Competition Bureau Canada
Bureau de la concurrence Canada

Fraud Facts

Recognize, Reject, Report Fraud

Canada

This publication is not a legal document. It is intended to provide general information and is provided for convenience. To learn more, please refer to the full text of the Acts or contact the Competition Bureau.

For information on the Competition Bureau's activities, please contact:
Information Centre
Competition Bureau
50 Victoria Street
Gatineau QC K1A 0C9

Tel.: 819-997-4282
Toll free: 1-800-348-5358
TTY (for hearing impaired): 1-866-694-8389
Fax: 819-997-0324
Website: www.competitionbureau.gc.ca

This publication can be made available in alternative formats upon request. Contact the Competition Bureau's Information Centre at the numbers listed above.

This publication is also available online in HTML at:
http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04334.html

Cat. No. Iu54-61/2018E-PDF
ISSN 978-0-660-24875-2

2018-02-22

Aussi offert en français sous le titre Faits sur la fraude - Détecter, contrer et signaler la fraude

Table of Contents

Introduction

We see and hear it all, from every type of person and from all across the country. Scammers are always setting traps 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 partners like the Canadian Anti-Fraud Centre (CAFC) and the RCMP. Together, they educate and encourage Canadians to learn about the signs of fraud, protect themselves from scammers, and report suspicious activity to law enforcement agencies.

To learn more about the impact of fraud on the marketplace, this Fraud Facts provides a snapshot of the different types of scams currently affecting Canadians and how 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 2017, Canadians lost more than $405 million to fraudsters.

While scam artists continue to use traditional techniques by telephone, email and in person, they 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, too. From January 2014 to December 2017, Canadians aged 60 to 79 lost an estimated $94 million to various scams.

The stigma of fraud

The Competition Bureau and the CAFC received over 70,000 complaints in 2017, compared to almost 90,000 in 2016. While complaints to the Competition Bureau focused mostly on false or misleading advertising and deceptive marketing practices, 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.

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

Consumers often don't report fraud because they are embarrassed that it happened to them. They may have only lost a small amount of money and don't want to go through the hassle of reporting it. As for businesses, they don't want to appear vulnerable or damage their corporate image, and see fraud 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 this year

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

Phishing

Phishing is a scam and, like its namesake, it has a hook: an email that looks and sounds legitimate, but isn't.

That message looks like it is coming from a bank or a service provider or even from someone close to you. If you take the bait, you are redirected to a website that looks normal but that is in fact a copy made by malicious "phishermen".

Thinking that you are on the real website, you are not surprised or even suspicious when they ask for personal information like your login information, password, account number or social insurance number. Once you provide your personal information, they can use it to commit fraud.

Emergency Scam - Grandparent Scam

If you receive an email or call from someone claiming to be a friend or relative in urgent need of cash to get out of trouble, it's probably a scam! Anyone can be targeted by the emergency scams but often, scammer will prey on seniors. Con-artists can make stories sound very credible.

For example, they will call and pretend to be their victim's grandchild. The scammer will ask for money to be sent immediately so that they can get out of trouble. The "grandchild" will insist on keeping this a secret so that their parents don't find out.

The victim will go on to send money through a money transfer service, pre-paid gift or credit cards or even in bitcoins, in hopes of helping their grandchild. Unfortunately, the victim gets scammed and the money goes to the fraudster.

In 2016, over 800 Canadians fell victim to this scam and lost more than a million dollars in total.

Wire Fraud - Supplier Swindles – CEO Scam

With almost $13 million taken out of honest Canadians' pockets, it's fair to say that "wire fraud" is a scam you need to be aware of. Also known as the "supplier swindle" or the "CEO scam", this is a scam that targets businesses.

In some instances, an employee receives an email from a high-ranking executive – often the CEO or the CFO. The email informs the employee that they need to transfer money quickly to close an important transaction.

In other cases, an employee receives an email from a trusted supplier. The email informs the employee that an order has not been paid or that their account information has changed. The employee is asked to change the suppliers banking information and send the payment.

In both scenarios, the email appears to be legitimate, so the employee goes on with the request and sends the money. In fact, the email was a very good imitation and came from an unscrupulous scammer. The money is gone.

Extortion scams

Extortionists are scammers who use every trick in the book to persuade you to give up money, services or even property. They can target anyone.

They contact you by phone, text messages, emails or social media messages. Once they have your attention, they lay out a sophisticated scenario in which you are left with what looks like only one sensible choice: to pay them. They can resort to threats against you, your family, your property or your reputation.

In the end, the only thing that they want is your money. They can ask for cash, but often enough, they will be subtle and use other means of payment: one that fits their scenario. They can ask for an e-transfer, gift cards, pre-paid credit cards or even cryptocurrencies like bitcoins.

If you believe you are being threatened by an extortionist, don't panic. Call the police. Extortion is a criminal offence.

Scams you should still watch out for

Subscription Traps

Subscription traps, sometimes also referred to as Continuity Scams, can take various forms. They can appear as an advertisement featured on your favorite 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 a call from a telemarketer. No matter the form, they will always offer you a "free" trial or purchase of a product, while all you have to do is simply pay the shipping and handling fees using your credit card. If consumers agree to this, they get signed up to an ongoing subscription service with unexpected charges. Contacting the company will direct 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 stop the charges.

Spoofed websites

A spoofed website is a site that misleads consumers into thinking that it represents a specific business, financial institution, government or charity. They generally imitate 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

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 you pay $100-$250 via Bitcoin, Ukash or PaySafe Card to have the computer unlocked.

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

Fake Online Endorsements and Sponsored Content – High numbers of followers and likes don't mean anything

Consumers are often enticed to purchase a product or service based on reviews by social media influencers or people with a significant online presence. Unfortunately, there's a chance 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

Astroturfing has similar characteristics to fake online endorsements. In an online advertising context, it refers to the practice of creating content that looks like the authentic experiences and opinions of impartial consumers,. These include fake consumer reviews and testimonials. Companies often do this to boost their own ratings or to lower the ratings of their competitors. For example, they might encourage their employees to post positive reviews on websites and review platforms, or 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 say no. Follow these tips to protect yourself:

- Review all fine print and terms and conditions before making a purchase.
- Google it 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.
- Before you send any funds or products, contact the person who requested the transfer in person or by telephone. 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.

Watch for our regular Consumer Alerts on the latest issues relating to fraud, false or misleading representations, and deceptive marketing practices. 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 and better protect consumers and businesses. If you think you've been the victim of fraud, report it to the Canadian Anti-Fraud Centre, the Competition Bureau or the RCMP.