THE REALITY OF FRAUD

By August the Canadian Anti-Fraud Centre (CAFC) had already received over 20,000 reports of fraud with over $43 million in losses for 2019. While that number is already high, the CAFC estimates that only 5% of victims report fraud to law enforcement agencies, which means the true financial cost of fraud could be closer to a billion dollars by 2020.

Fraud often goes unreported because victims are ashamed of themselves and too embarrassed to admit they fell for what now seems like a pretty obvious scam. The important thing to remember is – you are not alone. People don't fall for scams because they are stupid or gullible, they fall for them because the fraudsters are masters of deception. They know what to say and how to say it so that you feel flustered and scared and comply for fear of what will happen if you don't. What's even more disconcerting is they will take advantage of your kind heart and/or desperate financial situation.

The CAFC is the central agency in Canada that gathers information and criminal intelligence on all different frauds including romance scams, advance fee fraud, identity theft and mass marketing fraud (ex: send out thousands of e-mails requesting personal information under false pretenses hoping that someone will bite). By visiting the CAFC website, you can learn about the trending scams, how to spot them and how to report it.

Outlined below are the most common scams our members have encountered, signs indicating you have been scammed and step-by-step instructions to follow if you are targeted.

TRENDING SCAMS

Emergency/Grandparent Scams

In this scam, the victim will receive a call, usually in the middle of the night, or the wee hours of the morning when they are less alert. The caller will try and pass themselves off as a grandchild who is in some kind of trouble: maybe they are travelling abroad and have run into some trouble with the law, they've hurt themselves and need money for medical attention or for a plane ride home. The caller will start off the conversation by saying something like "Hi grandma/grandpa" and hope that the victim says, "Oh hi Dave/Becky" and they go from there. The caller is also hoping that the grandparent doesn't speak with their grandchild that often and wouldn't necessarily be aware of travel plans. The caller will usually give the victim a deadline to wire money so they don't have long to think it through. They may also advise the victim not to tell the parents of the grandchild for fear of worrying them or getting them in trouble. The scammer does not want the victim to tell anyone who may try to talk them out of sending the money.

Romance Scam

This scam is particularly cruel as it tugs on the heartstrings of lonely people yearning for love and companionship. Romance scams take longer to execute because the fraudster must develop a relationship with the victim and gain their trust. The scam usually begins online through a dating website or chatroom and the fraudster has likely already perused the victim's social media platforms gathering information to fabricate the persona of the victim's ideal mate. Once the fraudster has gained the victim's affections they will begin asking for money. The fraudster is often from an impoverished country and will claim they need money for medical expenses, a plane ticket to meet the victim in person or funds for a "once in a lifetime" investment opportunity. When a romance scam is identified, it is often difficult to convince the victim they've been played. The victim is crushed and doesn't want to admit to anyone, including themselves, that the love was not real.

Overpayment & Employment Scams

With all the buy/sell websites and online job opportunities coupled with people's appetite for "get rich quick" schemes, this scam is very popular. The victim may be selling something online for $200 and the "buyer/fraudster" will send them a cheque for $2000, then contact the victim explaining they accidentally wrote the cheque for the wrong amount. The buyer advises the payee to deposit the cheque for $2000 and keep their $200 plus an extra $100 for their troubles and to send back the remaining funds. The cheque will be returned unpaid and the victim will be out the money.

Another popular hook is to advertise an easy, well-paying job opportunity such as a secret shopper. The victim will receive instructions to go to a store and pretend to be a customer then answer questions about their shopping experience and, again, receive a cheque for much more than they were expecting.

Anti-Virus (Microsoft) Scam

You're on your computer and suddenly the screen goes black, a message appears instructing you to click a link or call a number otherwise your computer will crash, explode or something equally undesirable. They may say there is a virus on your computer and that you need to click a link to allow them remote access to your computer to fix the problem. Once you allow the fraudsters access, they can see all of your personal information which they can use to steal your identity or your money through online banking, credit cards, etc. They may also request payment to fix the problem and ask for your credit card information. If a message like this appears on your computer, unplug it immediately. Take your computer to Staples or a trusted computer technician (or a tech savvy friend/family member) to "clean" your computer, essentially making sure there are no viruses or malicious software installed on your computer.

CRA Scam

This scam happened to a friend of mine. She is a European immigrant and her husband received a call from a man stating he was from the Canada Revenue Agency and that he and his wife owed thousands of dollars in unpaid taxes. The victim was advised if the payment was not made within a very short time period, that him and his family would be deported. The husband panicked and paid immediately. Then he

called his wife/my friend to tell her what happened. As my friend and I both worked in the financial services industry, we knew immediately that they had been scammed.

A while back these fraudsters were actually requesting for CRA payments via iTunes gift cards. Surprisingly, people were complying. The takeaway from this is: the CRA will NEVER contact you over the phone or e-mail and request personal information (the CRA already knows it all) or payment for taxes owing. If you owe taxes, you will receive a bill in the mail. If you are doubtful of the legitimacy of the bill, contact the CRA (do not call the number provided, do an internet search and ensure you are calling the right place) and confirm the bill with a CRA representative.

Inheritance & Lottery Scams

This scam targets people who have a low income, are on social assistance or are simply desperate for money. You receive a letter stating you have won a lottery (interesting, since you never entered one) and that you have to send money for taxes or legal fees before you can collect your winnings, which of course, you never receive. Another popular hook is receiving a letter stating you have a long lost relative who has no other family and is leaving you with a life-changing sum of money, but of course, you must send them money first. Hint #1: When you win the lottery, *you get* money, you *don't give* it. Hint# 2: You *need to enter* the lottery *to win* the lottery.

Phishing Scams

I get these all the time: texts from one of the big five banks (which of course, I'd *never* bank with) claiming I've been locked out of my online banking account and to click a link to validate my identity and regain access to my account. NEVER CLICK THE LINK. Clicking on the link could have a number of undesirable results including downloading malicious software and/or viruses to your computer or the link may direct you to a questionnaire requesting personal information that they will use to perpetrate fraud. Another common one is a text or e-mail stating you have received an e-Transfer and to click the link to accept the money. If you were not expecting an e-Transfer and you also don't recognize the name of the person it's from, block the sender and delete the e-mail/text.

Debit Card Fraud

While debit card skimming has declined substantially in Canada since the rollout of chip technology, there is still a risk. Skimming occurs when the information from your card is captured at a compromised ATM or Point of Sale (POS) terminal and used to make a duplicate card to withdraw cash. Since foreign ATMs have not all switched over their terminals to chip, the magnetic stripe on our card needs to hold our banking information so it can be used when travelling abroad. This is why the expenditures resulting from skimming will occur outside Canada: they need a magnetic stripe enabled terminal to withdraw funds from the duplicate card. To prevent your card from being compromised, ensure you check the terminal for signs of tampering and *always* shield your PIN.

Many people shy away from **Interac Flash** for fear someone will get their card and go on a shopping spree. Since you cannot tap for a purchase over $100 and you are required to enter your PIN once the sum of your tap purchases reach $200, the risk is minimal. Even if someone did get your card, Interac's Zero Liability covers you for losses resulting from unauthorized purchases. Furthermore, Interac uses the latest technology to ward of skimming, counterfeiting and electronic pick-pocketing.

Identity Theft

Identity theft is not a fraud scam but a precursor to commit other frauds. There are many ways that fraudsters can obtain your personal information, steal your identity and commit fraud. Some of the most common methods include:

- dumpster diving (going through your trash)
- re-routing your mail to themselves
- obtaining unsecured personal documents such as identification cards, bank statements and tax papers
- phishing (tricking you into providing personal information via phone, e-mail or text message)

Once the fraudster has obtained enough personal information, they can use it to apply for credit in your name including bank accounts, credit cards, even a mortgage.

Signs your identity has been taken:

- missing mail
- your credit report shows inquiries for credit you have not applied for
- you start receiving calls from collection officers for debts that aren't yours

I'VE BEEN SCAMED! WHAT DO I DO?

Depending on the scam, some of the following actions may not apply, however, most of these steps should provide damage control for most frauds and prevent re-occurrence.

- **Contact both of the Canadian credit reporting bureaus; TransUnion and Equifax.** Advise them of the incident. Ask them to place a "Fraud Alert" on your bureau. Any time a creditor makes an inquiry on your bureau they will see the "Fraud Alert" and contact you at the number you provided to confirm the individual applying for credit in your name actually is you.

  TransUnion
  1-800-663-9980 select option 3

  Equifax
  1-800-465-7166

- **Contact your financial institution.** They may place a note on your account to ask for ID before each transaction, change your online banking password or close your account and open a new one with a different account number. This will all depend on the type and severity of the fraud.
- **Contact your credit card companies (especially if you pay them online!)** Advise them of the incident and cancel your cards immediately and have them reissue replacement cards. They will also review the recent transactions on your card to ensure they are authorized.
- **Get your computer "cleaned".** If the scam was perpetrated online, or involved your computer in any way, you should ensure that it is free of viruses and that no malicious software was installed on your computer before you use it again.
- **Report the fraud.** You can report the fraud to your local police station or do so anonymously online through the Canadian Anti-Fraud Centre or call them Monday – Friday between 10 am and 4:45 pm (eastern standard time) 1-888-495-8501

If you have any questions regarding fraud, whether it is prevention tips or you suspect you may be involved in a scam, please do not hesitate to reach out to us for advice. Don't be shy and don't be embarrassed. We aren't here to judge; we are here to help.

Oshawa Community Fraud Ambassadors

Amy Munro
Member Services Representative
E: amym@oshawacu.com
T: 905-436-5418

Linda Treen
Administration Manager/Compliance Officer
E: lindat@oshawacu.com
T: 905-436-5416