I Was Scammed!

by Marie Moliner

If fraud could happen to me, it could happen to you.

For a short time in the 80s, I was a Crown Attorney. Decades later, as Vice Chair of the Toronto Police Services Board, I learned more about good and evil. My spouse is a retired judge. So we understand crime. Yet I have been taken in by scammers.

In my 30s, I gave cash to a soccer player who claimed he'd lost his teammates en route to a match. In my 50s, while perusing a government pension website, a pop-up advert extracted hundreds from my credit card. This was after my voluntary $29 payment for a skin care cream that promised to make me 30 years younger. It turns out I had purchased a subscription, via a clause in tiny print on a separate screen embedded in the ether. I still have the bottle of gold-flecked liquid as a reminder that I need to pay more attention to the details.

I am now in my 60s. A senior. I am generous and trusting, perhaps to a fault. Like many of us, I get text scams advising me that I will be arrested if I don't pay the CRA or a bank right now. I recognize these for the deceit they are. Still, I know I will become more vulnerable.

In 2021, the Canadian Anti-Fraud Centre (CAFC) reported that $83.5 million was stolen from seniors (based on 12,944 reported frauds). Of this, $38 million was by investment fraud and $19 million was by fraud via romantic seductions.

Surprisingly, less than five percent of victims file fraud reports. Only 5,000 people reported identity fraud, the most frequent form of fraud affecting seniors.

Investment Fraud

Janet Watson of Sherbrooke knows about fraud. Seventeen years ago, she lost $68,000 from her RRSP savings. She became the spokesperson for a class action suit concerning the scheme. Investment fraud is the scam most often reported. In Watson's case, she had been working with a "trusted" financial advisor, a family friend. He kept suggesting a product with a company she later learned had stolen $130 million from her and 1,600 others.

"I was one of the lucky ones because of the relatively small amount of money I lost," Watson told me. "The effect on some of the other victims was pretty profound: suicide, marriage breakdowns, health issues."

After serving just 18 months, he was released on full parole in 2022. Watson took the time to register as a victim with Corrections Canada, an arduous process. This requires them to alert her when he leaves the Montreal area, a term of his parole which expires in 2026.

Are you being defrauded? Take these six steps.

Step 1. Gather all the information about the fraud.

Step 2. Write out a chronological statement of events.

Step 3. Report the incident to your local police.

Step 4. Report the incident to the CAFC via the Fraud Reporting System (FRS) or toll-free at 1-888-495-8501.

Step 5. Report the incident to the Financial Institution or Payment Provider used to send the money.

Step 6. If the fraud took place online, report the incident directly to the website involved.

- *Canadian Anti-Fraud Centre*

Watson was persistent and relentless. She regularly attended court where the fraudster would glare intimidatingly at her. She described him as charming and violent. He was convicted on several counts and sentenced to 13 years.

Email Fraud

Last year, Wanda from Montreal lost two email accounts, one on Christmas Day when her primary email account of 30 years was hacked.

“Whoever did it took control of my contact list and sent emails out in my name to thirty years of contacts, requesting money. Sadly, some did send money to the hacker. I still feel embarrassed and guilty about that.”

A few days later, a man identifying himself as Korean took control of her second email account, used to keep track of bills and reward cards. He asked for a ransom payment in bitcoin.

"I deleted the email, did not enter into any conversation with him and I did not pay the ransom. As yet, I have not been able to retrieve my access to that account. It is incredibly scary,” said Wanda.

“My confidence in emailing and the internet, in general, has been broken. I no longer feel secure. I am always wondering if someone is there with me looking at my mail. Now I have far too many email accounts as backups, and feel secure with none of them."

Phone/Internet Fraud

Most people are wary of disclosing their exposure to fraud. We are embarrassed at what we see as our own stupidity. The reality is that fraudsters use very sophisticated tactics, sometimes combining in-person visits with phone and computer contact. One fraudulent caller made the Sherbrooke Police phone number appear on the victim's phone screen, reported the Montreal Gazette.

Last summer, callers claiming to be from a bank or credit union advised victims that their ATM and credit cards had been compromised. They asked the victims, mostly in their 70s, to give the credit cards and their PIN to a Canada Post employee who, by chance, was outside their door, and even wearing a Canada Post uniform, reported the Record.

Manipulative cookie banners fuel internet fraud. These pop-ups ask your consent for the website to retain information about you between browsing sessions. Cookies, says the United Kingdom's Information Commissioner, are one example of “dark web design – the practice of creating user interfaces that are intentionally designed to trick or deceive the user into parting with their time, money and privacy."

Grandparents Scam

Sadly, the most common fraud affecting seniors, says the CAFC, is the Emergency/Grandparents Scam. Seniors or their family members are contacted by someone claiming their grandchild or family member was in an accident, charged with an offense or, in some cases, is ill with Covid-19. Suspects claim they are law enforcement officials, lawyers or even a grandchild or family member.

On that note, Watson has advice to grandparents. “People need to be very cautious. I won’t trust just anybody. I am very careful on Facebook. I just don’t post pictures of my grandchildren. Ever. I do bank online, but I am careful. I don’t live my life in fear. People will find out your info if they want to. I don’t make it easy.”

As for me, I am taking note and becoming more careful. I know banks and the CRA will never contact me by text message. I browse in "incognito mode" and check for the "https" URL ("s" for "secure") when online shopping. But dark web design scares me. Fraud is evolving and takes no prisoners, as the CAFC recently learned, when fraudsters began posing as CAFC employees in a new variation of the bank investigator scam. So, be very aware. If it sounds too good to be true, it very probably is.

Marie Moliner *is Assistant Editor of the Townships Sun and enjoys the magic of her surroundings every day.*