Toolkit for March Fraud Prevention Month 2018

Young Adults

FRAUD: Recognize. Reject. Report.

Table of Contents

Introduction	---	3
RCMP Videos	---	4
OPP Fraud Prevention Videos	---	4
Competition Bureau Fraud Prevention Videos	---	4
CAFC Logo	---	4
Calendar of Events - Facebook and Twitter	---	5
Statistics	---	6
Theme 2: Scams Targeting Young Adults	---	7
• Buying Online - Counterfeit Goods	---	7
• Job	---	8
• Phishing	---	9
• Sale of Merchandise	---	9
• Merchandise	---	10

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 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 actively be posting on Facebook and Twitter daily (#FPM2018, #MPF2018) and 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. Victims who report to the CAFC are also encouraged to report directly to their local police. 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. Your information may provide the piece that completes the puzzle. The CAFC is a support agency to law enforcement.

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/03809.html#tab2
- French - http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03809.html#tab2

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 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1 **Facebook & Twitter** Introduction to #FPM2018 **Bulletin** What to do if you're a victim	2 **Facebook & Twitter** Importance of Reporting	3
4	5 **Facebook & Twitter** Counterfeit **Bulletin** Continuity Scams	6 **Facebook & Twitter** Phishing	7 **Facebook & Twitter** Merchandise	8 **Facebook & Twitter** Job	9 **Facebook & Twitter** Sale of Merchandise	10
11	12 **Facebook & Twitter** Service **Bulletin** Binary Options	13 **Facebook & Twitter** Extortion	14 **Facebook & Twitter** Personal Info	15 **Facebook & Twitter** Loan	16 **Facebook & Twitter** Investments	17
18	19 **Facebook & Twitter** Romance **Bulletin** ID Fraud	20 **Facebook & Twitter** Lottery	21 **Facebook & Twitter** Recovery Pitch	22 **Facebook & Twitter** Emergency	23 **Facebook & Twitter** Bank Investigator	24
25	26 **Facebook & Twitter** Card-Not-Present **Bulletin** Cryptocurrencies	27 **Facebook & Twitter** Grant	28 **Facebook & Twitter** Wire Fraud	29 **Facebook & Twitter** Directory	30 **Facebook & Twitter** #Whatthefraud	31

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

6) Statistics

In 2017, the CAFC received 71,793 mass marketing fraud complaints with a total reported dollar loss of $110,329,034.47. 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 2017:

Complaint Type	Complaints	Victims	Dollar Loss
Phishing	1,965	1,215	$84,366.73
Extortion	1,256	204	$878,853.98
Sale of Merchandise	1,178	1,042	$489,464.57
Personal Info	766	519	$16,279.84
Merchandise	735	542	$515,214.66
Job	542	180	$750,113.58
Service	348	182	$99,527.55
Counterfeit Merchandise	230	227	$57,676.66
Loan	121	98	$128,469.97
Prize	70	17	$24,161.95

Top 10 Young Adult scams based on dollar loss in 2017:

Complaint Type	Complaints	Victims	Dollar Loss
Extortion	1,256	204	$878,853.98
Job	542	180	$750,113.58
Merchandise	735	542	$515,214.66
Sale of Merchandise	1,178	1,042	$489,464.57
Romance	54	38	$435,216.38
Loan	121	98	$128,469.97
Service	348	182	$99,527.55
Investments	37	26	$88,717.33
Phishing	1,965	1,215	$84,366.73
Counterfeit Merchandise	230	227	$57,676.66

➔ It's believed that fewer than **5%** of victims file a report with the CAFC regarding Mass Marketing Fraud.

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 5th – 9th).

Theme 2 - Monday, March 5th, 2018 - **Scams Targeting Young Adults**
Bulletin: **Continuity Scams**

Buying Online and Counterfeit Goods

Canadians need to be cautious when buying merchandise online and are encouraged to fully review feedback and deal with companies or individuals that they know by reputation or past experience. If the buyer is not familiar with a particular seller, they should independently verify who they are. A good rule of thumb: if the asking price of a product is too good to be true, it is.

Counterfeiters have also become proficient in producing websites that have the same look and feel as the legitimate manufacturer. Counterfeit products are far inferior and in many cases could pose a significant health risk to consumers. For example: counterfeit jackets have been found to contain bacteria, fungus and mildew.

Everybody should do their due diligence and thoroughly research an online store or website prior to making a purchase. Confirm that you are dealing with the actual manufacturer and look for any warnings posted on their website.

Warning Signs – How to Protect Yourself

- Never make a deal outside an auction site, and be cautious of items offered through online classified ads for extremely low prices.
- Inspect the website thoroughly. Often counterfeit websites will contain spelling mistakes and grammatical errors.
- Beware of sellers and renters from overseas.
- Beware of limited or no feedback ratings on sellers.
- Use a debit/credit card when available. You may have protection and be eligible for a refund.

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.

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 financial information, which can be used for identity theft and 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.

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.

A new twist to 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.

Merchandise

These scams involve the non-delivery of goods purchased through classified ads over the internet or internet auction sites, through a catalogue or by mail order. Merchandise scams can vary depending what the consumer is purchasing. The most common variations include puppy, rental units, and motor vehicles.

Puppy: Classified ads target dog lovers with the promise of a puppy, but only once all the necessary fees are paid. Scammers advise they have recently moved and to facilitate a quick transaction, are giving the dog away. The catch? The buyer is responsible to pay for shipping, insurance, customs, etc.

Rental: Scammers post ads of desirable rental units at discounted rates. Victims who contact the “owner”, are asked to provide a deposit on the rental – often by wire transfer. Consumers who attend the units may witness it’s for sale and the scammer copied the pictures/details from the real estate listing.

Motor Vehicle: Scammers post ads selling vehicles at below cost. They claim their work has caused them to relocate and as a result, to use a safe, third party payment agency. Victims who agree to the terms are asked to wire funds to the third party agency to hold until the vehicle is delivered. The car is never delivered and the money is lost.

Warning Signs - How to Protect Yourself

- When searching for rentals, visit the address. Schedule a showing to confirm availability.
- Limit your risk and buy local. View the merchandise in person to validate the sale.
- Complete open source searches on the seller – see if others have reported a scam.
- Know the average asking price. If it is too good to be true, it probably is.
- Never send money to strangers. Reduce your risk of victimization.

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 at http://www.antifraudcentre.ca