PERSONAL SAFETY

Chapter Contents

- Personal Safety Information
- Frauds and Scams
- False Charities
- Inheritance Scheme

PERSONAL SAFETY INFORMATION

Canadian Marketing Association

Phone: 416.391.2362 Email: donotmail@the-cma.org www.the-cma.org To reduce unwanted advertising mail register with CMA's Do Not Mail Service free of charge.

CMA Do Not Mail Service

- The Canadian Marketing Association does not maintain, rent or sell any consumer marketing lists. All our members that engage in direct (to consumer) marketing are required to use our Do Not Mail list to remove matching names from their marketing lists. Names are maintained on the service for 6 years and the service takes approximately six weeks to take effect.
- To reduce telemarketing calls, register your phone number with the National Do Not Call List. Call 1.866.580.3625 or visit www.LNNTE-DNCL.gc.ca

FRAUDS AND SCAMS

Every day, seniors are at risk of being taken advantage of by criminals. Although many legitimate businesses market their products and services over the telephone (telemarketing), door-todoor, or through the Internet, mail, newspaper and magazine ads, there are some dishonest people who will use these methods to try to take your money. Learn how to tell the difference between a legitimate and honest offer and individuals who could be defrauding you. The following information is from The Little Black Book of Scams, a fraud protection guide provided by the Competition Bureau. To order a copy: 1.800.348.5358. To view the full guide online, visit www. competitionbureau.gc.ca/eic/site/cbbc.nsf/eng/04333.html

Scammers Do Not Discriminate

Scammers target people of all backgrounds, ages and income levels. Fake lotteries, Internet frauds, get-richquick schemes, and miracle health cures are some of the favoured means of separating the unwary from their money. New varieties of these scams appear all the time. Some popular scams include:

Lotteries, Sweepstakes, and Contests

You cannot win money or a prize in a lottery unless you have entered it yourself, or someone else has entered it on your behalf. You cannot be chosen as a random winner if you did not submit an entry.

PERSONAL SAFETY

Money Transfer Requests

Be very careful when someone offers you money to help transfer their funds. Once you send money to someone, it can be very difficult, if not impossible, to get it back, and you also risk having your identity stolen.

Internet Scams

Don't just assume an email you receive is legitimate. If the email is asking you to visit a website to "update", "validate" or "confirm" your account information, be sceptical.

Handy Hints to Protect Yourself

Protect Your Identity

- Only give out your personal details and information where it is absolutely necessary and when you trust the person you are speaking to or dealing with.
- Destroy personal information: don't just throw it out.

Money Matters

- Never send money to anyone you don't know and trust.
- Do not send any money or pay any fee to claim a prize or lottery winnings.

The Face-to-Face Approach

• If someone comes to your door, ask to see some identification. You do not have to let them in, and they must leave if you ask them to.

Telephone Business

• Do not give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.

Email Offers

- Never reply to a spam email the best course of action is to delete any suspicious emails without opening them.
- Legitimate banks and financial institutions will never ask you for your account details in an email or ask you to click on a link in an email to access your account.

Internet Business

- Install software that protects your computer from viruses and unwanted programs and make sure it is kept current. If you are unsure, seek the help of a computer professional.
- Never enter your personal, credit card or online account information on a website that you are not sure is genuine.
- Never send your personal, credit card or online banking details through an email.

Scams and You: What To Do If You Get Scammed!

Report a scam. By reporting the scam to authorities, they may be able to warn other people about the scam and minimize the chances of the scam spreading further. You should also warn your friends and family.

If you think someone has gained access to your online account, telephone banking account or credit card details

call your financial institution immediately so they can suspend your account and limit the amount of money you lose. Credit card companies may also be able to perform a "charge back" (reverse the transaction) if they believe that your credit card was billed fraudulently.

If you have sent money to someone that you think may be a scammer:

- If you sent money through an electronic funds transfer (over the Internet), contact your financial institution immediately. If they have not already processed the transfer, they may be able to cancel it.
- If you sent a cheque, contact your financial institution immediately. If the scammer hasn't already cashed your cheque, they may be able to cancel it.
- If you sent money through a wire service (such as Western Union or Money Gram), contact the wire service immediately. If you are very quick, they may be able to stop the transfer.

Reporting a Scam

The Canadian Anti-Fraud Centre

www.antifraudcentre.ca Phone: 1.888.495.8501 See full listing this section

The Competition Bureau's Information Centre

www.competitionbureau.gc.ca Phone: 1.800.348.5358

Contact the police

If you are the victim of fraud - you have suffered a loss because of someone's dishonesty or deception - you should contact your local police (particularly if the amount involved is significant). You should contact the police if you have had your property stolen or have been threatened or assaulted by a scammer.

Alberta Securities Commission (ASC)

Toll-Free: 1.877.355.4488 Email: inquiries@asc.ca www.albertasecurities.com www.checkfirst.ca Hours of operation: Mon-Fri 8:00am–5:00pm (with some exceptions on major holidays) Develop your investor knowledge, avoid fraud and make informed and suitable investment decisions with unbiased resources and information brought to you by the Alberta Securities Commission (ASC). If you're approached with an investment opportunity, do your own research before making a decision.

Visit the ASC's investor education site CheckFirst.ca to:

- Access free unbiased information, factsheets, calculators and videos on investing wisely and avoiding fraud
- Make a complaint or report a suspicious investment opportunity; and
- Check registration and disciplinary history of an individual or firm offering an investment

Service Alberta and Consumer Contact Centre

Edmonton: 780.427.4088 Toll-Free: 1.877.427.4088 www.servicealberta.ca Follow the Consumer Information link. Information on Fraud Awareness is also available online at www.seniors.gov.ab.ca

The Canadian Anti-Fraud Centre

Box 686, **North Bay**, ON P1B 8J8 Toll Free: 1.888.495.8501 www.antifraudcentre.ca Hours of Operation: Mon-Fri 9:00am-4:45pm EST.

- The Canadian Anti-Fraud Centre (CAFC) is a joint forces operation with the RCMP, OPP and the Competition Bureau.
- The CAFC collects information and criminal intelligence on mass marketing fraud, and identity fraud schemes.
 The CAFC does not investigate but provides valuable assistance to law enforcement agencies all over the world.
- The CAFC Senior Support Unit has senior volunteers that call back senior victims to offer education and support.

The CAFC top mass marketing scams targeting seniors:

Tax scams: Fraudsters are calling impersonating the Canada Revenue Agency claiming that a recent audit has identified discrepancies from past filed taxes. Repayment is required immediately. Fraudsters threaten consumers with jail time and/or deportation. Fraudsters want payment asap. Contact the CRA at 1-800-959-8281 to confirm if you owe back taxes or are entitled to a refund. The CRA would never request payment by money service business, iTunes gift cards or bitcoin. Phishing Scams are misleading and deceptive emails, falsely claiming to be from a legitimate organization such as a financial institution, business or government agency in an attempt to have the consumer surrender private and personal information.

These unsolicited phishing scams are designed to get victims to click on malicious links or attachment that result in the installation of malicious software. Watch for spelling and formatting errors. Check the embedded hyperlink in the suspicious email by hovering your mouse over the link to verify the address. Do not click on any attachments; they can contain viruses and spyware. Go with your gut. If an email seems fishy it probably is.

Prize Scams may target you by phone, email or social media. They say you are winner of a large lottery or sweepstake. They may claim to represent "Reader's Digest" or "Publisher's Clearing House" and before you get your winnings, you are required to pay a small advance fee to cover taxes or legal fees associated with the win. Never pay fees upfront through a money service business such as Western Union, MoneyGram or by loading funds to prepaid credit cards such as iTunes. Any unsolicited phone call advising that you have won a lottery is fake. No winnings are ever received.

Service Scam: Any false, deceptive or misleading offer of services. These scams typically involve third parties offering antivirus protection, lower credit card interest rates.

Emergency/Grandparent Scam: A

grandparent receives a phone call from a con artist claiming to be a grandchild. They claim being in a car accident, and in trouble with the law and need money. Wanting to help, the victim sends the money as instructed. Variations on the scam exist but predominantly the emergency scam is directed toward the grandparents. **Extortion Scam**: Consumers receive a call or text message claiming that they owe "back taxes" as the result of an audit. The payment must be made immediately to avoid a fine. However, the recipient is told that the outstanding warrant can be avoided if the payment is made promptly. In many cases, individuals are told they will be deported if the taxes are not paid right away. Consumers are instructed to purchase and activate iTunes gift cards and provide the codes back to the fraudsters.

Warning sign(s) - How to protect yourself:

- If you are asked to pay for any service or product with CRA or CIC by prepaid cards such an iTunes gift card, don't do it, it's a scam!
- Ask yourself why the CRA would be asking for payment through an iTunes gift card over the phone or text message when they already have you on file as a taxpayer.
- Contact the CRA to confirm that you in fact owe back taxes, or are entitled to a refund, before providing any personal or banking information.

But the scam with the highest financial loss is the:

Romance Scam

Any individual with false romantic intentions towards a victim and by gaining their affection and trust (sometimes with the promise of marriage) gains access to the victim's money, bank account, credit cards or in some cases by getting the victims (usually unknowingly) to commit fraud on their behalf.

In 2011, Romance scams emerged as highest grossing scam, with over 12 million

dollars in losses reported by Canadians. This scam has also lead to incidents of suicide in cases where victims have lost their life savings and have been emotionally destroyed.

For more information about frauds and scams contact:

- Service Alberta and Consumer Information Centre
- The Canadian Anti-Fraud Centre

How To Report Fraud

It's not always easy to spot a scam, and new ones are invented every day. If you suspect that you may be a target of fraud, or if you have already sent funds, don't be embarrassed - you're not alone. If you are a victim of fraud – file a report with your local police. If you want to report a fraud, or if you need more information, contact The Canadian Anti- Fraud Centre:

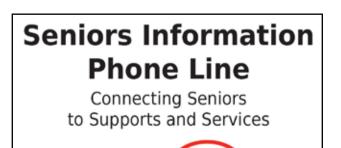
Ways to report fraud

• On-line:

www.antifraudcentre-centreantifraude.ca To all users: This application works best with Internet Explorer.

• Toll Free: 1.888.495.8501

Dial



Identity Theft and Identity Fraud Victim Assistance Guide

Tips that will help minimize your risk.

 Before you reveal any personally identifying information, find out how it will be used and if it will be shared.
Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time.

3. Guard your mail. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after delivery. Ensure mail is forwarded or re-routed if you move or change your mailing address.

4. Utilize passwords on your credit card, bank and phone accounts. Avoid using easily available information such as your mother's maiden name, your birth date, the last four digits of your SIN or your phone number.

5. Minimize the identification information and number of cards you carry.

6. Do not give out personal information on the phone, through the mail or over the internet unless you have initiated the contact or know whom you're dealing with.

7. Keep items with personal information in a safe place. An identity thief will pick through your garbage or recycling bins. Be sure to tear or shred receipts, copies of credit applications, insurance forms, physician statements and credit offers you get in the mail.

8. Give your SIN only when absolutely necessary. Ask to use other types of identifiers when possible.

9. Don't carry your SIN card; leave it in a secure place.

If you suspect or know that you are a victim of identity fraud, or if you unwittingly provided personal information or financial information: Keep records of steps taken to clear your name and re-establish your credit.

Step 1 - Contact your bank/financial institution and credit card company.

Step 2 - Contact the two national credit bureaus. Let them know you are a victim or at risk for ID fraud. Request a fraud alert be placed on your credit report (Dispute any activity on your report that you did not initiate).

Equifax Canada Toll-free: 1.800.465.7166

TransUnion Canada

Toll-free: 1.877.525.3823 Quebec residents: 1.877.713.3393

Step 3 – If you are a victim of ID fraud contact your local police force and file a report.

Step 4 - Report identity fraud to the **Canadian Anti-Fraud Centre** Toll free: 1.888.495.8501

FALSE CHARITIES

In Canada we have a long and honourable tradition of voluntary giving, often through charity organizations. If an unfamiliar charity organization contacts you - by mail, phone, or Internet - be careful. Are they bogus?

Warning signs

- High pressure or threatening.
- Want you to contribute immediately.
- Thanks you for a pledge you didn't make.
- Copycat, misleading, or deceiving names.

What you can do: Ask

- for information to be sent to you in writing.
- how much of your gift will be used directly for the charity.
- how much goes to administrative costs.
- if the charity is registered, get their charitable tax number. Call the Canada Revenue Agency at 1.800.267.2384. Compare numbers.

What else you can do:

- Never give your personal/financial information.
- Call the charity. Do they know of the appeal? Ask them the above questions.
- Remember, on an incoming call a person could be misrepresenting a legitimate charity.
- Once a year, decide which charities you want to donate to and send your cheque directly to their head office. There are more than 85,000 registered charities in Canada. The Canada Revenue Agency (CRA) reviews applications for registered status and determines if an organization's purposes and activities are charitable and provide a public benefit. To

find out if an organization seeking a donation from you is a registered charity, visit canada.ca/ charities-list

INHERITANCE SCHEME

Foreign Money Offer: Any solicitation commonly offering or requesting assistance in the transfer of a large sum of money from an international country. The solicitation may also come from a lawyer or some legal entity advising the victim of an inheritance of a sum of money. The victim must pay one or more advance fees before the money can be released. The money or inheritance is fictitious and the victim never receives the money promised. This is sometimes referred to as Nigerian, 419 or West African fraud.

IF YOU THINK A SENIOR IS BEING ABUSED

- 1. Call the Seniors Abuse Helpline at **780.454.8888** (available 24 hours).
- Contact your local police, RCMP department, or tribal police immediately when abuse involves theft, assault, or other illegal actions.
- Report abuse in a care facility through the Protection for Persons in Care Reporting Line (Toll Free) 1.888.357.9339.
- Call the Sage Seniors Safe House Intake Line at 780.702.1520.