Toolkit for March Fraud Prevention Month 2019

Young Adults

#KNOWFRAUD

FRAUD: Recognize. Reject. Report.

Table of Contents

Introduction

In preparation for March Fraud Prevention Month, the Canadian Anti-Fraud Centre (CAFC) has compiled a toolkit specifically designed for young adults to further raise public awareness and help prevent victimization. We encourage all partnering organizations to use the CAFC logo, contact points and resource materials in this toolkit on their website, in print and on their social media platforms. The CAFC will post daily on Facebook and Twitter (#FPM2019, #MPF2019) and be participating in the fraud chats: Use the following hashtag – #fraudchat – to join.

The CAFC is Canada's central repository for data, intelligence and resource material as it relates to mass marketing fraud and identity fraud. The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies all over the world by identifying connections among seemingly unrelated cases. Victims who report to the CAFC are also encouraged to report directly to their local police. Your information may provide the piece that completes the puzzle.

Young adult consumers can report directly to the CAFC by calling toll free 1-888-495-8501 or online through the CAFC Online Fraud Reporting System (FRS).

English - http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm

French - http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-fra.htm

Comments, questions or feedback on Fraud Prevention Month is always welcomed.

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**

- Face of Fraud Commercial (YouTube) - https://www.youtube.com/watch?v=0rlWUcc57dM
- A Cry from the Heart from Victims, Romance Scam (YouTube) - https://www.youtube.com/watch?v=blyhHl8rc7g – French video with English subtitles
- Telemarketing Fraud: The Seamy Side (YouTube) - https://www.youtube.com/watch?v=t7bhQJkelEg

2) **OPP Fraud Prevention Videos**

CAFC staff and volunteers highlight a number of well-known scams in these short videos. Videos are available in both official languages.

- English (YouTube) https://www.youtube.com/user/OPPCorpComm/search?query=scam
- French (YouTube) https://www.youtube.com/user/OPPCorpCommfr/search?query=scam

3) **Competition Bureau of Canada Fraud Prevention 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.

- English - http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04272.html
- French - http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/fra/04272.html

4) **CAFC Logo**

5) Calendar of Events - Facebook and Twitter "Scam of the Day"

Every day in March, the CAFC will highlight a particular scam on both Facebook and Twitter that will link directly to the CAFC website (information is available in both official languages). See the calendar of events below. Scams involving Young Adults will be highlighted in week 2.

March 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1 **Facebook & Twitter** Importance of Reporting	2
3	4 **Facebook & Twitter** Sale of Merchandise **Bulletin** Loan	5 **Facebook & Twitter** Phishing	6 **Facebook & Twitter** Personal Info	7 **Facebook & Twitter** Loan	8 **Facebook & Twitter** Job	9
10	11 **Facebook & Twitter** Extortion **Bulletin** Extortion	12 **Facebook & Twitter** Romance	13 **Facebook & Twitter** Investments	14 **Facebook & Twitter** Merchandise (Counterfeit)	15 **Facebook & Twitter** Vacation	16
17	18 **Facebook & Twitter** Emergency **Bulletin** Service	19 **Facebook & Twitter** Prize	20 **Facebook & Twitter** Service	21 **Facebook & Twitter** Bank Investigator	22 **Facebook & Twitter** Recovery Pitch	23
24	25 **Facebook & Twitter** Wire Fraud **Bulletin** Card Not Present	26 **Facebook & Twitter** Card Not Present	27 **Facebook & Twitter** Grant	28 **Facebook & Twitter** Directory	29 **Facebook & Twitter** Spear Phishing	30

Follow us on Twitter – @canantifraud
Like us on Facebook – Canadian Anti-Fraud Centre

6) Statistics

In 2018, the CAFC received 59,009 fraud reports from Canadian consumers and businesses. The total reported Canadian losses were $97,654,160.35. The top 10 reported scams affecting young adults during this time are listed below.

Top 10 young adult scams based on number of complaints in 2018:

Complaint Type	Reports	Victims	Dollar Loss
Extortion	3,299	470	$2,182,166.9
Identity Fraud	1,711	1,620	$2,119,557.81
Phishing	1,327	821	$23,166.96
Personal Info	922	625	$39,030.14
Sale of Merchandise	911	797	$474,977.09
Merchandise	583	462	$415,595.62
Job	519	209	$566,749.84
Service	372	211	$300,827.92
Counterfeit Merchandise	105	103	$33,756.57
Loan	99	76	$129,215.21

Top 10 young adult scams based on dollar loss in 2018:

Complaint Type	Reports	Victims	Dollar Loss
Extortion	3,299	470	$2,182,166.9
Identity Fraud	1,711	1,620	$2,119,557.81
Investments	42	30	$ 804,031.48
Job	519	209	$566,749.84
Sale of Merchandise	911	797	$474,977.09
Merchandise	583	462	$415,595.62
Service	372	211	$300,827.92
Romance	60	43	$154,190.37
Inheritance	10	4	$136,067.00
Loan	99	76	$129,215.21

➔ Fewer than **5%** of victims file a fraud report with the CAFC.

7) Fraud Warnings / Bulletins

Below are a few common frauds targeting young adults, which will be highlighted during week 2 of Fraud Prevention Month (March 4th – 8th).

Monday, March 4th, 2019 - **Scams Targeting Young Adults**
Bulletin: **Loan**

Sale of Merchandise

When selling merchandise online you need to be aware that not all offers received are good and honest. Consumers who are providing a service or selling merchandise may receive a fraudulent payment, often above asking price with instructions to forward the difference to a third party to complete the transaction (often a shipping company). Consumers who comply may lose the merchandise shipped and left responsible to repay the financial institution for any funds lost.

The scam involves an online transaction where the suspect suggests payment by PayPal, offering to pay extra if the victim will ship the merchandise. Victims who agree receive a spoofed PayPal email claiming the funds are available, however, can only be released once the victim confirms a tracking number. Victims who ship the merchandise are subsequently left without payment or goods.

Warning Signs - How to Protect Yourself

- Authenticate payments before shipping the goods.
- Scammers may use the word “item” instead of what is being sold.
- Beware when buyers try to change the shipping address at the last minute.
- Beware of overpayments with the request to send additional funds to a shipping agent.

Phishing

Traditional phishing emails are designed to trick the victim into thinking they are dealing with a reputable company. Emails are sent with the intentions of capturing personal information and/or financial information, which can be used for identity fraud. Common trends currently involve emails sent impersonating PayPal, Canada Revenue

Agency, Financial Institutions, and email providers. Victims who respond to these emails are encouraged to take the appropriate actions to protect their identity – contacting Equifax, TransUnion, Financial Institutions, local police, and the Canadian Anti-Fraud Centre.

Warning Signs - How to Protect Yourself

- 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.
- If an unsolicited email includes a hyperlink, do not click if you are suspicious.
- Beware of unsolicited emails from organizations asking you for your personal or financial information.

Personal Information

Any solicitation where an individual is asked for – or to verify – private and personal information. From bogus websites to cold calls asking for personal and financial information, fraudsters are employing numerous tactics to steal personal identities.

Warning signs—How to Protect Yourself

- Never provide your personal information over the telephone unless you initiated the call.
- Lock your financial documents and personal information in a safe place at home, and lock your wallet or purse in a safe place.
- Shred receipts, credit card offers, credit card applications, insurance forms, cheques, bank statements, and similar documents when you don't need them any longer.

Loan

Commonly, loan scam ads are found through online advertising or deceitful websites designed to look like a legitimate lending institution. Consumers who apply are asked to provide personal information, which can lead to ID fraud. Since all consumers are approved, fraudsters demand victims pay an upfront fee to secure the loan. Victims are assured the loan will be deposited into

their account within 24 hours of sending the fees. Once a victim sends money, communication with the fraudster usually stops and no money is ever received.

Warning Signs - How to Protect Yourself:

- If you are asked to make payments via email money transfer, money service business, or pre-paid credit cards cease all contact immediately.
- It is illegal for a company to request an upfront fee prior to obtaining your loan.
- Beware of companies offering a guaranteed loan even if you have bad or no credit.
- Contact consumer protection agencies and regulators to ensure that the company is a legitimate lender.
- Advertising through a recognized media outlet does not ensure that the ad was placed by a legitimate company.

Job

Scammers utilize popular websites like Kijiji, Craigslist, Monster, Indeed, and Workopolis to recruit potential victims. The most common scams include the Mystery Shopper, Car Wrapping and HR/Administrative jobs.

Mystery Shopper: Consumers are offered a job in response to an online ad or in receipt of a text message. The victim receives a cheque in the mail with instructions to complete local purchases and send funds by MoneyGram or Western Union. Victims are told to document all experiences and evaluate customer service. Eventually, the cheque is returned as counterfeit and the "employee" is accountable to pay for the funds that were wired.

Car Wrapping: Consumers receive an unsolicited text message advising they can earn $300-$500 per week by wrapping their vehicle with a "company" logo. Victims who agree are mailed a cheque with instructions to deposit and forward a portion of the funds to a graphics company.

Consumers who comply are notified that the original cheque was counterfeit. Scammers will impersonate legitimate companies to make the job seem real.

HR/Administrative: Another common job scam involves the victim acting as a financial receiver/agent. Victims are told to accept payment in their personal account (often by eTransfer or cheque), keep a portion and forward the remaining amounts to third party "employees" or "companies". Victims are eventually advised the original payment was fake or fraudulent and any subsequent monies sent must be repaid at the victim's expense. Scammers will attempt to process as many payments before the victim's financial institution warns of the ongoing scam.

Warning Signs - How to Protect Yourself

- Be mindful of where you post your resume. Scammers use legitimate websites to seek out victims.
- A legitimate employer will never send funds and request a portion of it back.
- Do your research; open source searches could save you thousands of dollars.
- Never use your personal account to process payments from strangers.
- Beware of unsolicited text messages offering employment.
- Be wary when a "company" uses a web-based email address to conduct business.

If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or report online through the Fraud Reporting Tool (FRS) at http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm