



Competition Bureau  
Canada

Bureau de la concurrence  
Canada



# Fraud Facts 2017

*Recognize, Reject, Report Fraud*

---

#FPM2017

Canada A stylized representation of the Canadian flag, with red and white horizontal stripes and a red maple leaf in the upper left corner.

# FRAUD FACTS 2017

We see and hear it all, from every type of person from all across the country. There is always a trap being set by scammers who are trying to separate you from your hard earned money. But that doesn't mean you have to fall for it.

Turn the tables on fraudsters by recognizing the tricks they use to try and get the best of you. Reject what they are trying to sell you or get you to do. And tell them you intend on reporting them to the authorities. They are scared of being caught and they will back off if you put your foot down and tell them to get lost.

Each year, as part of Fraud Prevention Month, the Competition Bureau works with its partners like the Canadian Anti-Fraud Centre (CAFC) and the RCMP to educate and encourage Canadians to learn about the signs of fraud, how to protect themselves from scammers, as well as the importance of reporting suspicious activity to law enforcement agencies.

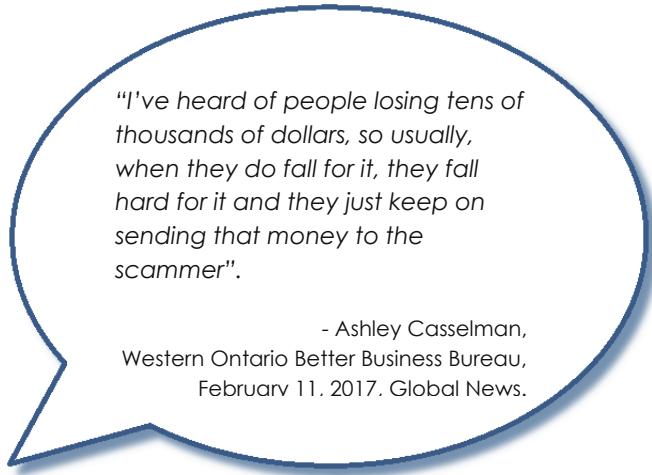
To give Canadians a better understanding of the impact fraud has on the marketplace, Fraud Facts 2017 provides a snapshot of the different types of scams that are currently affecting Canadians and what you can do to fight back. An informed consumer is a smart consumer and that is exactly what fraudsters don't want!

## Fraud costs everyone

Fraud is a crime that threatens every Canadian, regardless of their education, age or income. From January 2014 to December 2016, it is estimated that Canadians lost over \$290 million to fraudsters.

Scam artists continue to use traditional techniques by telephone, emails and in person, but have also latched on to social media platforms to target a new demographic: millennials and generation z. Despite being tech-savvy, this demographic has such a strong presence on social media that they have become natural targets for fraudsters.

Unfortunately, fraudsters continue to target seniors, and it is estimated that from January 2014 to December 2016, Canadians age 60 to 79 lost almost \$28 million to various scams.



"I've heard of people losing tens of thousands of dollars, so usually, when they do fall for it, they fall hard for it and they just keep on sending that money to the scammer".

- Ashley Casselman,  
Western Ontario Better Business Bureau,  
February 11, 2017. Global News.

## The stigma of fraud

The Competition Bureau and the CAFC received almost 90,000 complaints in 2016, compared to just under 70,000 in 2015. While complaints to the Competition Bureau focused mostly on false or misleading advertising and deceptive marketing, the CAFC received complaints related to more than 30 different types of mass marketing fraud and identity theft schemes. If you are unsure which agency to contact, start with the CAFC.

In 2016 alone, online scams accounted for more than 20,000 complaints and more than \$40 million in losses by Canadians.

However, it is estimated that only about five percent of fraud gets reported to authorities, which means that law enforcement agencies have a harder time staying ahead of the game and obtaining the necessary evidence to catch perpetrators and warn the public about potential fraud.

Consumers often don't report fraud because they are embarrassed that it happened to them, or maybe they only lost a small amount of money and don't want to go through the hassle of reporting it. Businesses don't want to appear vulnerable or damage their corporate image, and see it as the price of doing business today.

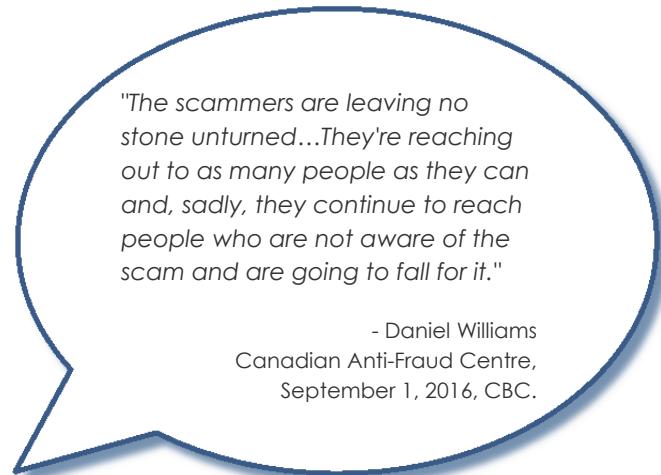
Even worse, there is a perception that this is not a "real" crime, and that law enforcement agencies have more important matters to tackle. This couldn't be further from the truth: laws exist to protect Canadians from fraud and the Competition Bureau, the RCMP and the CAFC take this very seriously.

It is extremely important to report fraud – it's one of the best ways authorities can gather evidence in order to bring down fraudsters and better protect consumers and businesses.

## Scams on the horizon

The Bureau and its partners are seeing a growing number of complaints related to cyber scams, as criminals are quick studies at using the latest platforms and technologies to commit fraud. What follows is an overview of the trends we see for fraud in the next year.

Some of these scams work by deceiving consumers or businesses into purchasing a product or service based on misinformation, while others are designed to defraud and coerce intended victims into paying money.



"The scammers are leaving no stone unturned...They're reaching out to as many people as they can and, sadly, they continue to reach people who are not aware of the scam and are going to fall for it."

- Daniel Williams  
Canadian Anti-Fraud Centre,  
September 1, 2016, CBC.

---

Some of the most prevalent and sneaky are:

#### Subscription Traps: Survey says...be careful

Subscription traps, sometimes also referred to as Continuity Scams, can take various forms. They can appear as an advertisement featured on your favourite social media site, a referral from a friend (on Facebook, for example), a fake "survey" that pops up on your computer while you're online on another website, or from a telemarketer. No matter the form, they will always offer you a "free" trial or purchase of a product, and all you have to do is simply pay the shipping and handling using your credit card. If consumers agree to this, they will find themselves signed up to a subscription service with ongoing fees and unexpected charges. Contacting the company will result in them pointing you towards their online terms and conditions, routinely buried in fine print. Unfortunately, by not returning the "free" product you ordered, you agreed to a monthly subscription of that product and authorized monthly charges on your credit card. Once, you are stuck in this situation, it is often extremely difficult to put a stop to the charges.

#### Spoofed websites: Ain't nothing like the real thing

A spoofed website is a site that uses deceptive means to mislead consumers into thinking that it represents a specific business, financial institution, government or charity. These websites generally imitate the real websites to sell products or services that may or may not be authentic, or to obtain sensitive financial or personal information from users. Often they will provide enough information to appear like the real thing, including the location of stores, phone numbers, terms and conditions, and logos.

#### Ransomware: When your hard-drive is kidnapped

Ransomware is a type of malicious software designed to block access to a computer until a sum of money is paid. A computer can be infected by ransomware in a number of ways, but most commonly, victims click on a malicious link or attachment received through a phishing email. Once infected, victims will see a "ransom" note which is often designed to scare or extort the victims into making a payment. For instance, a message could appear saying that your personal files and pictures will be deleted unless the consumer pays \$100-\$250 via Bitcoin, Ukash or PaySafe Card to have the computer unlocked.

---

## *Business Executive Scam: Don't follow this boss' orders*

Sometimes referred to as the Business Email Compromise scam, this fraud starts when a 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 email addresses that mimic those of the CEO or CFO. In other cases, the fraudsters have compromised and subsequently used the email account belonging to the CEO or CFO. Often, the email will indicate that the “executive” is working off-site and has identified an outstanding payment that needs to be made as soon as possible. The “executive” instructs the payment to be made and provides a name and a bank account where the funds, generally a large dollar amount, are to be sent.

Losses to this scam typically range from tens of thousands of dollars to hundreds of thousands of dollars.

And here are the ones that we keep seeing again and again:

### *Fake Online Endorsements and Sponsored Content – Followers and likes doesn't mean its good advice*

Consumers are often enticed to purchase a product or service based on reviews by social media influencers or those with a significant online presence. Unfortunately, there's a chance that these reviews are not genuine and have in fact been paid for by a company as a marketing tactic. By not revealing their business interests and creating what seem to be authentic experiences or opinions, these influencers are misleading consumers and could be subject to action under the Competition Act.

### *Astroturfing – It looks real, but it isn't*

Astroturfing has similar characteristics to fake online endorsements. The term “astroturfing”, when used in an online advertising context, refers to the practice of creating content that masquerades as the authentic experiences and opinions of impartial consumers, such as fake consumer reviews and testimonials. This is often part of organized efforts by companies to boost their own ratings or to lower the ratings of their competitors. For example, companies have been known to encourage their employees to post positive reviews on websites and review platforms, or to provide their customers with incentives to leave positive reviews.

### *Binary Options Scam: Never a good bet*

Similar to gambling, binary options work much like a wager. All or nothing “bets” are invested based on how an asset will perform within a certain timeframe. The asset could be a stock, a currency or a commodity. Websites are designed to attract users to trade binary options, by offering high rates of return and by claiming to be risk free. Initially, a virtual gain is seen, but there is no way to access the profits because they are non-existent. Currently in Canada no business is registered or authorized to sell or market binary options.

---

---

It is always risky to invest in offshore companies; investors who buy into a binary option run the risk of having their identity stolen, accumulating losses for unauthorized withdrawals on their credit cards and incurring high interest payments on an investment that doesn't exist.

### *Employment Scams: No experience needed!*

Scammers use online classified websites like Kijiji, Craigslist, Monster, Indeed, and Workopolis to recruit potential victims. The most common scams include Mystery Shopper and HR/Administrative jobs.

Consumers are offered a mystery shopper job after responding to an online ad or a text message. The victims receive a cheque in the mail with instructions to complete local purchases and send unspent funds through a money service business. 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.

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 by their bank that the original payment was fake or fraudulent and any subsequent monies sent are therefore paid out of the victim's own pocket. Scammers will attempt to process as many payments as possible before the victim's financial institution advises that the original payment was fake.

## **Know the signs**

The age old saying "if something seems too good to be true, it probably is" still applies today. No matter how sneaky fraudsters try to be, by keeping this in mind, you stand a better chance of warding off the bad guys. The best things in life may be free, but when you are asked for your credit card or personal information, it's best to just leave it be. Beyond trusting your best instincts:

- Review all fine print and terms and conditions before making a purchase.
  - Conduct open source searches to see if anybody has suggested the offer is a scam.
  - Beware of paid advertisements online. Paid banner ads are not always affiliated with the website you are viewing.
  - Prior to sending any funds or product, contact the person who requested the transfer in person or by telephone to confirm that the request is legitimate.
  - Beware of unusual or irregular email requests.
  - Never click on links or open attachments in unsolicited emails.
-

- 
- Review credit card statements regularly for unauthorized charges.
  - And remember, if it sounds too good to be true, it probably is.

The Bureau regularly puts out [Consumer Alerts](#) to warn Canadians of various issues relating to fraud, false or misleading representations and deceptive marketing practices that are making the rounds. Watch out for those. Follow us on [Twitter](#), [Facebook](#) and [LinkedIn](#) to stay informed.

## **Don't let fraudsters get away with it**

It's extremely important to report fraud to the authorities. Complaints are one of the best ways to gather evidence in order to better protect consumers and businesses. If you think you've been the victim of fraud, report it to the Canada Anti-Fraud Centre, the Competition Bureau or the RCMP.