IDENTITY THEFT

A. BACKGROUND

The crime of identity theft occurs when someone, without knowledge or permission, acquires personal information and uses it to commit fraud. It is the intent of this Fact Sheet to provide preventive measures to minimize personal risk against a selected sample of identity theft schemes.

A list of website links is included in the reference/glossary. Members should view this Fact Sheet as a cursory overview of this complex topic and take their own steps to ensure that they do not become victims, including becoming vigilant against new scams that appear on a regular basis.

B. STOLEN MAIL AND TRASH

1. Paper items containing financial information and personal identification should never be included with recyclables and trash.
2. Invest in a crosscut or diamond-cut shredder and shred all financial statements, credit/debit card slips, pre-approved credit offers, blank cheques (including those from pre-approved credit offers), cancelled cheques, tax information, cheque attachments, business items, credit cards, phone calling cards, CDs containing personal information; basically anything that contains personal information and identification.
3. Mail should not be left in rural or apartment mailboxes when on vacation or away for an extended period of time.

C. CREDIT REPORTS

1. Request a credit report at periodic intervals and check carefully for unauthorized inquiries, address changes or account activity. If possible, get reports from more than one source. Credit reports provide plenty of background information that would assist an identity thief.
2. Place fraud alerts with Trans Union (1.877.525.3823) and Equifax (1.800.465.7166) if an identity has been compromised.

D. CHEQUES, BANK/CREDIT CARDS AND RELATED STATEMENTS

1. Review various statements electronically, on line, or as soon as they arrive, for accuracy. This is the time to shred related slips once vetted against personal statements. Report unauthorized items right away.
2. Don't put phone numbers on cheques. Have new cheques sent to the bank instead of a residence.
3. Try to have a photo on credit and identification cards. In addition to signing the back of such cards, which should always be done, you may wish to print "Photo ID required" in indelible black ink, as an added protection against identity theft.

E. ATMS OR POINT-OF-SALE KEYPADS

1. Thieves use tiny cameras hidden on themselves and elsewhere to spy on individuals as they input PINs at ATMs or point-of-sale keypads on checkout counters. Shield the keypad when using these.
2. Try not to hand credit cards to servers who take them for processing. Pay at the cashier or insist they bring the machine to the table. Ensure cards are not swiped more than once. Thieves make duplicate passes with the cards, then steal the information to access accounts.
3. PINs should be changed regularly. Personal information should not be on card slips.

F. INTERNET AND EMAIL

1. When receiving a new computer, avoid the temptation to go online immediately. Take the time to activate, register and update the virus protection program. Many computers are compromised in the first fifteen minutes online because the operator began to browse before initiating the anti-virus program.
2. Most malware is constructed to target Microsoft products (Internet Explorer and Outlook Express). Other products seem less susceptible to attack, might have superior features, and typically are no-cost items, e.g. Mozilla's Firefox browser and Thunderbird and Google's G-Mail e-mail program.
3. Those with DSL or cable high speed service, especially with wireless access, are especially vulnerable to identity thieves. Turn off computers when you are not using them. Protect wireless networks with passwords to protect unwanted access.
4. If storing passwords electronically, consider using a removable drive with no locating information on it, instead of a hard drive. Avoid copy-and-pasting passwords. Thieves use programs which harvest data from temporary memory. Remove temporary Internet files regularly.
5. Online money transfer services (PayPal is one example) pose significant risks. Register only low-credit-limit credit cards or a low-balance bank account with such a service. See "Phishing" below.
6. Never click on a link, then enter personal or account information. Instead, open a new browser and go directly to the company's site and log in from there.
7. Install and regularly update appropriate firewalls (free at www.zonealarm.com), anti-spyware (free at www.microsoft.com/athome/security/spyware/software/default.mspx), and virus protection (free at www.avast.com). Routinely (or automatically) check for Windows or other operating system updates and install them.
8. Remember that VoiP (Voice-over-Internet Protocol) telephones can be hacked and conversations eavesdropped upon. VoiP providers can help users protect themselves against this type of potential identity theft.
9. Avoid aiding and abetting spam (unsolicited junk e-mail), the mechanism by which much of online identity threats are spread. Do not forward those jokes, hoaxes, chain letters etc. forwarded to you. If an email must be forwarded, copy and paste it into a new message and send it to a specific individual.
10. Avoid sending e-mail messages to entire lists unless the blind carbon copy (BCC) feature is used, so that individual email addresses are not revealed to the other recipients. Thieves love getting entire e-mail lists and compiling masses of them for sale to spammers.

G. PHISHING AND SPOOFING

1. Thieves will send emails with special offers or requests for information. Often, such emails look legitimate,

using exact logos and identifiers of trusted businesses. However, the legitimate businesses never ask for such information or make such offers on line. Sometimes, the tip-off to illegal activity lies in the awkward sentence structure or misspelled words of the message. Forward such messages to the legitimate website of the organization and ask for verification.

2. Never click on a link in an unexpected e-mail. If a fraudulent e-mail from its very appearance in an inbox looks suspicious, don't even open it, because the simple act of opening it may compromise a computer. Three sources of such phishing often involve fake banks, EBay or PayPal.

3. Some e-mails ask to update account information. Immediately forward such requests to the legitimate websites of these or other relevant companies (see above). Financial institutions do not contact clients by e-mail; neither does Microsoft, Bill Gates, etc.

H. GENERAL INFORMATION

1. Don't leave information open to view, even at home. Keep personal information in a secure place, ideally not in a dresser. Maintain a back-up list of all card numbers with emergency 800 numbers, and include items such as passports, licences, credit cards and SINs. Keep this list in a secure place (with copies for your spouse/partner), but not on the hard drive of a computer.

2. Passwords should be changed on a regular basis. Do not use the same password for all applications and don't use obvious passwords such as a mother's maiden name or partner's birthdate. Use a password which is case sensitive, alpha-numeric and at least 6 characters long, preferably more. Keep a secure list of your passwords, logins and what each relates to (but not on a hard drive). Update these lists regularly. If possible, passwords and licence/card numbers should be memorized.

3. When ordering new or replacement cards, make a note to watch for the incoming mail. If the replacements don't arrive in a week or so, notify the issuers. Cancel all cards not used for six months. "Open" credit is a prime target.

4. The three-digit code on the back of a credit card must be safeguarded. If a thief gets it, it is very difficult to prevent unauthorized on line or phone use of the card.

5. Don't carry a Social Insurance card, birth certificate or passport unless necessary.

6. Be very cautious about using credit cards for on-line payments, and if so, ensure that it's on a secure site (beginning with "https").

7. If donating to a tele-marketed charity or responding to a request from someone who asks for personal information, ask them to send a request in the mail or tell them you'll look up their phone number and so that a call will be placed with them to verify the authenticity of the request. Persevere and resist through their encouragement to "do it now, on the phone".

8. Don't permit photocopying of documents when asked to provide your ID.

9. Use initials on phone directories, not full names.

10. Cell phone users who are on line should be vigilant and alert and should seek advice from service providers with respect to protection against identity theft.

11. Banks and other financial institutions never ask for personal information over the phone. If someone tries to "verify" an account or asks for "help to catch an internal thief", this is a scam. Try to get a phone number from them and then call the bank to report the phone numbers as possibly fraudulent.

12. The Ontario government ensures that property will not be lost as a result of the registration of a falsified mortgage (obtained with stolen identity), a fraudulent sale of property or a counterfeit power of attorney. As well, consumers in Ontario have the right to have fraud alerts placed on their credit report to help stop identity thieves from using their personal information to commit fraud (see Fact Sheet E-10, Mortgage Fraud).

I. RESOURCES

While it is believed that these links represent reliable sources of information, it is a member's responsibility to verify authenticity. RTO/ERO takes no responsibility for a site's purported accuracy, completeness or reliability.

If you are accessing an electronic version of this fact sheet, practise cutting and pasting the links into your browser address line. This enhances your internet security. Phone numbers, if available, are also provided.

1. **Ontario government's website www.seniorsinfo.ca** has links to information for seniors in general, and for victims of identity theft in particular.
2. **Canadian Association of Retired Persons (CARP)** - fourteen links to relevant articles www.carp.ca/display.cfm?SEARCHTERM=identity+theft&search=yes
3. **Canadian Snowbirds' Association** alert about a fraudulent US Internal Revenue Service W8-BEN form – particularly useful for members who spend a significant amount of time or own property in the US www.snowbirds.org/html/w8-BENScam.html
4. **Consumer Measures Committee**, Consumer issues and information kits for seniors cmcweb.ca/epic/site/cmc-cmc.nsf/en/Home
5. **RCMP Phonebusters** www.phonebusters.com
6. **US Federal Trade Commission** – a variety of useful links www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

J. GLOSSARY

Alpha-numeric	a password or code having both letters and numbers, e.g. postal code P2B 3M5
Bcc	"blind carbon copy", a feature which distributes the message to all on the list but prevents each recipient from seeing the names and addresses of other recipients
Firewall	a program which detects and blocks the attempts of other computers to link with yours without your approval

ISP	Internet service provider
Malware	A generic term for programs written for malicious purpose
Pharming	(pronounced "farming") is an attack aiming to redirect a website's traffic to another, bogus or spoofed website
Phishing	attempt to lure a person into revealing information; occurs both online and by telephone
Spam	unsolicited e-mail, often disguised as an "attractive" opportunity, e.g. the Nigerian Letter which asks you to help move funds from overseas for a commission, for which purpose you are required to provide your bank account information
Spoofing	attempt to lure person into revealing information by setting up a facsimile website
Zombie	a computer which has been taken over for unscrupulous use, e.g. to forward spam via your e-mail account with the purpose of distributing a malicious program