Published in Dawson Trail Dispatch, April 2023, Vol. 27, Issue 8

Canadian Institutions Need to Be More Proactive to Protect Consumers from Scammers

By Monica Guetre

March was fraud Protection Month in Canada and it was no cause for celebration. The number of scammers stealing our money, property, safety, well being and even identities has reached historic levels.

The RCMP reported that in 2022, the Canadian Anti-Fraud Centre received fraud and cybercrime reports totalling $530 million in victim losses. That is a 40% increase from the $380 million in victim losses in 2021. In context, the increase wasn't because we are reporting criminals more, no, the increase is because scammers are targeting us more and getting more.

The realty is that the Canadian Anti-Fraud Centre says that only 5 to 10% of people report these fraudsters.

Whether you're a big corporation, medium sized or small family run business or an individual, we know the reported numbers don't even scratch the surface of how much of our hard earned pay cheque and savings are going to organized criminals and countries that actively do these crimes and aid in this activity.

Back in 2019 CTV news reported that one senior alone lost $732,000 to a romance scam and the bank didn't stop it. Or how about the recent CBC Marketplace report on an elaborate scam that all started with a knock at the door which leaves seniors with home improvement liens on their homes and high-interest mortgages they didn't need, want or understand. Canadian law and banks didn't protect those homeowners.

Even Statistics Canada totals look ridiculously low with 27,829 cybercrime incidents occurring in 2017 increasing to 70,288 in 2021 and for Manitoba in 2017 there were 455 incidents increasing to 1,523 in 2021.

Data collected by the Better Business Bureau 2022 survey of people reporting a loss shows that home improvement scams became the riskiest scam type, investment scams had the highest median dollar loss ($5,500) and nearly a third (29.5%) of all Canadians reported an online purchase scam, with 76.7% of people reporting monetary loss when targeted. The survey lists other scam types such as the advance fee loan, employment, rentals, credit cards, travel/vacation/timeshares, and phishing/social engineering scams like the grandparent scam where the fraudster urgently asks for money to get out of jail; or the scam letting you know that your computer's been hacked and offering to fix your computer or cell phone.

What can we do about it?

Let's ask our MPs, MLAs, and Municipal Councillors what they you are doing to protect us and ask that they move faster on the solutions.

Canada could position itself to organize the international community to broker more international cooperation to add teeth to prosecuting these criminals. Countries that continue to allow free reign to "scammers" need to face repercussions.

What about how to protect us from criminals trying to sell our property? A small solution is that all Provinces/Municipalities and legit Finance Institutions could link our property with a private (not visible online) "Not for Sale" "Pending Sale" categories. Real estate agents and lawyers could use this as further assurance (although not foolproof) that a sale is legit by checking a property's status with 2 legal institutions along with the other information they are required to collect to sell a property.

Ban all residential property liens without owner's knowledge and legal acceptance.

Outlaw door-to-door sales unless the municipality has provided a license after they've checked to see if the business is legit by collecting company information in-person and checking with the Canadian Anti-Fraud Centre and BBB.

Close all banking regulation loop holes that still allow our financial institutions from shirking responsibility to us the consumer and to refund money lost on criminal activity like a scam. This nefarious activity, including scammers and fraudster payments need to be stopped.

Ban telephone companies from selling robo-calls except for legitimate reasons such as messaging during election time.

Remind telemarketer's of their responsibility. Canada has a National Do Not Call List and when a consumer is on that list you can't call. Connect the violation reporting on the Do not Call List to the Canadian Anti-Fraud Centre.

On a local level, how about a joint effort between the Chamber of Commerce, Regional Development Corporation and Seniors Senior's

organizations to mail out to their residents reminders on what to look out for, and how to report and leading annual in-person or virtual education sessions?

Each of us should check regularly on family or others who might be vulnerable to persuasive and persistent scammers. Let them know what scams are going around and how to report it.

Don't sign any paper without taking the time to understand what you are signing and ask questions. Bring the papers to a knowledgeable family member or ask a legal expert for help.

Publish the Canadian Anti-Fraud Centre and BBB contact and scam information on the local news and municipal websites along with visible warning messages or alerts. Keep this information visible as a reminder. The out-of-site mentality, means forgetting or not being aware of a new scam and the once-in-a-while messaging is obviously not working.

When you go to buy a pile of gift cards for Christmas or birthdays and the store clerk asks if you are ok, did you get an urgent call to send money? Don't get angry with them. Say thank you because that person is trying to help you out of a bind.

Make it mandatory that stores selling gift cards have well placed check out signage itemizing what is a gift card scam along with the Canadian Anti-Fraud Centre reporting contact information.

Legislate to protect our personal data so that we have the option to store or not store any or all our information with a company offering on-line services unless we've allowed it. That goes for any on-line store, bank, utility, phone, internet, payroll provider, insurance, real-estate, Crown Corporation, government agency, etc. who stores data online or on a server accessible through the internet. Hold companies accountable with protecting our data and legislate liability so that we are reimbursed money lost automatically rather than having to go through the courts or get shuffled from one person to another.

Make our financial credit reports free of charge at least once a year and forever after an identity theft.

Let our MPs know we need to get the new Canadian Anti-Fraud Centre on-line reporting up and running. In 2020 the Government of Canada started developing a new reporting system but it's still only at the pilot testing stage and won't be operational until later in 2023 or 2024.

Never send money or provide personal documents to anyone without a face-to-face meeting. Don't over share on social media. Before you donate money to a charity, research the organization to ensure it is legitimate. Check the charity out by going to the Canada Revenue Agency's searchable online database of all registered charities in Canada. Never click on links or open attachments in unsolicited email or text messages.

Go ahead and hang up on unwanted phone calls. This is the time you shouldn't be a polite Canadian. Please don't carry on a conversation, do not encourage the person on the other end of the phone.

Remember that you're not the only victim of these crimes. These criminals are very organized and will continuing doing it until you say something. Don't let the scammer get away with it, lets help each other.

Ignorance is not bliss

Stay informed on the newest scammer activity at canada.ca/en/revenue-agency/campaigns/fraud-scams and the Canadian bbb.org.

YouTube has some interesting scam baiter resources. These scam baiters are publicly trying to stop online fraudsters in their tracks. I'm certainly not advocating that all of you IT experts become vigilantes, however if you come across information and are helping your fellow Canadians, I hope you share this information with the Canadian Anti Fraud Centre and the RCMP who I hope are open to getting this information and acting on it because the online criminals know no jurisdictional boundary.

You can watch some of these YouTube scam baiters, who offer helpful online tips on how to keep safe and what how they locate these criminals and delete victim's personal data. Check out some of the videos made by Jim Browning, Scammer Payback going by the name of Perogy, Scambaiter, and Pleasant Green.

How to Report it.

1. Have handy all information about the scam.

2. Alert your bank/financial institution that transferred the money and place flags on your accounts and check your credit report. The two national credit bureaus, to place a fraud alert on your credit report file are Equifax (1-888-836-6351) or TransUnion (1-866-525-0262).

3. Contact the Canadian Anti-Fraud Centre toll free at 1-888-495-8501 or through the Fraud Reporting System on line.

4. Contact your local police.

5. For online fraud, you can also notify the website where the fraud took place. If the fraud took place online, such as through Amazon, Overstock, Wayfair, Facebook, eBay, a classified ad website such as Kijiji, or a dating website, report the incident directly to the website. Each of those websites are supposed to have a “report abuse” or “report an ad” link.

6. Contact your local consumer affairs office to request an investigation that appears to come from within your own province or territory. In Manitoba contact the Better Business Bureau at 204-989-9010 or report online to file a complaint or leave a review about a business.