

APPENDIX FF

IDENTITY CRIME PREVENTION TIPS (SUMMARY VERSION)

- Minimize the risk. Be careful about sharing personal information or letting it circulate freely. When you are asked to provide personal information, ask how it will be used, why it is needed, who will be sharing it and how it will be safeguarded.
- Give out no more than the minimum, and carry the least possible with you.
- Never carry your birth certificate, SIN, or passport with you unless necessary.
- Be particularly careful about your SIN; it is an important key to your identity, especially in credit reports and computer databases. Provide other identifiers if you have the option.
- Don't give your credit card number on the telephone, by electronic mail, or to a voice mailbox, unless you know the person with whom you're communicating or you initiated the communication yourself, and you know that the communication channel is secure.
- Be suspicious of all email messages you were not expecting. Don't open attachments or click on links in electronic messages from people you don't know.
- Ensure that your computer is protected by virus/security software that is updated weekly.
- Pay attention to your billing cycle. If credit card or utility bills fail to arrive, contact the companies to ensure that they have not been illicitly redirected.
- Guard your mail. Promptly remove mail from an unsecured mailbox after delivery. Ensure mail is forwarded or re-routed if you move or change your mailing address.
- Notify creditors immediately if your identification or credit cards are lost or stolen.
- Access your credit report from a credit reporting agency once a year to ensure it's accurate and doesn't include debts or activities you haven't authorized or incurred.
- Ask that your accounts require passwords or customized question/answer challenges before any inquiries or changes can be made. Choose difficult passwords – not your mother's maiden name. Memorise them and store them in a non-obvious location.
- Key in personal identification numbers privately when you use direct purchase terminals, bank machines, or telephones.
- Find out if your cardholder agreements offer protection from fraudulent transactions; shop around for a better deal if you are not satisfied with the level of protection offered.
- Burn or shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc. Insist that businesses you deal with do the same.