CANADIAN ANTI-FRAUD CENTRE BULLETIN

2021 Fraud Prevention Toolkit – Young Adults 2021-02-15

FRAUD: RECOGNIZE, REJECT, REPORT

YOUNG ADULTS

2021 Fraud Prevention Toolkit

Royal Canadian Mounted Police | Gendarmerie royale du Canada | Competition Bureau Canada | Bureau de la concurrence Canada | Ontario Provincial Police | Canada

Table of Contents

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.

March is Fraud Prevention Month. This year's efforts will focus on the Digital Economy of Scams and Frauds.

The Canadian Anti-Fraud Centre (CAFC) has compiled a toolkit specifically designed for young adult Canadians (born 1987-2005) to further raise public awareness and prevent victimization. We encourage all our partner 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 will also continue to use the slogan "Fraud: Recognize, Reject, Report".

During Fraud Prevention Month, the CAFC will post daily on its Facebook and Twitter platforms (#FPM2021). Our weekly bulletin will be published every Monday and, every Wednesday, we will host a #FraudChat at 1 p.m. (Eastern Time) on Twitter. Everyone is invited to join the conversation.

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

Thank you,

Your 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=0rlWUcc57dM
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

2) OPP Videos

Fraud Prevention Month Playlist
https://www.youtube.com/playlist?list=PLbecW3cjtFJ4gxFvi9vuGlh8hJR13y1-c
Senior Internet Scams Playlist
https://www.youtube.com/playlist?list=PLbecW3cjtFJ6jyMpBlsY1NQkrj0-59Kp2
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/UCnvTfqttCb4K6wyVC6rMJkw/playlists

5) CAFC Logo

6) Calendar of Events

Throughout the month of March, the CAFC will release a bulletin every Monday aimed at Recognizing Fraud and highlighting our weekly themes tied to the Digital Economy of Scams and Fraud. Every Wednesday, we will host a Twitter #FraudChat at 1 p.m. (Eastern Time) providing advice on breaking the contact with fraudsters.

Bulletins
Week 1: Buying and Selling Online
Week 2: Online Financial Scams
Week 3: Securing Your Accounts and Your Identity
Week 4: Email Scams
Week 5: Online Scams

Fraud Chats
Week 1: Fraud initiated by telephone call
Week 2: Fraud initiated by email or text message
Week 3: Fraud initiated online
Week 4: Fraud initiated on social networks
Week 5: Fraud initiated by mail or in person

On a daily basis, the CAFC will highlight a fraud topic on our social media accounts.
Like us on Facebook – Canadian Anti-Fraud Centre
Follow us on Twitter – @canantifraud

On **March 2, 2021** - Join us on Facebook for a live 13-hour Canada-wide Fraud Prevention Month launch event.

March 2021

Mon., March 1 Facebook & Twitter Bulletin - Buying & Selling Online	**Tues., March 2** Facebook **13-HR LIVE LAUNCH**	**Wed., March 3** Facebook & Twitter Puppy Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 4** Facebook & Twitter Rental Scams	**Fri., March 5** Facebook & Twitter Merchandise and Counterfeit scams
Mon., March 8 Facebook & Twitter Bulletin -Financial Scams	**Tues., March 9** Facebook & Twitter Investment Scams	**Wed., March 10** Facebook & Twitter Loan Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 11** Facebook & Twitter Grant Scams	**Fri., March 12** Facebook & Twitter Job Scams
Mon., March 15 Facebook & Twitter Bulletin -Protecting Your Information	**Tues., March 16** Facebook & Twitter Id Theft and Fraud	**Wed., March 17** Facebook & Twitter Social Media Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 18** Facebook & Twitter Securing your Accounts	**Fri., March 19** Facebook & Twitter Ransomware
Mon., March 22 Facebook & Twitter Bulletin – Email and Text Message Scams	**Tues., March 23** Facebook & Twitter Phishing	**Wed., March 24** Facebook & Twitter Spear Phishing **1 p.m. Eastern** #Fraudchat	**Thurs., March 25** Facebook & Twitter Extortion Scams	**Fri., March 26** Facebook & Twitter Prize Scams
Mon., March 29 Facebook & Twitter Bulletin – Prevalent Online Scams	**Tues., March 30** Facebook & Twitter Romance Scams	**Wed., March 31** Facebook & Twitter Immigration scams **1 p.m. Eastern** #Fraudchat	**Thurs April 1** Facebook & Twitter Fraud is no joke	

7) 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.

8) Statistics

In 2020, the CAFC received 101,483 fraud reports involving nearly $160 million in reported losses. Moreover, 16,340 of the reports were from young adult Canadians, that reported losses totalling more than $16.6 million.

2020 young adult Canadians Top 10 frauds based on number of reports:

Fraud Type	Reports	Victims	Dollar Loss
Identity Fraud	4,772	4,772	N/A
Extortion	4,114	2,295	$4.6 M
Personal Info	1,894	1,426	N/A
Job	1,031	573	$0.9 M
Merchandise	974	834	$0.8 M
Vendor Fraud	832	688	$0.6 M
Phishing	717	371	N/A
Service	311	233	$0.3 M
Romance	139	103	$0.9 M
Investments	130	116	$1.8 M

Top 10 frauds affecting young adult Canadians based on dollar loss in 2020:

Fraud Type	Reports	Victims	Dollar Loss
Extortion	4,114	2,295	$4.6 M
Investments	130	116	$1.8 M
Job	1,031	573	$0.9 M
Romance	139	103	$0.9 M
Merchandise	974	834	$0.8 M
Vendor Fraud	832	688	$0.6 M
Service	311	233	$0.3 M
Loan	103	93	$0.2 M
Spear Phishing	116	91	$0.2 M
Prize	46	24	$83,000

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

9) Reporting Fraud

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. To make reporting easier the CAFC suggests completing the following six steps:

Step 1: Gather all information pertaining to the fraud.
Step 2: Write out a chronological statement of events.
Step 3: Report the incident to your local law enforcement.
Step 4: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 5: Report the incident to the Financial Institution or Payment Provider used to send the money.
Step 6: If the fraud took place online, report the incident directly to the appropriate website.

10) Most Common Frauds & How to Protect Yourself

Below are the most common frauds affecting young adult Canadians:

Identity Theft and Identity Fraud
A victim of identity fraud has previously been the victim of identity theft.

Identity theft occurs when a victim's personal information is stolen or compromised. This can happen as a result of volunteering personal or financial information, a phishing fraud, a stolen wallet, a database breach, etc.

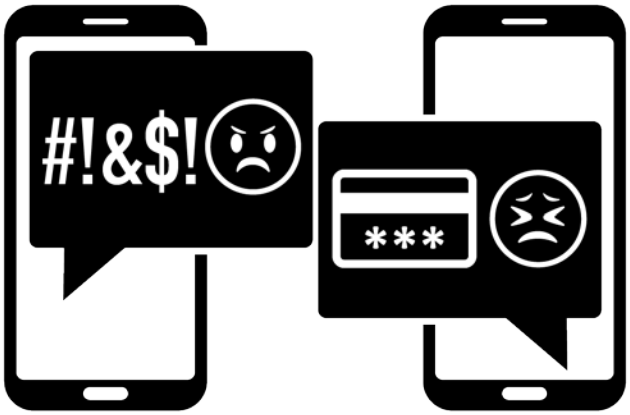
Identity fraud occurs when the fraudster uses the victim's information for fraudulent activity. Fraudsters may create fake identity documents, submit unauthorized credit applications and open financial accounts in your name, re-route your mail, purchase mobile phones, takeover your existing financial and social accounts, etc.

If you are a victim of identity theft and/or fraud, you should immediately complete the following steps:

- **Step 1:** Gather the information pertaining to the fraud.
- **Step 2:** Contact the two major credit bureaus to obtain a copy of your credit report and review with reports.
    - **Equifax Canada:** http://www.consumer.equifax.ca/home/en_ca, 1-800-465-7166
    - **TransUnion Canada:** http://www.transunion.ca, 1-877-525-3823
- **Step 3:** Report the incident to your local law enforcement.
- **Step 4:** Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
- **Step 5:** Review your financial statements and notify the affected agency if you notice any suspicious activity.
- **Step 6:** Notify your financial institutions and credit card companies, and change the passwords to your online accounts.
- **Step 7:** If you suspect that your mail has been redirected, notify Canada Post (www.canadapost.ca, 1-866-607-6301) and any service providers.
- **Step 8:** Notify federal identity document issuing agencies:
    - **Service Canada:** www.servicecanada.gc.ca, 1-800-622-6232
    - **Passport Canada:** www.passport.gc.ca, 1-800-567-6868
    - **Immigration, Refugees and Citizenship:** www.cic.gc.ca, 1-888-242-2100
- **Step 9:** Notify provincial identity document issuing agencies.

Extortion

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



Hydro: The business receives a call claiming to be from their hydro provider. The fraudster demands an immediate payment, typically via Bitcoin, or their power will be disconnected.

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

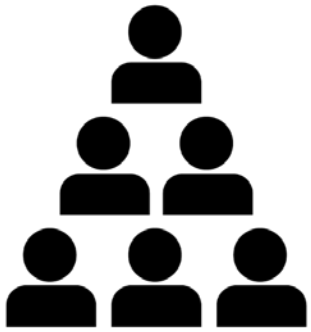
- Be familiar with your service provider's terms of service.
- Contact your service provider directly and verify that your account is in good standing.
- Do not open unsolicited emails and text messages.
- Do not click on suspicious links or attachments.
- Regularly back-up important files.
- Keep your 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 systems reviewed by local technicians.
- Report any database breach as per Canada's federal private sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA).

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).

Job

Fraudsters use popular job listing websites to recruit potential victims. The most common fraudulent job advertisements are for: Personal Assistant or Mystery Shopper, Financial Agent or Debt Collector, and Car Wrapping. In many cases, the fraudsters will impersonate legitimate companies.

Personal Assistant or Mystery Shopper: The victim receives a fake payment (unknowingly) with instructions to complete local purchases and send funds through a financial institution or a money service business. Victims are asked to document their experiences and evaluate customer service. Eventually, the payment is flagged as fraudulent and the victim is responsible for the money spent and sent to a third party.

Financial Agent, Administrative Assistant or Debt Collector: Consumers are offered a job that features a financial receiver/agent component. Victims are told to accept payments into their personal bank account, keep a portion, and forward the remaining amount to third parties. Victims are eventually informed that the original payment was fraudulent and any debts accrued are the responsibility of the victim. Fraudsters will attempt to process many payments in a short amount of time before the victim's financial institution recognizes the fraud.

Car Wrapping: Consumers receive an unsolicited text message promoting an opportunity for them to earn $300-$500 per week by wrapping their vehicle with advertisement. Interested victims are sent a fraudulent payment (unknowingly) with instructions to deposit and forward a portion of the funds to the graphics company. With time, the payment is flagged as fraudulent and the victim is responsible for the funds sent to a third party.

Warning Signs - How to Protect Yourself

- Be mindful of where you post your resume.
- Beware of unsolicited text messages offering employment.
- Most employers will not use a free web-based email address to conduct business.
- That the time to research a potential employer.

- Never use your personal bank account to accept payments from strangers.
- A legitimate employer will never send you money and ask you to forward or return a portion of it.

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.