CANADIAN ANTI-FRAUD CENTRE BULLETIN

12 Frauds of the Holidays 2025-12-03

FRAUD: RECOGNIZE, REJECT, REPORT

The tree is trimmed, the lights are glowing, and Canadians are gearing up for a busy holiday season. Unfortunately, fraudsters are just as active this time of year. The Canadian Anti-Fraud Centre (CAFC) is highlighting the most common holiday-related frauds so you can recognize the red flags, reject suspicious requests, and report fraud before it spoils your festivities.

- **Online Shopping –** These bright and shiny brand name offers are often listed for quick sale or for too good to be true prices. Save your money and your pride by shopping with retailers that are genuine. Research before your buy. If you do receive inferior or counterfeit products, they could pose significant health risks.

- **Selling Goods & Services –** Is someone wanting to buy your sleigh sight unseen or offering to pay more than the asking price? Confirm you've received some real bucks before you fulfill their order. Be wary of requests that become overcomplicated or require you to send money before you receive full payment.

- **Shipping Frauds –** Unsolicited text messages or emails, that impersonate legitimate shipping companies, that urgently request your personal or payment information due to incomplete shipping information, that inform you of delivery failures or packages being held for payment. Alternatively, fraudsters may request that you submit payment to their fabricated shipping company, like the North Pole Express.

- **Cellphone Promo Frauds –** Fraudsters are calling claiming to be a well-known service provider offering to gift you with a new cellphone and discounted plan. After collecting personal information required for credit checks, they'll order a new phone in your name. The phone may be shipped directly to these misfits. Alternatively, the victim may receive the 'wrong' phone and receive a request to ship it forward to the bad guys.

- **Investments -** Fraudsters are using social media and fraudulent websites to promote fraudulent crypto investment opportunities. They may even reach out through a random 'wrong number' text message. They'll sell you on how easy it is; while they gain remote access to your device and assist you in setting up accounts. They'll also guarantee that you'll be feasting on profits in no time and with just a small investment to start. Research your advisor, their company and the feasibility of all investment offers. Verify that they're on the *Nice* list by using the National Registration Tool (www.aretheyregistered.ca).

- **Romance Fraud –** Can't get your new online love to meet you under the mistletoe, but they have no problem sending you sweet nothings followed by countless requests for money? Time to pull the bow off their motives and investigate the legitimacy of every piece of information they've shared with you. You should never send money to someone you have never met.

- **Recovery Offers -** These fake law enforcement or recovery specialist will claim that they can recover your financial losses from a previous fraud. They'll make you jump through several reindeer games, all while collecting more of your hard-earned money. Report incidents of fraud to your local law enforcement and financial institutions as soon as possible to maximize your real chances at recovery.

- **Gift Cards –** Gift cards are a popular and convenient way to give a gift. They make great stocking stuffers; except when they're empty! When buying gift cards in-store, make sure they haven't been tampered with by comparing others in stock and running your finger over barcodes. When purchasing gift cards online, avoid resale and auction sites. Legitimate businesses and organizations will not request gift cards as payments; especially under pressure.

- **Donating –** 'Tis the season of giving and fraudsters are looking to be taking. Charity frauds involve any false, deceptive, misleading or fraudulent solicitation for a donation to a charity, association, federation or religious cause. Always ask or locate the charitable tax number and confirm their registration with the Canada Revenue Agency - List of Charities or by phone at 1-800-267-2384. Whenever possible, donate at the source.

- **Prize and Vacation Notifications –** What could be better than planning your escape from a winter wonderland? Winning a car, $1M, or even a free holiday vacation! First, you just need to confirm your personal information and then cover a few fees before your winnings can be claimed. Remember: if you didn't enter a contest or raffle, you can't win. You also can't enter another country's lottery without purchasing a ticket from within that country. In Canada, if there are fees associated to a prize, they will be deducted from the total winnings.

- **Toll Route & Infraction Phishing Text Messages** - With more Canadians travelling for the holidays, fraudsters send fake text messages claiming you owe unpaid toll fees, speeding infractions, or road-use charges. These messages often include urgent language and a malicious link. Genuine toll agencies wont demand immediate payment by text message. Do not click the link and report it to the CAFC.

- **Identity Theft and Identity Fraud –** In all the hustle and bustle of the season,
  DO: keep your wallet on your person and cover your PIN;
  DON'T: share passwords or provide your personal information freely.
  Fraudsters love a good shopping spree; especially when they're using someone else's information and money. Contact your financial institutions and credit bureaus, Equifax Canada and TransUnion Canada, as soon as you notice:

Anyone who suspects they have been the target of cybercrime or fraud should report it to their local police. Also visit the Report Cybercrime and Fraud website to report online or by phone at 1-888-495-8501.