, and explain how to recognize them and respond if you become a victim of identity theft.

Facts

Identity theft has become one of the fastest-growing crimes in the United States and Canada. In the United States, identity theft complaints to the Federal Trade Commission have increased five-fold in the last three years, from 31,117 in 2000 to 161,819 in 2002. In Canada, the PhoneBusters National Call Centre received 7,629 identity theft complaints by Canadians in 2002, that reported total losses of more than \$8.5 million, and an additional 2,250 complaints in the first quarter of 2003 that reported total losses of more than \$5.3 million. In addition, two major Canadian credit bureaus, Equifax and Trans Union, indicate that they receive approximately 1,400 to 1,800 Canadian identity theft complaints per month, the majority of which are from the province of Ontario.

One reason for the increase in identity theft may be that consumers often become victims of identity theft without having any direct contact with the identity thieves who acquire their personal data. Simply by doing things that are part of everyday routine – charging dinner at a restaurant, using payment cards to purchase gasoline or rent a car, or submitting personal information to employers and various

levels of government – consumers may be leaving or exposing their personal data where identity thieves can access and use it without the consumers' knowledge or permission.

How Identity Theft Occurs

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

- *Theft of Payment Cards and Documents*
Identity thieves often steal purses or wallets, and steal newly issued cards or credit-card applications from your residential mailbox. Some, known as “dumpster divers,” will even rummage through trash to pick out bank and credit card statements. 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 sent to the recipient (i.e., you), but at a new address of the identity thief's choosing
- *“Shoulder Surfing”*
Some identity thieves also engage in “shoulder surfing”: looking over your shoulder or from a nearby location as you enter your Personal Identification Number (PIN) at an ATM machine. By installing a fake ATM device that reads your card's encoded data, or by distracting you while your card is taken or switched with another, an identity thief can then use your PIN to drain your bank account without your knowledge.
- *“Skimming”*
Identity thieves also “skim” or “swipe” customer credit cards at restaurants or cash stations, using an electronic device known as a skimmer. The skimmer records the personal information data from the magnetic stripes on the backs of the cards. Identity thieves then transfer or transmit those data to another location, sometimes overseas, where it is re-encoded onto fraudulently made credit cards.
- *E-Mail and Website “Spoofing”*
Many criminals who want to obtain personal data from people online use a technique known as “spoofing”: the creation of e-mails and websites that appear to belong to legitimate businesses, such as financial institutions or online auction sites. Consumers who receive e-mails claiming to be from a legitimate business are often directed to a website, appearing to be from that business, at which the consumers are directed to enter large amounts of personal data. In fact, the criminals who created these e-mails and websites have no real connection with those businesses. Their sole purpose is to obtain the consumers' personal data to engage in various fraud schemes.
- *Theft from Company or Government Databases*
Law enforcement agencies in both Canada and the United States have noticed a

significant increase in efforts by identity thieves to access large databases of personal information that private companies and government agencies maintain. Criminals have broken into offices to steal computer hard drives, bribed or compromised employees into obtaining personal data for them, and hacked into databases.

What You Can Do Today to Minimize Your Risk of Identity Theft

- Sign all credit cards when you receive them and never lend them to anyone.
- Cancel and destroy credit cards you do not use and keep a list of the ones you use regularly.
- Carry only the identification information and credit cards that you actually need. Do not carry your social insurance card (Canada) or social security card (United States); leave it in a secure place. This applies also to your passport unless you need it for traveling out of country.
- Pay attention to your billing cycles and follow up with your creditors and utility companies if your bills do not arrive on time.
- Carefully check each of your monthly credit-card statements. Immediately report lost or stolen credit cards and any discrepancies in your monthly statements to the issuing credit card company.
- Shred or destroy paperwork you no longer need, such as bank machine receipts, receipts from electronic and credit card purchases, utility bills, and any document that contains personal and/or financial information. Shred or destroy pre-approved credit card applications you do not want before putting them in the trash.
- Secure personal information in your home or office so that it is not readily accessible to others, who may have access to the premises.
- 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 such information, ensure that the organization is legitimate by checking its website to see if it has posted any fraud or scam alert when its name has been used improperly, or by calling its customer service number listed on your account statement or in the phone book.
- Password-protect your credit card, bank, and phone accounts, but do not keep a written record of your PIN number, social insurance or social security number, or computer passwords where an identity thief can easily find them. Do not carry such information in your purse or wallet.
- Order a copy of your credit report from the major credit reporting agencies at least once every year. Check with the credit bureaus to see whether there is a

charge for this service. Make sure your credit report is accurate and includes only those activities that you have authorized.

If You Are A Victim

The United States Department of Justice and the Department of the Solicitor General advise that if you have become a victim of identity theft, you should take three immediate steps. First, contact your bank or credit card company if you have had your checks or credit cards stolen or wrongfully obtained. Second, report the matter to your local police of jurisdiction. Police authorities often will take police reports even if the crime ultimately may be investigated by another law enforcement agency. In addition, a creditor who mistakenly believes that you are the person responsible for a fraudulent transaction may want to see a copy of a police report before correcting your credit account or credit report. Third, report your identity theft case immediately to the appropriate government and private-sector organizations listed below. Canadian and American agencies such as these are compiling information on identity theft to identify theft trends and patterns, and using the information to assist law enforcement agencies in possible investigations.

Resources for American Victims of Identity Theft

Federal Trade Commission Identity Theft Hotline

Toll free: (877) IDTHEFT (438-4338)

Web: www.consumer.gov/idtheft

Credit Reporting Agencies: Place fraud alerts on your credit reports by contacting the credit bureaus that operate in the United States.

Equifax

Report fraud: (800) 525-6285

Web: www.equifax.com

Experian

Report fraud: (888)-EXPERIAN (397-3742)

Web: www.experian.com

TransUnion

Report fraud: (800) 916-8800

Web: www.transunion.com

If you need other information or have other questions concerning identity theft, please contact the PNCC in Canada, or the FTC in the United States, as listed above.

Resources for Canadian Victims of Identity Theft

PhoneBusters National Call Centre (PNCC)

Ontario Provincial Police Anti-Rackets
Toll Free: (888) 495-8501
Toll Free Fax: (888) 654-9426
Email: info@phonebusters.com
Web: www.phonebusters.com

Credit Reporting Agencies: Place fraud alerts on your credit reports by contacting the credit bureaus that operate in Canada.

Equifax Canada
Report fraud: (800) 465-7166
Web: www.equifax.com/EFX_Canada

Trans Union Canada
Report fraud: (877) 525-3823
Web: www.tuc.ca/TUCorp/consumer/personalsolutions.htm

Further Information

For further information on identity theft and how you can protect your valuable personal information, please consult the following sources: PNCC, Identity Theft, http://www.phonebusters.com/Eng/SpotaScam/scams_identity_theft.html Federal Trade Commission, Identity Theft, <http://www.consumer.gov/idtheft>.

###