



**2020 Fraud Prevention Toolkit:  
Middle Aged**

**#KNOWFRAUD**  
**#SHOWMETHEFRAUD**  
**Fraud: Recognize. Reject. Report.**



## Table of Contents

<b>Introduction</b>	---	3
RCMP Videos	---	4
OPP Videos	---	4
Competition Bureau of Canada Videos	---	4
CAFC Fraud Prevention Video Playlists	---	4
CAFC Logo	---	4
Calendar of Events	---	5
Statistics	---	6
Reporting Fraud	---	7
<b>Common Frauds Targeting Middle Aged</b>	---	7
• Extortion	---	7
• Romance	---	8
• Investment	---	9
• Merchandise	---	10
• Service	---	11
• Phishing & Smishing	---	12

## Introduction



The Canadian Anti-Fraud Centre (CAFC) has compiled a toolkit specifically designed for middle age (from 30 to 59) Canadians to further raise public awareness and prevent victimization. We encourage all our partners to use the resources in this toolkit on their website, in print and on their social media platforms.

Throughout the year, the CAFC will be using the #kNOwfraud and #ShowmetheFRAUD descriptors to link fraud prevention messaging. We encourage our partners to make use of these hashtags as well as #Take5 and #Tell2, protect many. Take Five is a successful national campaign that was first launched by UK Finance; it encourages consumers to pause, reflect and not react under the pressure of fraudsters. #Tell2 is a movement that was started by D.C. Tony Murray from Durham Fraud (UK). The initiative 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.

During Fraud Prevention Month (March), the CAFC will post daily on its Facebook and Twitter platforms (#FPM2020). Our weekly bulletin will be published every Monday and, every Wednesday, we will host a #FraudChat at 1PM Eastern on Twitter. Everyone is invited to join the conversation.

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 piece that completes the puzzle.

Consumers and businesses can report directly to the CAFC through our online [Fraud Reporting System](#) (FRS) or toll free at 1-888-495-8501.

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

Thank you,  
The CAFC Fraud Prevention Team

Follow us on Twitter – [@canantifraud](#)  
Like us on Facebook – [Canadian Anti-Fraud Centre](#)



## This Toolkit Includes:



### 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=PLbecW3cjtFJ4gxFvi9vuGlh8hJR13y1-c)  
<https://www.youtube.com/playlist?list=PLbecW3cjtFJ4gxFvi9vuGlh8hJR13y1-c>
- Senior Internet Scams Playlist  
<https://www.youtube.com/playlist?list=PLbecW3cjtFJ6iyMpBlS 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.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04272.html>

### 4) CAFC Fraud Prevention Video Playlists

- <https://www.youtube.com/channel/UCnvTfqtCb4K6wyVC6rMJkw/playlists>

### 5) CAFC Logo



## 6) Calendar of Events



Throughout the month of March, the CAFC will release a bulletin every Monday. Every Wednesday, we will host a Twitter #FraudChat at 1PM (Eastern). Both will be based on the following weekly fraud prevention themes:

**Week 1:** Fraud initiated by direct call

**Week 2:** Fraud initiated by email or text message

**Week 3:** Fraud initiated online

**Week 4:** Fraud initiated on social media

**Week 5:** Fraud initiated by mail or in person

On a daily basis, the CAFC will highlight a “Fraud of the Day” on our social network accounts. See the calendar below for more details.

On **March 2, 2020** - Join us on Facebook for a live 13-hour Canada-wide Fraud Prevention Month launch event.

### March 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1 Tools used by Fraudsters	2 <b>13-HR LIVE LAUNCH</b>  <b>Bulletin</b>	3 Personal Information	4 Charity  <b>#Fraudchat</b>	5 Payment Methods	6 Prize	7 Vacation
8 Phishing	9 ID Theft & Fraud  <b>Bulletin</b>	10 Spear Phishing	11 Extortion  <b>#Fraudchat</b>	12 Ransomware	13 SIM Swap	14 Emergency
15 Subscription Traps	16 Job  <b>Bulletin</b>	17 Sale of Merchandise	18 Merchandise  <b>#Fraudchat</b>	19 Card-Not-Present	20 Investment	21 Rental
22 Stay Safe Online	23 Puppy  <b>Bulletin</b>	24 Service	25 Pyramid  <b>#Fraudchat</b>	26 Grant	27 Romance	28 Sextortion
29 Inheritance	30 Overpayments  <b>Bulletin</b>	31 Brand Protection	April 1 Fraud is no joke  <b>#Fraudchat</b>			

Like us on Facebook – [Canadian Anti-Fraud Centre](#)

Follow us on Twitter – [@canantifraud](#)

## 7) Statistics



In 2019, the CAFC received 46,465 fraud reports from Canadian consumers and businesses. The total reported Canadian losses were \$96,163,328.64. The top 10 frauds reported during this time are listed below.

Top 10 frauds affecting middle agers based on number of reports in 2019:

Fraud Type	Reports	Victims	Dollar Loss
Extortion	5,198	977	\$2,399,174.29
Personal Info	3,665	2,620	
Phishing	2,029	559	
Service	1,333	709	\$2,261,944.47
Merchandise	1,221	867	\$1,471,023.97
Sale of merchandise	755	470	\$626,691.03
Job	744	265	\$762,626.81
Romance	497	334	\$6,071,048.79
Prize	334	87	\$319,607.69
Loan	327	226	\$877,878.22

Top 10 frauds affecting middle agers based on dollar loss in 2019:

Fraud Type	Reports	Victims	Dollar Loss
Investments	191	161	\$7,092,618.26
Romance	497	334	\$6,071,048.79
Extortion	5,198	977	\$2,399,174.29
Service	1,333	709	\$2,261,944.47
Merchandise	1,221	867	\$1,471,023.97
Loan	327	226	\$877,878.22
Job	744	265	\$762,626.81
Sale of merchandise	755	470	\$626,691.03
Timeshare	32	25	\$392,721.05
Prize	334	87	\$319,607.69

➔ Is it estimated that fewer than **5%** of victims file a fraud report with the CAFC.

## 8) Reporting Fraud

In an effort to mitigate the impact of fraud, the CAFC suggests following the six steps below.



**Step 1:** Gather all information pertaining to the fraud.

**Step 2:** Report the incident to your local law enforcement.

**Step 3:** Report the incident to the CAFC through the [Fraud Reporting System](#) (FRS) or toll free at 1-888-495-8501.

**Step 4:** Report the incident to the Financial Institution or Payment Provider used to send the money.

**Step 5:** If the fraud took place online, report the incident directly to the appropriate website.

**Step 6:** Follow the RCMP Identity Theft and Fraud Assistance Guide:

<http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm>

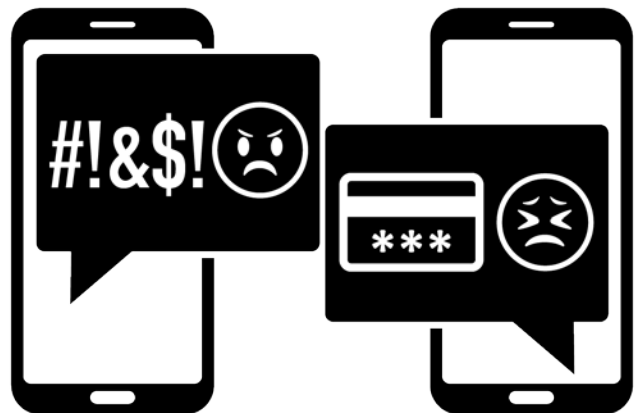
## 9) Common Frauds & How to Protect Yourself

Below are a few common frauds affecting middle agers:

### Extortion

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

*SIN Scam:* Consumers are receiving recorded messages about their Social Insurance Number (SIN) being linked to fraudulent or criminal activity. The fraudsters are claiming to be different federal government agencies and stating that the SIN has been blocked, compromised or suspended. There may be threats of an arrest warrant or imprisonment, if the consumer does not cooperate with the fraudster's demands. They may request personal information (SIN, DOB, address etc.) or request that consumers empty their bank accounts and deposit the funds elsewhere. The fraudsters claim to want to clear the money from illegal activity and that it will be returned once their investigation is complete.





## 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.
- No government agency will contact you and tell you that your SIN is blocked or suspended, nor will they threaten you with legal action.
- Never provide personal information over the phone to an unknown caller.
- No government or law enforcement agency will demand an immediate payment or to submit all of your money for investigation.
- No government or law enforcement agency will request payment by Bitcoin, a money service business, or gift cards (ie. iTunes, Google Play, Steam).
- How to recognize the CRA fraud: <https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud.html>



## 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.



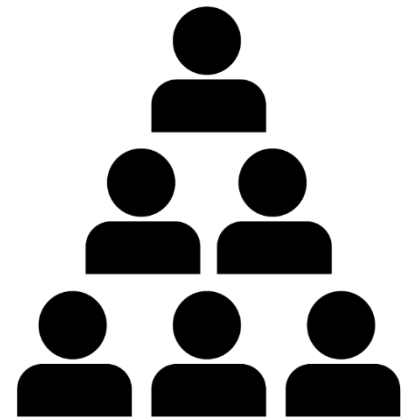
## Investment



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.

*Initial Coin Offerings:* The virtual currency market is constantly changing. New virtual currencies are developed monthly. Like an Initial Public Offering (IPO), an Initial Coin Offering (ICO) is an attempt to raise funds to help a company launch a new virtual currency. In an ICO fraud, the fraudsters solicit investment opportunities with fake ICOs. They provide official looking documentation, use buzz words and may even offer a real "token". In the end, everything is fake, and you lose your investment.

*Pyramids:* Similar to a Ponzi scheme, a pyramid scam focuses primarily on generating profits by recruiting other investors. A common pyramid scam 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 selling is illegal in Canada. It's a criminal offence to establish, operate, advertise or promote a scheme of pyramid selling.

### 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 visit their National Registration Search Tool ([www.aretheyregistered.ca](http://www.aretheyregistered.ca)).

## 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.

*Vehicle for Sale:* Vehicles are advertised at a lower than average price. Fraudsters claim to be located overseas and a third-party agency will deliver the vehicle. The victim is asked to submit payments for the vehicle and delivery. Nothing is ever delivered.



*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.

## Service

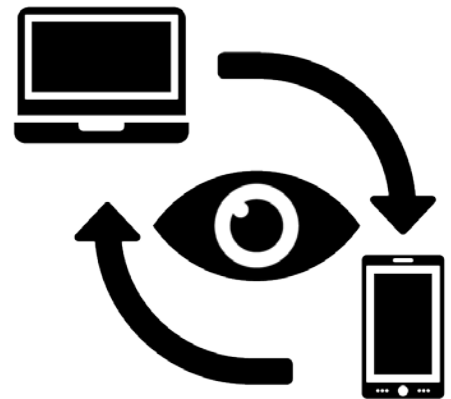
These frauds often involve offers for telecommunications, internet, finance, medical, and energy services. In addition, extended warranties, insurance and sales services may also fall under this category.



*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.

## Phishing & Smishing



Traditional phishing emails and smishing text messages are techniques designed to trick the victim into thinking they are dealing with a reputable company (i.e. financial institution, service provider, government). Phishing/Smishing 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.

### Warning Signs - How to Protect Yourself

- 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 links as they can contain malware.

Canadian Anti-Fraud Centre



Centre antifraude du Canada

**FRAUD: RECOGNIZE IT. REPORT IT. STOP IT. LA FRAUDE : IDENTIFIEZ-LA. SIGNALEZ-LA. ENRAYEZ-LA.**



Competition Bureau  
Canada Bureau de la concurrence  
Canada



Royal Canadian  
Mounted Police Gendarmerie royale  
du Canada



Canada 100