
# Toolkit for March Fraud Prevention Month 2019

# Businesses

**#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 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 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.

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

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 Businesses will be highlighted in week 5.

### March 2019

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

Top 10 business scams based on number of complaints in 2018:

| Complaint Type | Complaints | Victims | Dollar Loss |
|---|---|---|---|
| Extortion | 347 | 28 | $105,865.00 |
| Sale of merchandise | 277 | 177 | $875,989.08 |
| Wire Fraud | 273 | 70 | $11,121,222.70 |
| Directory | 211 | 18 | $12,759.09 |
| Phishing | 181 | 6 | $1,369.40 |
| Service | 141 | 38 | $398,764.08 |
| Merchandise | 92 | 54 | $629,832.07 |
| Spoofing | 80 | 42 | $0.00 |
| Personal Info | 79 | 26 | $0.00 |
| Spear Phishing | 78 | 34 | $263,219.79 |


Top 10 business scams based on dollar loss in 2018:

| Complaint Type | Complaints | Victims | Dollar Loss |
|---|---|---|---|
| Wire Fraud | 273 | 70 | $11,121,222.70 |
| Sale of merchandise | 277 | 177 | $875,989.08 |
| Job | 71 | 13 | $746,570.19 |
| Merchandise | 92 | 54 | $629,832.07 |
| Service | 141 | 38 | $398,764.08 |
| Spear Phishing | 78 | 34 | $263,219.79 |
| Extortion | 347 | 28 | $105,865.00 |
| Unauthorized Charge | 6 | 5 | $65,269.40 |
| Fraudulent Cheque | 6 | 3 | $43,132.47 |
| Loan | 16 | 5 | $15,990.03 |

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

## 7) Fraud Warnings / Bulletins

Below are a few common frauds targeting businesses, which will be highlighted during week 5 of Fraud Prevention Month (March 25th – 29th).

Monday, March 25th, 2019 - **Scams Targeting Businesses**
Bulletin: **Card Not Present**

**Wire Frauds**

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

In 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 or existing contractor. The scam targets businesses that have existing relationships and accounts with suppliers, wholesalers or contractors. 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 – to facilitate the shipment, pay another vender, etc. By doing so, scammers are essentially turning stolen credit cards into cash.


Another version of CNP fraud targets merchants who sell a product or service that can be used later, i.e. tickets for travel or amusement. In this version, the scammers purchase the tickets using stolen credit cards and then resell the tickets online on classified ad sites and/or social media for a cheaper price. 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

Businesses must take caution when searching online for business grants and loans. Scammers develop websites designed to help small businesses access grants and loans across Canada, which has the appearance of being a government department. Sometimes scammers go as far as to mimic the websites and/ or names of a legitimate government department. These websites offer for a one-time fee, typically requested by credit card, that they will help businesses find a grant or provide them with a program or package with information and listings for grants/loans. In some cases, businesses are told that the one-time fee is refundable if no grant has been obtained.

### Warning Signs - How to Protect Yourself

- Do not pay any money for a “free” government grant.
- Beware what information you share with an organization.
- 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.

**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.

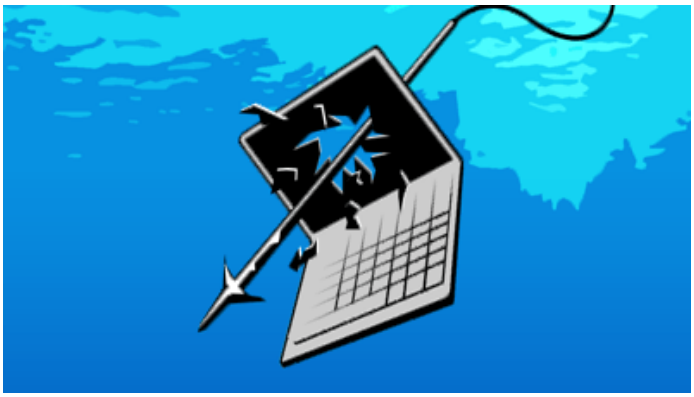
**Warning Signs – How to Protect Yourself**

- 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.

**Spear Phishing**

Spear Phishing is a fraudulent practice of sending emails that appear to be from a known sender such as your boss, a co-worker or a client. This is known as spoofing. Criminals use spear phishing to make the recipient believe they have received an email from a trusted source. This tactic induces the recipient to reveal confidential or sensitive information. Often, spear phishing emails request the recipients click on a malicious link or attachment. This could results in the loss sensitive information.

Spear Phishing tactics are also used in different scams to deceive employees into sending money. A common scam that targets businesses involves spoofed email requests that appear to come from a manager, owner or president of a company. These emails are sent to individuals within the business. The emails ask them to buy pre-paid gift cards i.e. ITunes, Google, Amazon etc. and email the prepaid card numbers back to the sender. In other instances, the fraudsters may request them to send money via e-transfer.



**Warning Signs - How to Protect Yourself**

- Verify that the email is coming from a legitimate source.
- Be aware of irregular requests for purchase.
- Implement increased precaution when sending funds/making purchases.


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