

Tax, Retirement and Estate Planning

Trusted experts partnering with advisors

Scams, Fraudsters and the Covid-19 Pandemic

The Covid-19 pandemic has been a priority for many families and businesses. It has also been headline news around the world as we try to understand the virus and curb its impact. While many families and businesses have seen a reduction of income due to the pandemic, fraudsters and scam artists have taken the opportunity to expand their scope at the expense of unsuspecting Canadians. In fact, according to the Canadian Anti-Fraud Centre, between March 6 and May 1, 2020, there has been 766 Canadian reports of Covid-19 fraud, 188 victims and \$1.2 million lost from this activity.

In early May, police in the Central Okanagan issued a warning to residents that a new scam has hit the region. Kelowna RCMP indicated that they have received numerous complaints lately about a text-message scam involving the Canada Emergency Response Benefit (CERB), one of a myriad of income supports offered by the federal government in response to the pandemic¹. According to police, a text message is sent to a phone indicating that the recipient has received a CERB deposit, and the message includes a link or attachment. Police warn that by clicking on the link or attachment, the victim may allow malware to be installed on their device, or they could be taken to a website where they'll be asked to divulge personal information. Either option can lead to identity theft. If you receive this text message, advice from police is to not click on any links or attachments.

In addition to the above, as per the RCMP², examples of recent Covid-19 frauds include:

- Private companies offering fast Covid-19 tests for sale;
- Door-to-door solicitors offering fake decontamination services;
- Fraudsters posing as police and imposing on-the-spot fines to consumers wearing masks claiming that wearing a mask in public goes against a full-face veil law;
- The urging of investments in hot new stocks related to the virus;
- The sending of emails, texts or online campaigns that capitalize on the public's fears about Covid-19;
- Fraudulent online ads offering cleaning products, hand sanitizers and other high demand items.

Unfortunately, scams are not new to Canada as fraudsters have, for years, tried to increase wealth — often illegally — at the expense of others. The Canada Revenue Agency (CRA) is often used as a tool to carry out such scams. Consider the following scenario sourced by the CRA:

Amy is a young professional beginning her career after her recent graduation. One day at work, she receives a call from a number that she doesn't recognize. The individual on the line identifies himself as a CRA employee, and claims that Amy has an outstanding debt. He explains that confirmation of Amy's personal information, including her birthdate and bank account, is required to sort out the debt with a re-payment plan.

Amy does not recall owing the CRA money. What's more, she does not remember providing the CRA with her work number. When she voices these concerns, the requester becomes agitated, and warns Amy that there will be consequences if she does not cooperate. Although she is apprehensive, she has never personally dealt with the CRA and assumes the request must be normal. She reluctantly agrees to provide the information.

Many Canadians, including seniors, have received similar telephone phishing calls. Those who are not aware of such scams often experience fear and anxiety which, in some cases, has lead to identity and/or financial theft. Taxpayers should be vigilant when they receive, either by telephone, email, mail or text, fraudulent communications that claim to be from the CRA. Such communications are often seeking personal information such as a social insurance number, credit card number, bank account or passport number, and the communications often involve threatening or coercive language designed to scare individuals into paying a fictitious CRA debt in a timely way.

 $^{^1} See\ here\ for\ federal\ government\ support\ in\ response\ to\ Covid-19:\ https://www.canada.ca/en/department-finance/economic-response-plan.html$

² Royal Canadian Mounted Police.

What to expect from the CRA

To reduce the chance of falling prey to this type of fraud, taxpayers should know what to expect when the CRA contacts them.

By telephone ³		
The CRA may:	The CRA will never:	
 verify identity by asking for personal information such as name, date of birth, address or social insurance number; in the case of a business enquiry, ask for details about an account; call to begin an audit process; call to offer tax help for a small business. 	 ask for passport, health card, or driver's license information; demand immediate payment by e-transfer, bitcoin, prepaid credit cards or gift cards; use aggressive language or threaten with arrest; leave voicemails that are threatening or give personal or financial information. 	

By email ³		
The CRA may:	The CRA will never:	
 notify by email when a new message or a document, such as a notice of assessment, is available for viewing in secure CRA online portals; email a link to a CRA webpage, form, or publication that a taxpayer asks for during a telephone call or meeting with an agent. 	 give or ask for personal or financial information by email and ask taxpayers to click on a link; email a link asking to fill in an online form with personal or financial details; send an email with a link to a refund; demand immediate payment by e-transfer, bitcoin, prepaid credit cards or gift cards; threaten with arrest or a prison sentence. 	

The CRA may:	The CRA will never:
 ask for financial information such as the name of your bank and its location; send a notice of assessment or reassessment; ask for payment of an amount owed through any of the CRA's payment options; take legal action to recover amounts owed if a taxpayer refuses to pay a CRA debt; write to begin an audit process; write to offer tax help for a small business. 	 set up a meeting in a public place to take a payment; demand immediate payment by e-transfer, bitcoin, prepaid credit cards or gift cards; threaten with arrest or a prison sentence.

By text messages/instant messaging³

The CRA **never** uses text messages or instant messaging to communicate with taxpayers under any circumstance. If a taxpayer receives text or instant messages claiming to be from the CRA, they are scams!

³ Source: Canada Revenue Agency (CRA).

Protect yourself from fraud

Regardless of the type of fraud, the Canadian Anti-Fraud Centre has provided the following tips to help Canadians protect themselves from scams and frauds:

Don't be afraid to say no: Don't be intimidated by high-pressure sales tactics and watch out for urgent pleas that play on your emotions.

Do your research: Verify that the organization you're dealing with is legitimate before you take action. Watch out for fake or deceptive ads or spoofed emails.

Don't give out personal information: Beware of unsolicited calls where the caller asks you for personal information. If you didn't initiate the call, you don't know who you're talking to.

Beware of upfront fees: Many scams request you to pay fees in advance of receiving goods, services or a prize. Know that there are no prize fees or prize taxes in Canada – if you won it, it's free.

Protect your computer: Watch out for urgent-looking messages that pop up while you're online. Don't click on them or call the number they provide. Make sure you have anti-virus software installed and keep your operating system up to date.

What to do if scammed

If money or valuables have been lost, or personal information has been provided, contact local police. Also, report the scam to the Canadian-Anti Fraud Centre (https://www.antifraudcentre-centreantifraude. ca/index-eng.htm) even if no money or valuables have been lost or personal information given.

IMPORTANT DISCLAIMERS

This communication is published by CI Investments Inc. ("CI"). Any commentaries and information contained in this communication are provided as a general source of information and should not be considered personal investment advice. Facts and data provided by CI and other sources are believed to be reliable as at the date of publication.

Certain statements contained in this communication are based in whole or in part on information provided by third parties and CI has taken reasonable steps to ensure their accuracy. Market conditions may change which may impact the information contained in this document.

Information in this presentation is not intended to provide legal, accounting, investment or tax advice, and should not be relied upon in that regard. Professional advisors should be consulted prior to acting on the basis of the information contained in this publication.

You may not modify, copy, reproduce, publish, upload, post, transmit, distribute, or commercially exploit in any way any content included in this communication. Unauthorized downloading, re-transmission, storage in any medium, copying, redistribution, or republication for any purpose is strictly prohibited without the written permission of Cl.

CI Investments® and the CI Investments design are registered trademarks of CI Investments Inc. Trusted Partner in Wealth™ is a trademark of CI Investments Inc

©CI Investments Inc. 2020. All rights reserved.

Published May 28, 2020



Vancouver

604-681-3346