Watch Your Identity: Tips for Reducing the Risk of Identity Theft

Prevention of identity theft is a shared responsibility between a consumer and the entities that have possession of their personal and financial information. Both consumers and business must take steps to safeguard the security of their data. While you may not be able to prevent identity theft entirely, the following are important steps that you can take to reduce your risk.

Guard your Personal Information and Documents

- Carry only the ID that you need. Keep all other identification (i.e. SIN, birth certificate, passport) locked in a safe place.
- Be careful about sharing personal information and don't give out more than you need to. If someone asks you for information that is not relevant to the transaction you are making, ask them why.
- When disclosing personal and financial information talk in a discreet manner and always shield your PIN when using your debit card. Please note that consumers have certain rights and responsibilities under the *Canadian Code of Practice for Consumer Debit Card Services.* For more information contact the Financial Consumer Agency of Canada (www.fcac-acfc.gc.ca).
- Ask about the security of your information at work and with businesses and charities.
- Don't leave personal information lying around at home, in your vehicle or at the office. Don't put more than your name and address on your personal cheques.
- Lock your household mailbox, if possible. If you are going to be away, arrange for a trusted neighbour to pick up your mail. You can also go to your local post office (with identification) and ask for Canada Post's hold mail service. There will be a charge for this service.
- Never give personal information by phone, Internet or mail unless you initiate the contact and you know the company very well. Identity thieves may use phony offers or pose as representatives of financial institutions, Internet service providers or even government agencies to trick you into revealing identifying information.
- Shred or destroy sensitive personal documents before tossing them into the garbage or recycling. This will help defeat dumpster divers looking for transaction records, copies of credit applications, insurance forms, cheques, financial statements and old income tax returns. Cut up expired and unused credit and debit cards. The card may have expired but the number may still be valid and could be used to make purchases.

Cat. No Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

Be Vigilant

Pay attention to financial details

Paying attention to financial details can help you watch for signs that you may be a victim of identity theft.

- When using your bank/debit card to withdraw cash or make a purchase, always shield the entry of your PIN. Never give your PIN to anyone, including anyone claiming to be a police officer or bank employee. Choose a PIN that can't be easily guessed, as you could be liable if you use a PIN combination selected from your name, telephone number, date of birth, address or Social Insurance Number (SIN). Remember that no one from a financial institution or the police will ask you for your PIN.
- Keep credit card, debit card and automatic banking machine (ABM) transaction records so you can match them to your statements. If you choose to dispose of your records or statements, shred or destroy them, do not dispose of them in a public place.
- Report any discrepancies on your statements to your financial institution right away, whether it is transactions that appear which you have not made, or transactions that you know you have made, but do not appear.
- Know when your credit card, financial statements and utility bills are due. If they don't arrive when they are supposed to, call the financial institution or utility company – an identity thief may have changed the billing address. If you are missing mail from more than one business, contact the post office to inform them that you are concerned someone is redirecting your mail.
- Pay attention to credit card expiry dates. If your replacement hasn't arrived call the company. Someone may have taken it from your mail or changed the mailing address.
- Keep a list of the names, account numbers and the expiration dates of your cards in a secure place. This will help you when alerting your credit grantors about a lost or stolen card.

Check your credit report

Once a year, or if you think your personal information has been stolen, get a copy of your credit report from each of the major credit reporting agencies (credit bureaus). The report tells you what information the bureau has about your credit history, financial information, judgments, and any collection activity. It also shows who has asked for your information. You can receive a copy of your credit report from one of the following companies in the mail for free or online for a fee:

Equifax Canada Inc.: www.equifax.ca (1-866-779-6440)
Trans Union Canada: www.tuc.ca (1-866-525-02692 Quebec 1-877-713-3393)
Northern Credit Bureau: www.creditbureau.ca (1-800-532-8784)

By checking, you can spot debts that are not yours and see who has been asking about you. You need to follow up if a lender or credit card issuer has asked for a report and you don't have an account with them and haven't applied for credit or a card from them. Someone else may have been using your name.

For more information on understanding what a credit report is, take a look at, Understanding your Credit Report and Credit Score, available from the Financial Consumer Agency of Canada (www.fcac-acfc.gc.ca).

Guard your Computer and its Information

Cat. No Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

Online chats, shopping and banking add a lot of convenience to our lives but, if you don't have appropriate security for your computer, your personal and financial information could be at risk.

A common way for hackers to steal personal information is by using "spyware" which is software that gathers user information through the user's Internet connection without his or her knowledge. Spyware applications are typically bundled as a hidden component of freeware or shareware programs (such as music and video downloading software or online games) that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

The following measures can help protect you against identity theft while online:

- Always create passwords that include a combination of letters (upper and lower case), numbers and symbols. Do not use automatic login features that save your user name and password.
- Install fire-wall, anti-virus, anti-spyware and security software, and keep it up to date.
- Do not send personal or confidential information over email. Email messages are NOT secure.
- Don't try, don't buy and don't reply to spam (unsolicited emails) or phishing emails that ask for personal or financial information. Spam and phishing emails are often a source of scams, viruses and offensive content. *Delete!*
- Install security patches on your operating system and update regularly and frequently. Most software manufacturers regularly release updates and patches to their software to fix bugs that could allow attackers to harm your computer. However, it is up to you to find out.
- Check for suspicious activity online. Almost all firewalls and encryption programs include audit functions that record activities on the network. Check audit trails for unusual or suspicious activity, e.g., computer files in use when you are not aware.
- When disposing of, selling or giving away computer equipment, make sure that you permanently destroy the personal information on the hard drive. If you are disposing of the equipment you can physically destroy it, otherwise use overwrite software. If you don't know how, find out.
- If you use a laptop, physically lock it to prevent thieves from walking away with it and any personal information it contains.

Only shop and bank online with trusted merchants

- Make sure that the website is legitimate. Fraudsters can create a fake website ("brand spoofing") to trick consumers into revealing personal and financial information. Check that the URL is correct – including the domain (.com, .ca, etc.)
- Before submitting any personal information to a website, review its privacy policy for an understanding of how your information may be used.
- Before giving your credit card number or other financial information to a business, make sure the merchant has a secure transaction system. Most Internet browsers indicate when you are using a secure Internet link. To check to see if a website is secure look for a web site address that starts with http**s**://, a closed lock or an unbroken key icon at the bottom right corner of the screen.
- After completing a financial or online banking transaction, make sure you sign out of the website and clear your Internet file/caches and "cookies". Most financial institutions provide instructions on how to do so under their "security" section.
- If you receive an unsolicited email that asks for personal or financial information, do not reply. They are "phishing" for your information. Some fraudsters send email messages posing as a business or a bank that you normally deal with, sometimes even sending you to a site that looks exactly like the business's or bank's website, but is actually a

Cat. No Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155

fraudulent site. Reputable companies will never ask for your personal or financial information in this manner. Note that similar attempts to steal your identity can take place by telephone (sometimes referred to as “vishing”). If you're not sure who you are dealing with when someone calls claiming to be from your financial institution, hang up, and call to confirm using the telephone number that appears on your financial statements, not the telephone number given to you by the person calling you.

Personal Electronic Devices

Any electronic device with personal information could be used to steal your information if a thief were to gets their hands on it. Personal digital assistants (PDAs), cellphones, digital audio players or laptops can be used to carry your personal information. In order to protect your information, try to create passwords when possible. Most devices offer a way to “lock” the device so that the information can only be accessed with a password. Also, when carrying an electronic device, carry it in a manner that you cannot easily drop it or mistakenly leave it somewhere. If you plan to sell, give away or discard an electronic device, ensure you take measures to properly erase all of your personal information from the device. Most manufacturers can provide you with information on how to do so.

Keep your Key Documents Secure

Only carry the ID that you need:
If you drive, you will need to carry your driver’s license of course, and it is also a good idea to carry your provincial or territorial health card as well. However, your birth certificate, SIN (Social Insurance Number) card and passport/citizenship cards should be kept under lock and key, unless you need to bring them with you for a specific purpose. If the documents are stolen they can be used to commit a crime or to impersonate you, resulting in serious consequences. If you do need to carry an important ID card with you, be sure to keep a photocopy of it in a safe place.

Types of documents to keep secure:

- Birth certificate
- Social Insurance Number
- Passport

Note that your Social Insurance Number (SIN) is a confidential number that is only required, by law, for tax reporting if a customer is earning income (either employment or investment).While many companies may ask for you SIN for other purposes, you have the right to refuse under these circumstances. For more information visit the Office of the Privacy Commissioner of Canada at www.privcom.gc.ca.

Cat. No Iu23-6/2007E-PDF
ISBN 978-0-662-44825-9
60155