Protecting Personal Information

Steps you can take to keep your information secure:

- Keep your personal information safe. An identity thief will pick through your bins or recycling, so be sure to shred or tear up unwanted documents that contain personal information before discarding them.
- Keep personal information confidential. Do not give out personal information on the phone, through email or the Internet unless you can verify the identity of the person asking for your information and you know who you are dealing with.
- Bring in your mail daily. Update your address and contact information as soon as you move.
- Limit your exposure. Only carry credit cards you use. Don't carry your birth certificate and social insurance card when you don't need them, instead keep them in a safe place.
- Be aware of billing and statement cycles. If your bills or statements don't arrive on time, follow up immediately to ensure they have not been fraudulently redirected. Request electronic statements.
- Review your monthly account statements thoroughly and report any suspicious activity to us immediately.
- Contact your local police detachment and the The Canadian Anti Fraud Centre if you are a victim of fraud or theft.

Protect Yourself Against Identity Theft

The first step in safeguarding your identity is to understand how identity thieves operate and where you are most vulnerable. For example, if you shred all your confidential information, a would-be identity thief will have little chance of accessing your discarded, but potentially sensitive, information. If you leave a list of passwords next to your office computer, your online data may be far less secure.

Things You Should Do

- Keep all personal information, including passwords and account numbers, in a safe place.
- Secure your purse or wallet at work and elsewhere.
- Make sure no one is lingering nearby before you give personal information over the phone or in person, or enter it into an ATM or other device.
- Use only secure mailboxes for incoming and outgoing mail.
- Shred personal documents before discarding.
- Ask companies with which you do business about their security procedures.
- Don't carry your Social Insurance Number (SIN) card with you.
- Don't give out your SIN number, account numbers, passwords or any other private information in response to e-mail, phone or in-person requests from sources you don't know.
- Don't enter personal information on websites unless you know they are legitimate and secure.

Protect Yourself Online

Following are some easy precautions you can take to help prevent identity theft and/or other abuse of your personal information.

Things You Should Do

- Be wary of any e-mail requesting financial information or other personal data. Do not reply to the e-mail and do not respond by clicking on a link within the e-mail message. Contact the business that allegedly sent the e-mail to verify if it is genuine. Call a phone number or visit a website that you know to be legitimate, such as those provided on your monthly statements.
- Install a firewall to prevent unauthorized users from accessing your computer.
- Make sure you have the most current operating system and web browser software and use their anti-spyware features. Only download software from sites you know and trust.
- Select the highest security setting practical on your browser to prevent unauthorized downloads.
- Beware of anti-spyware offers: Some links in spam that claim to prevent spyware actually install it. Get anti-spyware software from a vendor you know and trust – and scan your computer with it regularly.
- Use “strong” passwords that contain numbers, letters and special characters and that do not include personal information such as name or date of birth.
- Shift to secure online services – such as online banking – to cut down on paper statements, bills and checks. When using online banking or shopping services, make sure the URL (web address) starts with “https:” The “s” indicates a secure transmission of data.
- Run a “wipe” utility before disposing of any computer to erase your personal information.
- Do not send personal information such as credit or debit card numbers, Social Security numbers or PINs in response to any e-mail request.
- Do not click on web page pop-up links; clicking on links within pop-ups can install software on your computer.
- Do not store personal information on a laptop computer.
- Avoid using Internet cafés or public kiosks to access financial sites such as your bank or brokerage account.