Toolkit for March Fraud Prevention Month 2018

Businesses

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 5: Scams Targeting Businesses	---	7
• Wire Frauds	---	7
• Card Not Present	---	8
• Grant	---	9
• Sale of Merchandise	---	10
• Directory	---	10

Introduction

In preparation for March Fraud Prevention Month, the Canadian Anti-Fraud Centre (CAFC) has compiled a toolkit specifically designed for use by private sector partners to further raise public awareness and help prevent victimization. We encourage all partners 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 be actively posting daily on Facebook and Twitter (#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.

Consumers and businesses 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 are always welcomed.

Thank you,
The CAFC Fraud Prevention Team

Canadian Anti-Fraud Centre
C A F C
Centre antifraude du Canada
FRAUD: RECOGNIZE IT. REPORT IT. STOP IT. LA FRAUDE: IDENTIFIEZ-LA. SIGNALEZ-LA. ENRAYEZ-LA.

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 Businesses will be highlighted in week 5.

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 scams reported affecting businesses during this time are listed below.

Top 10 Business scams based on number of complaints in 2017:

Complaint Type	Complaints	Victims	Dollar Loss
Wire Fraud	554	95	$18,603,330.5
Sale of Merchandise	377	248	$1,162,343.76
Directory	289	12	$13,895.51
Extortion	244	38	$96,876.95
Phishing	188	22	$308,500.69
Service	184	50	$ 191,958.5
Merchandise	140	92	$6,644,006.45
Job	119	22	$768,716.97
Other	110	30	$106,420.22
Personal Info	77	25	$48,950.00

Top 10 Business scams based on dollar loss in 2017:

Complaint Type	Complaints	Victims	Dollar Loss
Wire Fraud	554	95	$18,603,330.5
Merchandise	140	92	$6,644,006.45
Investments	25	13	$2,262,753.75
Sale of Merchandise	377	248	$1,162,343.76
Job	119	22	$768,716.97
Loan	30	7	$309,827.7
Phishing	188	22	$308,500.69
Service	184	50	$191,958.5
Other	110	30	$106,420.22
Grant	6	5	$ 97,767.00

➔ 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 businesses, which will be highlighted during week 5 of Fraud Prevention Month (March 26th – 29th).

Theme 5 - Monday, March 26th, 2017 - **Scams Targeting Businesses**
Bulletin: **Cryptocurrencies**

Wire Frauds

Canadian businesses are being targeted by two types of wire fraud: the Business Executive Scam and the Supplier Swindle.

The Business Executive Scam (BES), also known as the Business Email Compromise, the potential victim receives an email that appears to come from an executive in their company who has the authority to request wire transfers. In some cases, the fraudsters create an email addresses that mimics that of the CEO or CFO. In other cases, the fraudsters have compromised and used the email account belonging to the CEO or CFO. The spoofed email message will be sent to an employee that has authorization to conduct wire transfers. The email will indicate that the "executive" is working off-site and has identified an outstanding payment that needs to be paid as soon as possible. The "executive" instructs the payment be made and provides a name and a bank account where the funds, generally a large dollar amount, are to be sent. Losses are typically in excess of $100,000.

In the Supplier Swindle, Canadian businesses are targeted by fraudsters claiming to represent their regular supplier. The scam targets businesses that have existing relationships and accounts with suppliers and wholesalers. The scam usually involves a spoofed email informing the buyers of a change in payment arrangements. The email notice provides new banking details and requests that future payments be made to this "new" account

Warning Signs – How to Protect Yourself

- Beware of irregular email requests for urgent fund transfers.
- Prior to sending any funds or product, make contact with the requestor in person or by telephone to confirm that the request is legitimate.
- Watch for spelling and formatting errors and be wary of clicking on any attachments as they can contain viruses and spyware.

Card Not Present (CNP)

CNP fraud is defined as the unauthorized and/or fraudulent gathering, trade and use of payment data (card numbers, expiry dates and passwords). For CNP to occur, this data must be used in instances where the card and cardholder are not present (via phone, email, fax, or website).

A scammer places an order for a product or service via a merchant's Card-Not-Present channel (phone, email, fax, or website) intending to make the payment using a stolen payment card. The merchant, believing this to be a legitimate purchase, processes the payment on the stolen payment card(s) and delivers the product(s) or provides the service(s). Eventually the real cardholder identifies and disputes the unauthorized charge. As a result, the merchant receives a chargeback and is responsible for paying back the amount charged on the stolen card. It's important to remember that any merchant who accepts CNP orders can become a victim.

It is also common to witness an overpayment request when dealing with CNP fraud transactions. Scammers may demand the merchant charge extra on the card and forward funds to a third party – often a *moving company* -- to facilitate the shipment. By doing so, scammers are essentially turning stolen credit cards into cash.

Another version of CNP fraud seen within the airline industry is for scammers to purchase airline tickets using stolen credit cards and sell the tickets for a cheaper price online on classified ad sites. In situations like this, the merchant is not the only victim, so is the person purchasing the tickets being resold. In most cases, the purchaser will not be able to use the tickets as the merchant cancels them once fraud is confirmed.

Warning Signs - How to Protect Yourself

- Prior to shipping merchandise, call the phone number the customer provided and verify the transaction information.
- Be sensitive to priority shipments for fraud-prone merchandise, which may indicate a fraudulent transaction.
- Be aware of orders that occur with a request for urgent shipment, especially if the shipping address does not match the billing address of the payment card provided.
- Be aware of orders from repeat customers that differ from their regular spending pattern.
- Contact your processor and ensure security measures are established to prevent victimization and reduce unwanted chargebacks.
- Merchants who accept CNP orders can better avoid fraud by using the automated verification tools supplied by their acquirer and the payment associations.

Grant

Any false, deceptive, misleading or fraudulent solicitation involving the advertisement of a grant. Commonly, these ads are found in a publication such as newspapers, classified ads, magazines or through online ads and websites. Other times, it is through a phone call claiming to be from a "government" agency or some other official sounding organization. When a victim responds to the ad or phone call they are requested to provide their checking account information to either have the grant directly deposited into their account or to cover a "processing fee". Payments are often requested via iTunes gift cards, money service businesses, wire transfers, payment cards, and email money transfers. In the end, no grant is received, and if bank account information is provided it gives scammers the ability to disappear with your money.

Warning Signs - How to Protect Yourself

- Advertising through a recognized media outlet does not ensure that a legitimate company placed the ad.
- Do not give out any personal or banking information to anyone you do not know.
- Do not pay any money for a "free" government grant.
- Beware what information you share with an organization.

Sale of Merchandise

When selling merchandise online you need to be aware that not all offers received are good and honest. Businesses that 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). Businesses who comply may lose the merchandise shipped and be 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, they 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 last minute.
- Beware of overpayments with the request to send additional funds to a shipping agent.

Directory Scam

Businesses receive an invoice for a directory, publication or listing that they did not order or authorize. Fraudsters will place a call to the business and speak to an employee and ask to confirm details such as company’s address, telephone number and other particulars. An invoice is sent to the company and often payment is made by the accounting department, not realizing the company never ordered or agreed to pay for the directory. The fraudster may record the initial conversation and use that against the company to verify the purchase of the directory.

Warning Signs – How to Protect Yourself

- Educate employees at every level to be wary of unsolicited calls.
- Compile a list of companies typically used by your business.
- Fraudsters will use real company names like Yellow Pages to make the invoices seem authentic. Inspect invoices thoroughly prior to making payment.

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