

# APPENDIX F

---

## **IDENTITY CRIME PREVENTION ADVICE (DETAILED VERSION) FOR VICTIMS AND OTHER INDIVIDUALS**

### **Staying Alert**

Once resolved, most cases of identity theft stay resolved. But occasionally, some victims have recurring problems. To help stay on top of the situation, continue to monitor your credit reports and read your financial account statements promptly and carefully. You may want to review your credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft, such as:

- failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- receiving credit cards that you didn't apply for.
- being denied credit, or being offered less favourable credit terms, like a high interest rate, for no apparent reason.
- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

### **What Everyone Should Do Now**

- Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SIN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask if you can use a password or customized question/answer instead.
- Ensure that documents with personal information are secured in your home, especially if you have housemates, employ outside help, or are having work done in your home.
- Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personal information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

### **Maintaining Vigilance**

- Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity criminals are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their SIN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line,

rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book. For more information, see *How Not to Get Hooked by a 'Phishing' Scam*, a publication from the U.S. Federal Trade Commission.

- Treat your mail and trash carefully:
  - Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox unless it is locked. If you're planning to be away from home and can't pick up your mail, call Canada Post at 1-866-607-6301 or go online to <http://www.canadapost.ca/tools/pg/manual/PGholdmail-e.asp> to request a vacation hold.
  - To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.
- Don't carry your SIN card, birth certificate or other unnecessary identity documents with you; instead, store them in a secure place.
- Carry only the identification information and the credit and debit cards that you'll actually need when you go out.
- Give your SIN out only when required by law (i.e., for income and tax reporting purposes). Ask to use other types of identifiers instead.

#### **A Special Word About Social Insurance Numbers**

Your employer and financial institutions will need your SIN for wage and tax reporting purposes. Other businesses may ask you for your SIN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your SIN for general record keeping. If you are asked for your SIN, ask:

- Why do you need my SIN?
- How will my SIN be used?
- How do you protect my SIN from being stolen?
- What will happen if I don't give you my SIN?

Getting satisfactory answers to these questions will help you decide whether you want to share your SIN with the business. The decision to share is yours.

NOTE: It is illegal for businesses in Canada to refuse to provide you with a service or benefit simply because you won't provide your SIN to them, unless they have a legitimate need for the SIN (See the federal Personal Information Protection and Electronics Document Act, Schedule 1, Principle 4.3).

- Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

- ❑ When using credit or debit cards, never let them out of your sight. Key in personal identification numbers privately when you use direct purchase terminals, bank machines, or telephones.
- ❑ When ordering new cheques, pick them up from the bank instead of having them mailed to an unsecured home mailbox.
- ❑ Review the cardholder agreement for your debit and credit cards and confirm the level of protection from fraudulent transactions that they offer you. Shop around for a better deal if you are not satisfied with the protection that they offer.

### **The Doors and Windows Are Locked, But . . .**

If you store your SIN, financial records, tax returns, birth date, and bank account numbers on your computer, you are at a higher risk of identity theft. These tips can help you keep your computer - and the personal information it stores - safe:

- ❑ Update your virus protection software regularly (set it to update automatically every week). Install patches for your operating system and other software programs to protect against intrusions and infections that can lead to the compromise of your computer files or passwords. The Windows XP operating system can be set to automatically check for patches and download them to your computer.
- ❑ Never open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard. For more information, see *File Sharing: Evaluate the Risks* and *Spyware*, publications from the U.S. Federal Trade Commission.
- ❑ Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.
- ❑ Use a secure browser - software that encrypts or scrambles information you send over the Internet -to guard your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You also can download some browsers for free over the Internet. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.
- ❑ Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password a combination of letters (upper and lower case), numbers and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become 1LFHA6c. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it's harder for a thief to access your personal information.

- ❑ Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.
- ❑ Look for website privacy policies. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy - or if you can't understand it - consider doing business elsewhere.