



# CANADIAN ANTI-FRAUD CENTRE BULLETIN

2021 Fraud Awareness Information Package

2021-03-01

FRAUD: RECOGNIZE, REJECT, REPORT

## SENIORS

**2021 Fraud Awareness Information  
Package with added fraud information for  
the OSSTF ARM chapter 9 members**

- MONEY MULES
- COVID19 FRAUDS
- RECOVERY PITCH



Royal Canadian Mounted Police  
Gendarmerie royale du Canada



Competition Bureau  
Canada

Bureau de la concurrence  
Canada



Ontario Provincial Police

Canada

## Introduction

As fraud rates continue to increase in Canada, the world is going through a global pandemic. The COVID-19 has created an environment that is ripe for fraud and online criminal activity. The COVID-19 has resulted in never-before-seen numbers of people turning to the internet for their groceries, everyday shopping, banking and companionship. Coupled with the profound social, psychological and emotional impacts of COVID-19 on people, one could argue that the pool of potential victims has increased dramatically.

The Canadian Anti-Fraud Centre (CAFC) has specifically designed this fraud awareness information package for seniors (60 years of age and older) to further raise public awareness and prevent victimization. We encourage everyone to read and share this information.

The CAFC is Canada's central repository for data, intelligence and resource material as it relates to fraud. The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies by identifying connections all over the world. Victims who report to the CAFC are also encouraged to report directly to their local police. The information provided may be the clue needed to solve the puzzle. Let local police know that you are a senior victim of fraud and wish to file a report.

Comments, questions or feedback on fraud prevention are always welcome.

Thank you,

Your CAFC Fraud Prevention Team and the Senior Support Unit

Website - [www.antifraudcentre.ca](http://www.antifraudcentre.ca)

Follow us on Twitter – [@canantifraud](https://twitter.com/canantifraud)

Like us on Facebook – [Canadian Anti-Fraud Centre](https://www.facebook.com/CanadianAntiFraudCentre)



## CAFC Senior Statistics

### Top 10 Frauds - by dollar loss

Fraud Pitch	Reports	Victims	Dollar Loss
Romance	251	169	\$7.3 million
Service	692	419	\$6.5 million
Investment	96	86	\$6.1 million
Prize	408	133	\$2.5 million
Bank Investigator	524	228	\$2.5 million
Spear Phishing	183	84	\$1.1 million
Extortion	3,651	1,207	\$1.1 million
Inheritance	86	8	\$0.8 million
Emergency	501	172	\$0.7 million
Loan	55	35	\$0.5 million

In 2020 the CAFC received 101,483 fraud reports involving nearly \$160 million in reported losses. Moreover 11,447 of the reports were from senior Canadians that reported losses totalling more than 31.8 million dollars.

These statistics show the Top frauds that targeted seniors based on dollar loss in 2020.

The top 3 are briefly explained below:

**Romance scams at all-time high**: romance fraudsters are making more money than ever before. Sending money to someone you have not met for love and friendship is a risky move. You not only lose your money but your heart and trust in someone that you were sure loved you back. Current issues regarding this scam is that they start out on a dating website where the scammer develops trust, friendship and then suggests investing opportunity into crypto currency with Bitcoin being the preferred investment choice.

#### **Service scams**

There are a variety of service scams reported to the CAFC, some of the more common and current service scams include:

Help with government documents

- For a fee, a website offers services to help you:
- get a passport

- get a birth certificate
- book a driver's road test
- get a pardon or criminal record waiver
- the website may promise faster processing times or other guarantees.

The reality is -the forms needed to get government identification are free. No one can speed up the process.

### Immigration websites

Scammers create fake websites and online ads that offer "cheap" immigration services or even may "guarantee" high paying jobs. Many of the websites will look like official government sites.

Beware if they are asking you to pay for application access fees or deposits before the application is even started.

### Low interest rate offers –

the offer could come in the form of a pop up, and or if you have been searching online for credit, you may receive a personal offer from a scammer offering reduced interest rates on credit cards or line of credit. They request personal information from you, such as your:

- Social Insurance Number (SIN)
- mother's maiden name
- date of birth
- credit card information

In most instances, the scammers request a one-time fee for the service. The reality is that scammers do not have the ability to lower interest rates. Only your credit card companies can do that. They're stealing your personal information and/or your money for a service that they cannot provide.

### Resale

Common resale scams target automobiles, timeshares and rental or property listing. Typically, you'll be targeted after posting something for sale online. The scammer claims to have a buyer and offers their help to sell the item, for a fee. If you pay, you learn there is no buyer and your money is gone.

### Tech support

A scammer claims a virus has infected your computer. The communication might happen through:

Alarming website pop-ups that demand you call a number urgently

Unsolicited telephone calls (they may claim to be a Microsoft or other well-known computer company employee)

The scammer states that your computer is sending out viruses or has been hacked and must be serviced. They request access to your computer and may run programs or alter settings.

The scammer asks you to pay a fee for fixing your computer via credit card or money transfer. In some cases, the scammer asks you to log into your bank account to transfer funds.

**An investment scam** is any solicitation for investments into false or deceptive investment opportunities. These opportunities falsely promise higher-than-normal returns. However, investors lose most or all their money.

As mentioned the “Hot” investment schemes these days involve crypto currency. Always check with your provincial securities commission to see what the current regulations are before investing. In Ontario that would be the Ontario Securities Commission

## **Money Mule Awareness**



Increasingly, fraud networks are recruiting unsuspecting victims—including seniors to receive and transfer money from other victims. This is against the law.

**What is a money mule?**

**A money mule is person who's recruited by fraudsters to serve as a middle person to transfer stolen money. This is known as money laundering, which is a crime. The victim/money mules may or may not know that they're a pawn in a larger network. When a mule moves money, it becomes harder to identify the fraudsters from the victims.**

**Scammers don't tell you the money is stolen. Instead, they tell you a story-full of lies and deceit.**

**Maybe they meet you online and create a relationship. Then, they ask you to deposit some money and send some of it to someone else.**

**Or maybe you find a job online. They send your first paycheck and ask you to give some of it to a "supplier" or "client."**

**Or they say you've won a prize, lottery or sweepstakes. They send you money, telling you to keep some for yourself as winnings, then forward part of it elsewhere.**

**But in fact, there never was a relationship, job or prize – just a scam.**

**These are just some of the ways that scammers may get you to move stolen money.**

**The reality is –the fraudsters have woven a complex web of deceit. And in many incidents the senior victims are unaware of their participation in a worldwide billion dollar fraud scheme.**

**Victims are often told to transfer the money using the popular payment methods:**

- **cash by courier**
- **bank wire transfers**
- **email money transfers**
- **money services, businesses**
- **and virtual currencies, Bitcoin being the preferred choice**

**Typically, mules receive a small percentage of the money transferred –especially if they are thinking they have a job moving money around.**

## **Recovery Pitch Awareness**

**Just when you thought it couldn't get any worse, it can.**

**If you've recently been a victim of any fraud - watch out for the "recovery pitch"...victims may be at risk of being targeted again by the same scammer with the hopes of obtaining additional funds.**

**How does it work?**

**The recovery pitch involves scammers trying to convince you that there is an opportunity to recover the money you lost in the previous scam.**

**The scammers may appear to be a member of law enforcement, investigating agencies, bank employees, investment firm, or lawyers with the goal of establishing trust and credibility.**

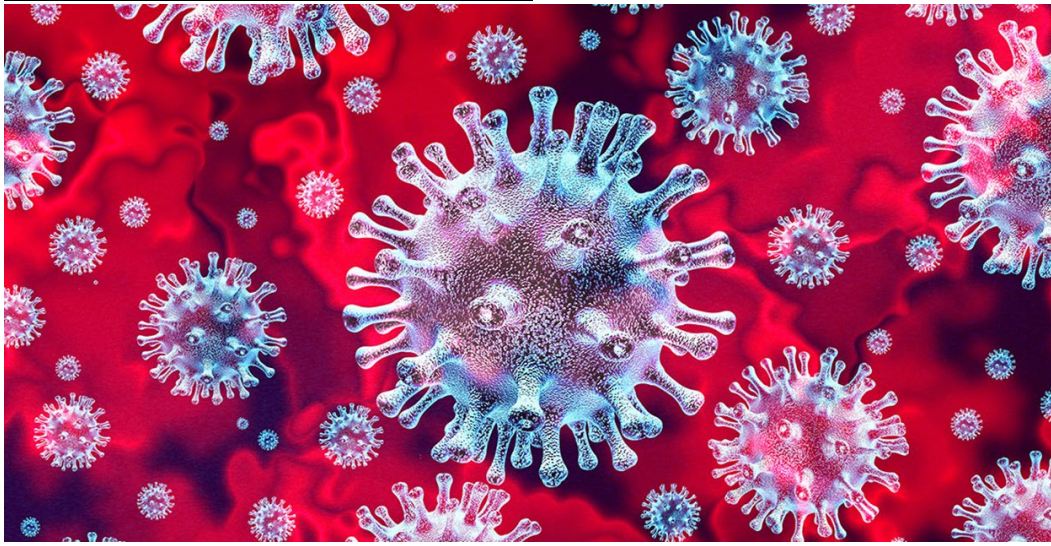
**This picture shows a boiler room where victims of the fake tech support scam were re-contacted by the fraudsters and told that they would be getting their money back, and all they had to do was give them remote access and they would refund the money that they lost to the tech support scam. They were so convincing that many Canadians fell for the recovery pitch and either sent money or gave remote access of their computer to the criminal once again.**

**Also, if you have been victimized- be aware that scammers also make money from selling your contact information to other organized crime groups that may target you with a different pitch. Perhaps the emergency grandparent scam, the romance scam, or the investment scam. Stay on top of all frauds and learn how to recognize, reject and report fraud, by visiting our CAFC website often.**

**[www.antifraudcentre.ca](http://www.antifraudcentre.ca)**



## **Covid-19 Fraud Awareness**



**The list of Covid 19 related frauds is almost endless.**

**Beware of:**

- **Unsolicited emails stating your Covid booster has been booked for you – requesting you to click a link requesting your sensitive information to confirm the date and time.**
- **Potential counterfeit vaccine passports**
- **Potential counterfeit COVID-19 vaccines**
- **Private companies selling fraudulent products that claim to treat or prevent the disease**
- **Unapproved drugs threaten public health and violate federal laws**

**The only way to access safe and effective COVID-19 vaccines is through clinics organized or endorsed by your local public health authority in collaboration with Canada's federal, provincial and territorial governments**

- **Coronavirus-themed emails or text messages and COVID-19 vaccination themed emails or text messages that are trying to:**
- **trick you into installing malicious COVID-19 notification apps**
- **trick you into opening malicious attachments**
- **trick you to reveal sensitive personal and financial details**

**Unsolicited calls claiming to be from a private company or health care providers offering home vaccination kits for an up-front fee:**

- **Private companies offering fast COVID-19 tests for sale**

- Questionable third-party companies offer to help you fill out applications, such as CERB
- Criminals using your identity to sign-up for CERB and receive payments
- Spoofed government, healthcare or research information
- Unsolicited calls, emails and texts requesting urgent action or payment and/or offering medical advice, financial relief, or government assistance and compensation

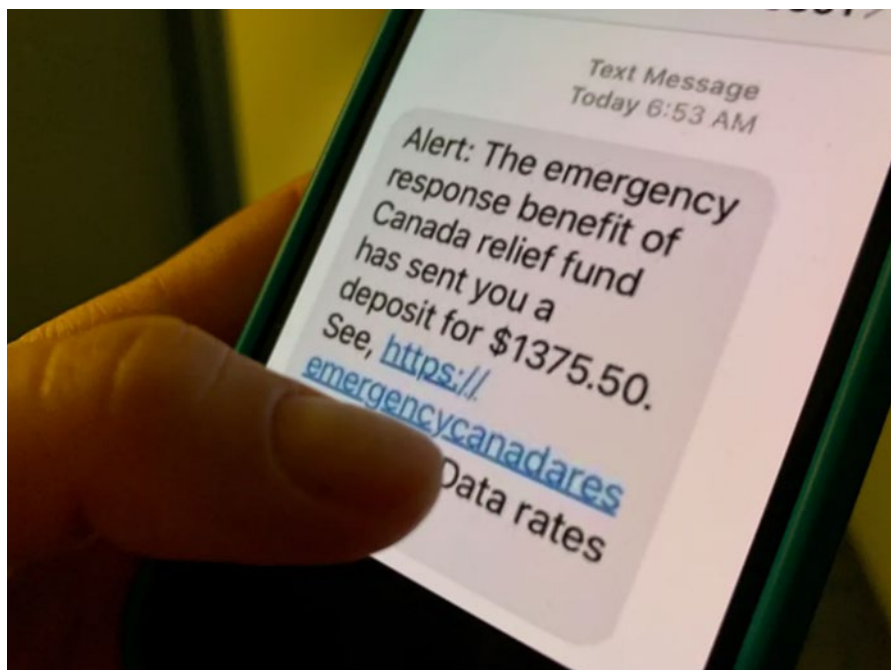
**If you didn't initiate contact, you don't know who you're communicating to:**

- Never respond or click on suspicious links and attachments
- Never give out your personal or financial details
- Unauthorized or fraudulent charities requesting money for victims, products or research
- Don't be pressured into making a donation
- Verify that a charity is registered on the CRA's website

**Beware of high-priced or low-quality products purchased in bulk by consumers and resold for profit. These items may be expired and/or dangerous to your health.**

**To summarize questionable offers might include:**

- vaccine passports
- miracle cures
- herbal remedies
- vaccinations
- faster testing
- fake and deceptive online ads



**Current reported scams to the CAFC include:**

**Phishing, spear phishing and malicious links sent from what looked like a familiar email address or text message The text message might claim to be from your Ministry of Health and will say that your third COVID-19 vaccine/the booster has been scheduled. The message then asks you to click on a malicious link. After clicking, you are asked to download software that contains malware.**

**Or**

**A text message claiming to be from the Government of Canada that says "due to a recent vaccination, Canadians are eligible for a Vaccine Relief Fund". The message then tells you to claim your funds by clicking on a link. The goal is to steal your personal and/or financial information, which can be used for identity fraud**

**Or**

**An email containing links or content related to COVID-19 vaccines and once you click on them it freezes your computer, makes you call a toll-free number and then they demand money from you to unfreeze your account**

**And**

**Phone calls offering home vaccination kits**

**A phone call from someone claiming to work for a pharmaceutical company and offering a "6 shot vaccine system" which you receive by mail after paying large sums of money.**

**So please slow down, be cautious, take the time to verify, verify, and verify any unsolicited offers with a trusted source. If fraud is detected –report it to the CAFC and or if you are in doubt call us to see what we know about it.**

**From March 6, 2020 and September 30, 2021, the CAFC received:**

- **Canadian reports of COVID-19 fraud: 28,290**
- **Canadian victims of COVID-19 fraud: 26,230**
- **Lost to COVID-19 fraud: \$7.75 M**

## **Links to Fraud Awareness & Prevention videos:**

### **1) RCMP Videos**

The Face of Fraud <https://www.youtube.com/watch?v=0rIWUcc57dM>

French: <https://www.youtube.com/watch?v=cXXP35rICQY>

A Cry from the Heart from Victims

<https://www.youtube.com/watch?v=blyhHl8rc7g>

French: <https://www.youtube.com/watch?v=cHZfvpH2YW8>

Telemarketing Fraud: The Seamy Side

<https://www.youtube.com/watch?v=t7bhQJkelEg>

French: [https://www.youtube.com/watch?v=XteG\\_fdasdw](https://www.youtube.com/watch?v=XteG_fdasdw)

### **2) OPP Videos**

Fraud Prevention Month Playlist

<https://www.youtube.com/playlist?list=PLbecW3cjtFJ4gxFvi9vuGIh8hJR13y1-c>

Senior Internet Scams Playlist

[https://www.youtube.com/playlist?list=PLbecW3cjtFJ6jyMpBlS\\_Y1NQkrj0-59Kp2](https://www.youtube.com/playlist?list=PLbecW3cjtFJ6jyMpBlS_Y1NQkrj0-59Kp2)

French: <https://www.youtube.com/user/OPPCorpCommFR/search?query=fraude>

### **3) Competition Bureau of Canada Videos**

Mass marketing fraud can take many forms. These videos help describe the way they work and how to avoid victimization. Videos are available in both official languages.

<https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04272.html>

<https://www.bureaudelaconcurrency.gc.ca/eic/site/cb-bc.nsf/fra/04272.html>

### **4) CAFC Fraud Prevention Video Playlists**

<https://www.youtube.com/channel/UCnvTfqttCb4K6wyVC6rMJkw/playlists>

## About the CAFC

The CAFC is Canada's central repository for information about fraud. We help citizens and businesses:

- report fraud;
- learn about different types of fraud;
- recognize the warning signs of fraud;
- protect themselves from fraud.

The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies by identifying connections all over the world. Our goals include:

- disrupting crime;
- strengthening the partnership between the private and public sectors;
- maintaining Canada's economy.

The CAFC is jointly managed by the [Royal Canadian Mounted Police](#), the [Competition Bureau](#), and the [Ontario Provincial Police](#).

### **Fraud: Recognize, Reject, Report.**

Many frauds today are designed to play on a potential victim's emotions and get them to respond without thinking. They attempt to illicit responses based on panic, fear, desperation, elation, love which are often escalated by presenting urgent situations requiring immediate action. The slogan for fraud prevention is geared toward getting citizens in Canada to slow down and not react to potential fraud solicitations.

We encourage people to **recognize** that fraudsters are using every means at their disposal to target them; telephone, email, text messaging, social media, internet and mail. We ask that they change how they react to the unsolicited offers or demands.

**Rejecting** fraud involves protecting your personal information and money. Routine practices to develop include checking credit profiles, monitoring accounts for unauthorized activities, updating operating systems and antivirus software, and not doing business over the phone. We want people to slow down, to think about and assess the situation before reacting. This can involve saying no, doing

due diligence, researching and confirming information, and talking to family members and friends. We want to encourage people to take their time, and to scrutinize all offers and demands.

**Reporting** fraud means speaking up, even when no money was lost. Like other crimes, if fraud is not reported, we don't know what is happening and can't warn other people. The information from one fraud occurrence (a bank account, email address, virtual currency address, telephone number, etc) can be investigated and is useful in linking other occurrences. Moreover, reporting provides other opportunities for disruption. By reporting the information to the banks, money service businesses, email providers, telephone companies, dating websites, social media networks; steps can be taking to block or remove these fraudulent accounts and their content.

- **Fraud Prevention Checklist:** A few questions to ask yourself every time you are contacted for personal information. If any of the following apply, do not provide your information and seek advice.

- Is the call unsolicited? Was it expected or out of the blue?
- Are they asking you to confirm personal information such as your name, address, or account details?
- Is there a chance they could be impersonating someone?
- Are they looking for a fast or instant response?
- Do you feel pressured?
- Are they asking you for money?
- Is the caller avoiding using the actual name or the company or financial institution?
- Are they offering you a prize, inheritance, free gift, or trial?
- Are they claiming to be the police or investigating something?
- Does the email have an odd email address?

## **Reporting Fraud**

**It is estimated that fewer than 5% of victims file a fraud report with the CAFC.**

Fraud is evolving. A fraud can often carry on over an extended period of time and is a crime that is difficult to recognize and report. If you are a victim of fraud –

### **Collect your thoughts**

Stay calm. Gather all information about the fraud, including:

- documents
- receipts
- copies of emails and/or text messages
- write a chronological list of what happened while it is fresh in your mind.
- Start a log of dates, times, who you reported this to and what they said.

### **Contact your financial institutions**

Report the incident to the financial institution that transferred the money.

If you're a victim of identity fraud:

- place flags on all of your accounts
- change all of your passwords
- use 2 factor authentication where possible
- report the fraud to both credit bureaus ([Equifax](#) and [TransUnion](#))

### **Contact the police**

Report the incident to your local police, let them know you are a senior victim of fraud and want to file a report, have all your documents with you. Ask for a file number for future reference. If you find any further suspicious activity after reporting, update your file with the police.

### **Report the incident**

Contact the **Canadian Anti-Fraud Centre** toll free at 1-888-495-8501 or online through the [Fraud Reporting System](#).

Depending on the type of fraud, or how it occurred, you'll also want to report it to other organizations involved.

### **Fraud that took place online through a website**

Report the incident directly to the administrators of the website. You can do so through a link such as "Report Abuse" or "Report an Ad".

### **Redirected mail**

If you suspect that someone had your mail re-directed, contact [Canada Post](#).

You should also notify your service provider (telephone, cell phone, electricity, water, gas, etc.) of the identity fraud.

### **Protect yourself from future fraud**

Scammers often target victims of fraud a second or third time with the promise of recovering money. Always do your due diligence and never send recovery money.

Scammers will often sell a victim's personal information to other scammers who are looking for a good and trusting senior to target with a different scam.

Scammers use call-spoofing to mislead consumers. This technology is easily available. Never assume that the phone numbers appearing on your call display are accurate. Likewise, never assume that an incoming text, email, or messenger message has not been spoofed or altered. If it is asking you for personal information or money to be sent – don't be pressured.

Take the time to Verify Verify Verify the offer/demand with a trusted source before sending money or giving personal information.

The impact of criminal victimization is serious, throwing victims into a state of **shock, fear, anxiety** and **anger**. The emotional, physical, psychological and financial ramifications of crime can be devastating to victims. Coping with and recovering from victimization are complex processes. We encourage victims to reach out to their health care professionals, should they feel the need.

We encourage victims to talk to their family, friends, neighbours and co-workers about their experience. It may prevent someone else from becoming a victim.

## **Most Common Frauds & How to Protect Yourself**

Below are the most common frauds targeting senior Canadians:

### **Extortion**

Extortion happens when someone unlawfully obtains money, property or services from a person, entity or institution through coercion.



*Impersonation:* The consumer receives a call claiming to be from their police or government agency. The fraudster demands personal information and an immediate payment, typically via gift cards, wire transfer or Bitcoin, or else –they may be arrested or deported for illegal activity.

*Ransomware:* A type of malware designed to infect or block access to a system or data. A device can be infected by a malware in a number of ways; but, most commonly, it starts with a victim clicking on a malicious link or attachment. At present, the most common form of ransomware will encrypt data. Once the system or data is infected, victims will receive the demand for ransom. There may also be threats of distributing the data publicly if the ransom is not paid.

### **Warning Signs – How to Protect Yourself**

- A government agency or a law enforcement agency would never call and threaten you.
  - No government or law enforcement agency will request payment by Bitcoin, a money service business, or gift cards (ie. iTunes, Google Play, Steam).
  - Use aggressive language or threaten you with arrest or sending the police

- Leave voicemails that are threatening or ask for personal or financial information
- No government agency will contact you and tell you that your SIN is blocked or suspended, nor will they threaten you with legal action.
- How to recognize government frauds:  
<https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud.html>
- Be familiar with your service provider's terms of service.
- Contact your service provider directly and verify that your account is in good standing.
- Do not open unsolicited emails and text messages.
- Do not click on suspicious links or attachments.
- Regularly back-up important files.
- Keep your operating system and software updated.
- Paying a ransom request does not guarantee that your files and devices will be restored. Fraudsters may continue to request additional funds.
- Have your system reviewed by local technicians.

### **Romance**

Fraudsters use every type of dating or social networking site available to contact their victims. Their accounts are created using photos stolen from legitimate people. Their background stories often mimic the victim's and they are often in the military, work overseas, or are successful business people. They quickly profess their love to gain their victims' trust, affection, and money. This type of fraud relies heavily on victim emotions and may last for months, years, or until the victim has nothing left to give. The fraudsters will always run into trouble and are unable to refund their victims; however, they will continue to make empty promises and ask for more money.



### **Warning Signs - How to Protect Yourself**

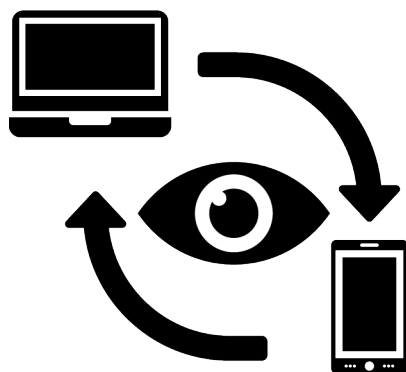
- Beware of individuals quickly professing their love for you.
- Beware of individuals who claim to be wealthy, but need to borrow money.

- When trying to setup an in-person meeting, be suspicious if they always provide you with reasons to cancel. If you do proceed, meet in a public place and inform someone of the details.
- Never send intimate photos or video of yourself as they may be used to blackmail you.
- Never send or accept money under any circumstances. You may, unknowingly, be participating in money laundering which is a criminal offence. This is referred to as being a Money Mule.

### **Service**

These frauds often involve offers for telecommunications, internet, finance, medical, and energy services. In addition, extended warranties, insurance and sales services may also fall under this category.

***Tech Support:*** Consumers receive a pop-up or a call claiming to be from a well-known tech company (e.g. Microsoft or Windows). The computer is said to be infected with malware or viruses, or that someone is attempting to hack it. The fraudster will offer to resolve the issue by gaining remote access to the computer. This allows them the opportunity to steal your personal information.



***Lower Interest Rate:*** Fraudsters call consumers to offer a reduced interest rate on their credit card. The goal of the fraud is to collect the consumer's personal and credit card information.

***Home Repairs & Products:*** Home owners are offered services at lower prices. These services can include air duct cleaning, furnace repairs, water treatment systems, or home renovations. If the services are completed at all, they are of low quality, offer impractical warranties or can cause further

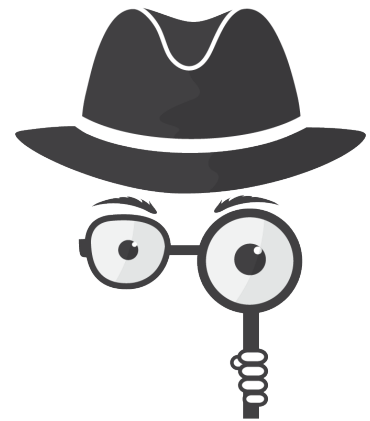
damage.

### **Warning Signs - How to Protect Yourself**

- Never allow an individual to remotely access your computer. If you are experiencing problems with your operating system, bring it to a local technician.
- Verify any incoming calls with your credit card company by calling the number on the back of the card. Be sure to end the original call and wait a few minutes before dialing.
- Never provide any personal or financial information over the telephone, unless you initiated the call.
- Only a credit card company can adjust the interest rate on their own product.
- Research all companies and contractors offering services before hiring them.

### **Bank Investigator**

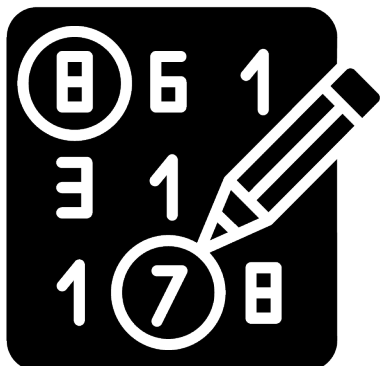
Fraudsters call consumers claiming to be a financial institution or a major credit card provider. To prove the legitimacy of the call, the fraudsters often ask the consumer to end the call and immediately call the number on the back of their card. The fraudsters then inform the consumer that they are investigating unauthorized activity on their account. The fraudsters ask the consumer to help them catch the criminal. By providing remote access to their device, the fraudsters will claim to put money into the victim's account so that they can send *bait money*. Unfortunately, the funds seen going into the victim's account are coming from their other accounts and the money being sent is going directly to the fraudsters.



### **Warning Signs - How to Protect Yourself**

- Typically, these calls tend to happen early in the morning. Always make sure you are alert when dealing with finances.
- If you end a call on a landline phone and immediately dial another call, the original call may not be completely disconnected. Wait a few minutes or use another phone to complete another call.
- Never provide personal or financial information over the phone unless you called your financial institution.
- Financial institutions will never ask for assistance from the public for internal investigations. They will also never ask you to transfer money to an external account for security reasons.
- Never provide remote access to your device to unknown callers.

## Prize



Consumers are informed that they are the winner of a large lottery or sweepstake even though they have never purchased a ticket or entered to win. Prior to receiving any winnings, the victim will be asked to pay a number of upfront fees. No winnings are ever received.

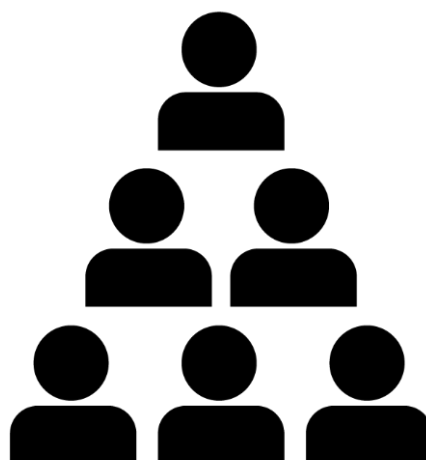
A variation of this fraud includes the consumer receiving a message from one of their friends on social media. The friend shares that they won a prize and asks the consumer if they have already collected their prize as they noticed their name was also on the winner's list. The consumer's friend encourages them to contact the person responsible for delivering the prizes. Unfortunately, unbeknownst to the victim, their friend's social account has been compromised and they have been communicating with the fraudster the entire time.

## **Warning Signs/ How to Protect Yourself**

- Never give out personal or financial information to strangers.
- The only way to participate in any foreign lottery is to go to the country of origin and purchase a ticket. A ticket cannot be purchased on your behalf.
- In Canada, if you win a lottery, you are not required to pay any fees or taxes in advance.

## Investment

Any false, deceptive, misleading or fraudulent investment opportunity, often offering higher than normal or true monetary returns. Victims often lose most or all of their money. Investors run the added risk of having their identity stolen, accumulating losses for unauthorized withdrawals on their credit cards and incurring high interest payments on investments that do not exist.



**Pyramids:** Similar to a Ponzi scheme, a pyramid scheme focuses primarily on generating profits by recruiting other investors. A common pyramid scheme today takes the form of a *gifting circle*. Participants gift a sum of money to join and ultimately must recruit others to make their money back. These schemes may offer products, but they usually have very little value. Pyramid schemes are illegal in Canada. It's a criminal offence to establish, operate, advertise or promote a pyramid scheme.

### Warning Signs – How to Protect Yourself

- Be careful when asked to provide personal or financial information to reclaim your investment profits.
- Beware of opportunities offering higher than normal returns.
- Beware of any urgency pressuring you to make an investment so that you don't miss out.
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project. Check the registration and enforcement history.
- The Canadian Securities Administrators (CSA) encourages all investors to use their 'Investor Tools' to verify if a company is registered [www.securities-administrators.ca](http://www.securities-administrators.ca)

### Personal Information & Phishing

Fraudsters impersonate financial and government agencies and contact consumers requesting their personal and banking information. Traditional phishing emails and text messages are designed to trick the victim into thinking they are dealing with a reputable company (e.g. financial institution, service provider, government). Phishing messages will direct you to click a link for various reason, such as, updating your account information, unlocking your account, or accepting a refund. The goal is to capture personal and/or financial information, which can be used for identity fraud.



### Variation: Spear Phishing

Spear phishing scams involve scammers pretending to be from a friend or acquaintance. The fraudster asks them for a favour and convinces them to buy gift cards on their behalf—because they are out of town. They promise to reimburse them asap. The victim is instructed to buy approx. \$200 in gift cards (i.e. Google Play or iTunes cards, etc.), then is told to scratch and give the codes off the back of the gift cards to the fraudster. Only to find out later that their friend and or acquaintance did not send the email. These scams leverage existing relationships between the person receiving the email and the person sending it. The sender's address appears to be the actual email address of the source they're pretending to be, a tactic known as spoofing.

### Warning Signs - How to Protect Yourself

- Let unsolicited calls go to voicemail.
- Fraudsters use call-spoofing to mislead consumers. This technology is easily available. Never assume that the phone numbers appearing on your call display are accurate.
- Do not open or click the link in unsolicited emails or text messages.
- Look for spelling and formatting errors.
- Verify the hyperlink behind the link's text or button by hovering over the text.
- Do not click on any suspicious attachments as they can contain malware.

Contact your friend / acquaintance by another method i.e. phone and ask if they sent you the email, asking for a favour.

### Emergency (Help)

Any phone call or email from someone claiming to be a friend or family member who is in some kind of trouble and requires money immediately.



Fraudsters will call seniors claiming to be a close relative of friend. They will have the consumer confirm which one by asking them if they recognize who's calling. From there, fraudsters will claim that there has been an accident and they require money immediately. Common incidents include an at-fault car accident where the

other victim was in a rental and on their way to the airport, an at-fault car accident where they were under the influence, and being stranded out of the country. A law enforcement or medical representative may be added to the phone call to help build legitimacy and urgency to the call. The funds are said to cover medical expenses, bail, bribe law enforcement to sweep everything under the rug or allow the person to make it back home. The fraudsters will ask the consumer to keep everything a secret. They may also claim that they will reimburse the consumer the next time they see them.

### **Warning Signs – How to Protect Yourself**

- Fraudsters use call-spoofing to mislead consumers. This technology is easily available. Never assume that the phone numbers appearing on your call display are accurate.
- A family member requests money urgently and provides instructions on how to proceed.
- Do not volunteer information over the phone; wait for the caller to provide it. Some families use code words to confirm their identity.
- Confirm with other relatives the whereabouts of the family member or friend.
- Law enforcement and other legal entities will never make urgent requests for money.

### **Merchandise**

Fraudsters may place advertisements on popular classified sites or social networks. They may also create websites that share the look and feel of legitimate manufacturers. Fraudsters will generate traffic to their products by advertising them at deep discounts. Consumers may receive counterfeit products, lesser valued & unrelated goods, or nothing at all.

*Animal for Free:* Fraudsters will often advertise animals for free; puppies and kittens are used most often. They will claim that the animal is free; however, the victim will be required to pay shipping. Once the payment is received, the fraudsters will begin to request additional payments for: transportation cage, vaccinations, medication, insurance, customs and brokerage fees, etc.



### **Warning Signs/ How to Protect Yourself**

- If it sounds too good to be true, it probably is.
- Beware of pop-ups that direct you away from the current website.
- Consumers should verify the URL and seller contact information.
- Search for any warnings posted online and read reviews before making a purchase.
- Spelling mistakes and grammatical errors are other indicators of a potentially fraudulent website.
- Use a credit card when shopping online. Consumers are offered fraud protection and may receive a refund. If you have received anything other than the product you ordered, contact your credit card company to dispute the charge.

### **Recovery Pitch**

If you have been victimized in the past, you are likely to be contacted again by someone promising to get your money back. The imposter may claim to be an investigating agency, law enforcement representative or lawyer. The fraudster will claim a recent investigation has found a guilty party and money was recovered from a previous scam. Often, victims are promised a portion or all of their lost funds, only if legal fees and taxes are paid. Scammers may purchase “lead lists”, which include your information and involvement in past scams.



## Warning Signs - How to Protect Yourself

- If you are the victim of a scam, you are likely to be called again by someone promising you a refund. Be careful not to lose more money.
- No government or law enforcement agency will ask you to participate in a sting operation to recover your lost funds.
- Do not pay money to get money.

Throughout the year, the CAFC will be using the **#kNOwfraud** and **#ShowmetheFRAUD** descriptors to link fraud prevention messaging. We encourage everyone to be mindful of these strategies. As well **#Take5** and **#Tell2** - protect many. Take Five encourages consumers to pause, reflect and not react under the pressure of fraudsters. **#Tell2** is a movement that asks consumers to prevent fraud by sharing anti-fraud messaging with at least two people and encouraging them to do the same. ***An unbroken chain of 25 Tell2'ers would cover the entire population of Canada.***



Seniors can report mass marketing fraud and ID fraud directly to the CAFC through our website <https://www.antifraudcentre.ca> under the heading 'Report Fraud' or call in on our toll free at **1-888-495-8501**. Our phone lines are open 9-4:30pm EST Monday to Friday.

Please report:

- unsolicited phone calls to the Do Not Call list registry: call 1-866-580-3625 or visit their website [www.lnnte-dncl.gc.ca](http://www.lnnte-dncl.gc.ca)
- SPAM to the SPAM Reporting Centre: [www.fightspam.gc.ca](http://www.fightspam.gc.ca)