Client protection playbook

Common types of scams you should be aware of and how to protect yourself

Book 2 of 3

Table of contents

Message from Keith Gordon

Executive Vice President & Chief Security Officer,
Canadian Imperial Bank of Commerce (CIBC)

Technology plays a big role in our everyday lives - from checking our bank account balances online to streaming our favourite movies. With the advancement of technology, it brings about extraordinary benefits to our lives and shapes the world we live in. At CIBC, we continuously embrace new technology and security features that help make your ambitions a reality by protecting your money and information.

With technology evolving, so are the strategic tactics of fraudsters. According to the Canadian Anti-Fraud Centre and the Federal Trade Commission, North Americans lost just over $6 billion to fraud last year. Since the pandemic began, the global volume of online transactions has increased significantly, and while that's been convenient for consumers and essential for businesses, it's also created an ideal environment for fraud to escalate. Fraudsters are constantly trying to find new ways to scam people out of money and obtain their personal and banking information. At CIBC, we work around the clock to stop fraudsters and keep our clients safe.

Cyber security impacts everyone and cyber security threats represent one of the most significant risks that financial institutions face today and require constant vigilance and improvement to stay ahead in the current environment. As such, CIBC regards information & cyber security as a core capability. The protection of our systems and information is one of our strategic objectives and is part of our organizational DNA. We're constantly improving how clients can bank safely and securely - but the first line of defense starts with you.

Increasing your fraud knowledge decreases your chances of falling for a scam. Knowing how to prevent, identify and respond to fraud is essential for your defense against fraud. As fraud comes in many different forms, it's important to understand different tactics fraudsters use to try to trick people. Use this playbook as a guide to enhance your fraud knowledge, as you'll learn how to identify common types of scams and tips to protect yourself, so you'll know a scam when you see one.

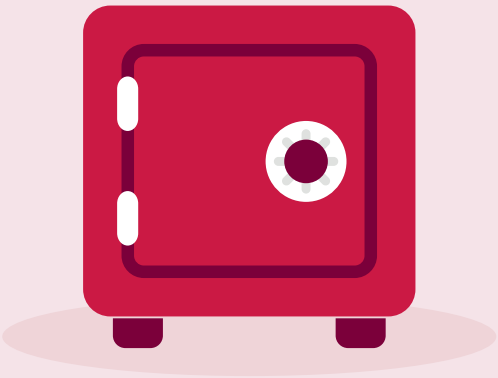
Let's work together and keep everyone safe.

Keith Gordon

Background information on scams

With the ongoing enhancements to technology, social media, and e-commerce, personal and banking information is at risk of being stolen every day. Fraudsters continually create new and evolving schemes aimed at illegally obtaining and exploiting victims' personal information, with the goal of financial gain.

CIBC is committed to keeping you and your banking information safe and providing you with information about the risks that may affect you.



so·cial en·gi·neer·ing
/ˈsōSHəl ˌenjəˈni(ə)riNG/

The use of psychology to manipulate our human instinct to respond to urgent requests and fear, so that victims are lured into revealing confidential information that may be used to commit financial fraud.

The basis of many scams

Fraudsters use **social engineering** tactics in order to take advantage of and obtain confidential information from victims. Tactics are often in the form of suspicious emails, calls and text messages that may impersonate family members, friends, government agencies and financial institutions. Once fraudsters obtain confidential information, they will use it to commit financial fraud and deplete their victims' funds.

Here are three key characteristics of social engineering techniques:

Using fear as a motivator by sending threatening emails, phone calls or texts to scare you into revealing information or conducting transactions.

Urgent and unexpected requests for personal or business information through written communications, such as email or text messages.

Offers, prizes or contests that sound too good to be true, often claiming to provide a reward in exchange for login credentials or other personal or business information.

Know the signs:

Red flags that may indicate you are dealing with a fraudster

Requests to conduct a wire transfer or pay using untraceable methods

Scams typically request victims to send money through *Interac* e-Transfer®, purchasing prepaid gift cards, or the transfer of cryptocurrencies, due to their nature of being untraceable and often irreversible once sent. Beware of requests to transfer money electronically.

Suspicious and unsolicited emails, text messages or telephone calls

Be skeptical of calls, emails or text messages from individuals or entities claiming you owe taxes, your accounts have been suspended or compromised, your package delivery has been missed, you have unauthorized charges on your credit card, or that you are being offered a job that offers high pay for little to no work. These communications purposely instill a sense of urgency and lure you into clicking a suspicious link that can download malware onto your devices, or providing sensitive information, such as your social insurance number, driver's license or bank accounts. Take note of spelling or grammar errors, and email and web addresses and examine whether there are subtle mistakes or differences.

An offer that sounds too good to be true

Promotions, investment opportunities, or sales that sound too good to be true, are likely just that. Fraudsters want you to respond quickly to a time-sensitive deal or a "once-in-a-lifetime" opportunity that does not exist so that you are pressured to conduct transactions or provide information without considering whether the offer is legitimate.

Buyers want to overpay you

When selling items online, be cautious of buyers who overpay you for an item and request you to send back the difference or ask you to cover the transportation costs, promising to reimburse you after the product is delivered. A fraudster may send you a counterfeit cheque for an amount greater than the price you advertised and ask you to deposit the cheque and wire the excess funds immediately back to them. Once sent to the fraudster, they will cease all communication before the cheque bounces, leaving you on the hook for the deposited and out of the money transferred.

Online best practices:

Keep your money and your information safe by following the best practises below

- Do not share One-Time Verification Codes (OTVC) with anyone.
- Set up *Interac* e-Transfer Autodeposit to ensure funds sent to you are automatically deposited into your bank account.
- Never click on an attached link inside an email to visit a website – type the address into your browser instead.
- Keep your passwords secured offline, or in a reputable password manager.
- Do not respond to or click on pop-up messages claiming your computer is at risk.
- Check monthly banking statements regularly for any unauthorized charges.

How CIBC protects you from identity theft and fraud

CIBC and other legitimate entities will never contact you and ask you directly for your personal or banking information – do not share these details with those claiming to be from legitimate companies.

Enroll in CIBC's MyAlerts on mobile or online banking to monitor suspicious activity on your banking accounts.

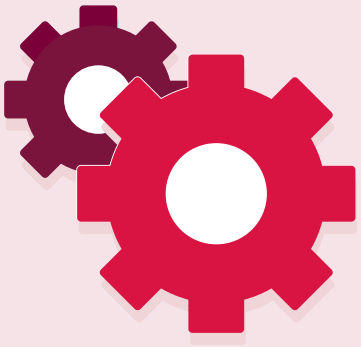
Sign up for CIBC's voice verification security feature to bank faster, securely, and protect yourself from fraud. *Must be 13 or over to enroll (Quebec: must be 14 or over).*

Opt-in to CIBC's push notifications on mobile banking to receive One-Time Verification Codes (OTVC) when conducting high-risk transactions.

Subscription traps

How it works

In a subscription trap, fraudsters and deceptive companies advertise products online as “miracle products” with convincing benefits and may even include fake celebrity endorsements. Victims are offered a “limited-time free trial” of the product with no strings attached, only paying for a small shipping and handling fee.



Hidden in the fine print or terms and conditions, once consumers provide their credit card and complete their order, they agree to pay expensive, monthly subscriptions to products – and in some cases, automatically pay for upsell products they did not order at all. Victims end up being locked into large recurring payments and many face difficulties contacting the seller to stop the subscription and obtain a refund.

Common products advertised in subscription traps:	Dietary supplements	Weight loss products	Muscle-enhancement pills	Anti-aging facial products
Red flags to look for				
The product is advertised as a free trial and the customer only pays for shipping/handling	✕	✕	✕	✕
Website or advertisement creates a sense of urgency using methods such as a countdown timer	✕	✕	✕	✕
Terms and conditions, return policies and contact information are difficult to find or understand	✕	✕	✕	✕
Company has little to no online reviews, poor grammar in their communications and web design, or were mentioned in scam complaints	✕	✕	✕	✕

Protect yourself from subscription traps

1. Identify any red flags

Check for any elements of the subscription offer that seem fishy from the outset.
Ask yourself:
- What exactly am I being offered, and at what price?
- Is the offer clear and easy to understand?
- Does the product promote outlandish health claims or other benefits?
- What does a quick Google search say about this specific company or product?

2. Dig deeper

Read the terms and conditions of the offer carefully before proceeding with the offer. Search for independent reviews of the product and the company on Google along with keywords such as “scam” or “fake”. If there are little to no reviews of the product or you find multiple complaints associated with the company, do not proceed with the offer.

3. Slow down. Don’t rush.

Never complete an order or sign up for a subscription because you feel pressured. Fraudsters will use methods such as a countdown timer on the product website or phrases like “OFFER ENDS SOON” to urge consumers to act quickly.
Proceed with an offer only after you have confirmed its legitimacy, read all the terms and conditions, and fully understand what is being presented.

4. Be cautious

Always be skeptical of websites that promote products with health claims and other benefits not supported by science. Verify the accuracy of the claims made using resources such as published medical journals from reputable researchers, and consult your healthcare provider if you are still unsure. Do not fall for celebrity endorsements, as they are difficult to validate and should not hold any merit in the efficacy of a product.

If you have decided to proceed with a product trial, closely monitor your monthly banking statements for extra charges or unwanted subscription fees made to your credit card.

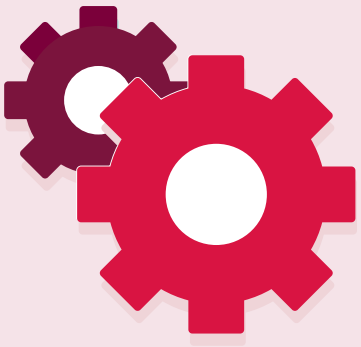
5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion. If you remain unconvinced or suspicious, do not proceed with purchasing a subscription and ignore all communications.

Investigator scams

How it works

In an investigator scam, victims receive a call from a fraudster who knows their name, claiming to be from their financial institution, law enforcement, or a merchant. Their main goal is to persuade victims to send funds to them via *Interac* e-Transfer, cash withdrawals, the purchase of gift cards, or reveal personal and banking information.



Fraud prevention around OTVC deception

Fraudsters may contact you, pretending to be a member of CIBC's fraud team. They may claim your account's been compromised due to suspicious activity. They may also ask you to share a 6-digit one-time verification code with them to protect your account. If anything like this happens, disconnect the call immediately and call the number on the back of your card.

Variations of the bank investigator scam	
Fraudster claims to be from a financial institution investigating a series of fraud cases and asks the victim to wire money out of their account to assist with the investigation, which will be used as evidence to catch the fraudster.	✕
Fraudster deposits money into the victim's account using fraudulent cheques or the victim's own loan products, pretending they sent it to them accidentally. Then, they request the victim to wire the money back to the fraudster or purchase gift cards.	✕
Fraudster claims to be from a major credit card provider and says that there are unauthorized charges on the victim's account. They then demand the victim provide their credit card information.	✕

Red flags to look for	
Victim is told that information must be kept confidential from the Banking Centre	✕
Requests for personal or banking information, or one-time verification codes	✕
Requests to transfer money, withdraw cash, or purchase gift cards to assist with an investigation	✕
Offers of financial compensation for participating in the investigation from a law enforcement investigator	✕
Requests to download software onto the victim's computer	✕

Protect yourself from investigator scams

1. Identify any red flags

Legitimate financial institutions and law enforcement organizations would never ask you to conduct financial transactions to help in a fraud investigation. If you receive contact and are asked to do so, **ask yourself:**

- Why am I being asked to withdraw or send money to help with an investigation? Why would my personal credentials be relevant?
- Why would my financial institution offer me compensation to assist with an internal investigation? Why would I be asked to lie to anyone at the Banking Centre?
- Does the email or text message seem suspicious? Am I being asked to click on an attached link and download software?

2. Dig deeper

Closely examine the contents of an email or text message and identify whether it seems suspicious. If you receive a call, identify whether the caller is using fear, urgency, or offers that sound too good to be true to persuade you to perform financial transactions or reveal personal and banking information.

3. Slow down. Don't rush.

Take time to think carefully about what is being asked of you and whether it makes sense. Fraudsters will often try to get you to respond to their requests by changing topics frequently during a conversation, or by pressuring or instilling fear in you. Do not fall for their tactics; take control of the situation by taking time to think about the information presented to you.

4. Be cautious

- If you are being pressured to conduct transactions or withdraw money and keep all activities confidential from family, friends, and your financial institution, it is likely a scam.
- Be wary of emails or text messages that claim to be from a financial institution, law enforcement agency, or credit card provider. Closely examine the email addresses and elements of the website that seem suspicious.
- Deny requests to provide confidential information, withdraw or transfer money, or download software onto your computer.

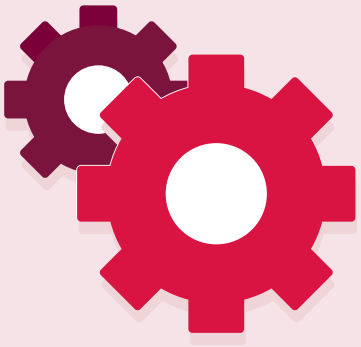
5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on the communications or offers presented to you, and whether they make sense. If you remain unconvinced or suspicious, deny the request altogether, or contact your financial institution or credit card provider to confirm.

CRA / Tax scams

How it works

In a CRA scam, victims receive fraudulent communications from individuals that claim to be from the Canada Revenue Agency (CRA). Scammers insist that personal information is needed for the victim to receive a tax refund, or they must pay outstanding taxes immediately or face extreme consequences. Scammers will often direct the victim to send funds via *Interac* e-Transfer, a prepaid gift card, or cryptocurrencies such as Bitcoin.



Fraudsters use different methods of communication, such as by **phone, text, email or letter**, to pose as the CRA. By persuading victims that they owe fictitious debt or need to collect their tax refund, fraudsters can obtain their personal information such as their SIN or credit card number and use them for financial gain.

Who it affects

CRA scams can affect anyone – however, those most commonly targeted are seniors, newcomers to Canada, and small business owners or self-employed individuals.

Red flags to look for	Seniors	Newcomers to Canada	Small business owners
The caller contacting you cannot provide you proof of working for the CRA, such as name and office location.	✕	✕	✕
The caller is asking for information you would not include on your tax return (i.e. credit card number).	✕	✕	✕
The caller is asking you to pay with prepaid cards, cryptocurrency or other unconventional method, and is pressuring you to act quickly.	✕	✕	✕
The caller is offering to apply for Government of Canada benefits on your behalf and requests your personal information.	✕	✕	✕

Protect yourself from CRA scams

1. Identify any red flags

Before giving over money or personal information to someone claiming to be from the CRA, **ask yourself**:

- Am I being threatened with arrest, pressured or urged to immediately pay outstanding taxes through unusual payment methods?
- Is the caller unable to confirm their identity as a CRA agent with a name, telephone number and office location?
- Am I being asked for information that I would not include in, or does not relate to my tax return, such as my passport or driver's license number?
- Am I being sent an email that asks for my personal or banking information, or that asks me to click on a link to fill in personal details?

2. Dig deeper

It is important to investigate the situation and confirm whether a CRA communication is legitimate before providing personal information.

Dig deeper by determining whether you should be expecting a call from the CRA. For example, request the caller to explain the purpose of the call while checking to see whether you've received a letter stating that your tax return is being reviewed by the CRA. If you signed up for email notifications, check to see if you recently received an e-letter by signing in to CRA's MyAccount.

3. Slow down. Don't rush.

Take time to think carefully about what is being requested and whether it makes sense. It is important to remember that the CRA will never demand immediate payment over the phone, use aggressive language, threaten you with arrest, or leave threatening voicemails. The CRA will also never send you an email requesting personal information or ask you to click on a link to complete an online form providing personal or banking details. If you receive any of these types of communications, it is likely a scam.

4. Be cautious

If you receive a call from someone claiming to be a CRA agent:

1. Notify the caller that you would like to first verify their identity
2. Ask for, and make note of their name, phone number, and office location
3. Check that the information you received was legitimate by contacting the CRA at the number that you have sourced on CRA's website
4. Request the CRA employee to discuss the reason for the call

If you receive an email claiming to be from the CRA:

- Verify the email address and determine whether it looks suspicious
- Ignore emails that request personal information or ask you to click on a link to provide personal information

Visit the CRA's website to learn more:
What to expect when the Canada Revenue Agency contacts you

5. Verify with a trusted individual

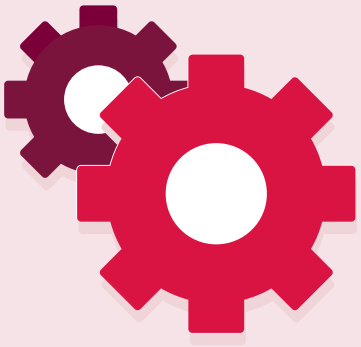
When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on messages, calls or other forms of unsolicited contact that you are not sure are legitimate. If you are still unsure, deny any requests for personal information and contact the CRA through the number on their website to confirm details.

Tech support scams

How it works

In a tech support scam, fraudsters reach victims via telephone, email, or using computer pop-up messages claiming to be representatives of well-known technology companies. Using various technical words, they convince the victim that their computer is at serious risk and they must provide personal information, user credentials, or download an application allowing remote access to their computer for the fraudster to remedy the issue.

With the level of technology available today, fraudsters are also capable of spoofing caller ID numbers to match that of legitimate companies, and create phony websites of real companies that look legitimate.



Common tactics fraudsters use in tech support scams

Enrolling the victim in a worthless or fake computer maintenance program in exchange for a fee	✕
Requesting credit card information to bill the victim for fake or worthless services	✕
Directing the victim to phony websites that ask the victim to enter their personal or banking information	✕
Installing programs disguised as malware that allows remote access to the victim's computer and its sensitive data	✕

Red flags to look for

A pop-up message stating that your computer is at risk, prompting you to install software or click on a link	✕
Offers of financial compensation for participating in an investigation from a law enforcement investigator	✕
An unsolicited call or email from someone selling software or repair services, requesting information, or convincing you to download an application	✕
Receiving a tech support call when you are not expecting one or have not scheduled an appointment for one	✕

Protect yourself from tech support scams

1. Identify any red flags

It is important to understand that legitimate technology companies will not contact you by phone, email or text messages to claim that your computer is at risk. Their security po-up messages will also not ask you to click on an external link. Before responding to tech support communications, **ask yourself**:

- Am I being contacted from a technician who is trying to sell me software or services and pay for them by gift card or wire transfer?
- Does the pop-up message ask me to download a program on my computer to remove viruses or click on a link?
- Does the email or text message seem suspicious? Am I being asked to click on an attached link and download software?

2. Dig deeper

Closely examine the contents of an email or text message and identify whether it seems suspicious. If you receive a call, determine whether the caller is using fear, urgency, or offers that sound too good to be true to persuade you into performing financial transactions, paying for services you do not need, or revealing personal and banking information.

3. Slow down. Don't rush.

Take time to think carefully about what is being asked of you and whether it makes sense. Fraudsters will often try to get you to respond to their requests by changing topics frequently during a conversation, or by pressuring or instilling fear in you. Do not fall for their tactics; take control of the situation by taking time to think about the information presented to you.

4. Be cautious

- If you are receiving an unsolicited call, email, or text message claiming your computer is at risk and are asked to download software, it is likely a scam.
- **Recent twists of this scam involve unsolicited emails claiming your account** (i.e. Netflix, iTunes, Zoom, social media, etc.) has been suspended. Do not click on suspicious links attached, as they may install malware that allows fraudsters remote access to your computer.
- Deny requests to provide confidential information, purchase gift cards or conduct wire transfers, or download unfamiliar software onto your computer.

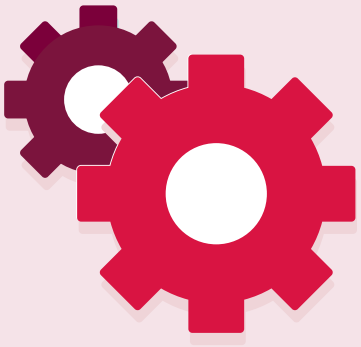
5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on the communications or offers presented to you, and whether they make sense. If you remain unconvinced or suspicious, deny the request altogether.

Loam scams

How it works

In loan scams, fraudsters create fake loan advertisements or contact victims directly via phone or email, posing as a legitimate lender and offering better loan rates than other companies. Fraudsters lure the victim by informing the that they have been approved for a loan, or can be guaranteed loan funds without a credit check in exchange for an advance or upfront fee. After the victim accepts the fake offer and pays the upfront fee through the fraudster's preferred method of payment, the fraudster stops all communication with the victim and is never heard from again.



Common types of loan scams

Auto loan scam	✕	Student loan scam	✕
Mortgage loan scam	✕	Personal loan scam	✕
Payday loan scam	✕		

Red flags to look for

Unsolicited loan approvals; you are congratulated via phone or email for being approved for a loan you did not apply for	✕
You cannot find reviews of the lender and the lender has virtually no online presence	✕
Urgency, or aggressive sales tactics employed by the lender, claiming the loan offer expires soon	✕
The lender is requesting an upfront payment or advance fee before providing the loan, and accepts payment via Bitcoin, gift cards, or *Interac* e-Transfer	✕

Protect yourself from loan scams

1. Identify any red flags

When obtaining a loan, it is important to understand the offer and whether it is legitimate before proceeding.

Ask yourself:

- Is the lender promising a loan approval from the outset without the need for a credit check?
- Am I being asked to pay an advance fee before receiving loan funds?

> **NOTE:** it is illegal for lenders in North America to request an advance fee or upfront payment before consumers receive the loan. Although many loans do have processing fees, legitimate lenders would deduct these from the loan proceeds. (Source: Better Business Bureau)

- Are there incomplete or no contracts to sign? Does the contract have pre-checked boxes?

2. Dig deeper

Verify the authenticity of the lender by researching whether they are a registered lender in Ontario or accredited by the Better Business Bureau.

Search for reviews of the lender online, and identify whether the lender has an online presence. Closely examine the terms of the loan and whether it makes sense.

3. Slow down. Don't rush.

Take time to think carefully about what is being asked of you, and whether it makes sense or sounds too good to be true. Fraudsters will often try to get you to act quickly to their requests by changing topics frequently during a conversation, or by pressuring or instilling fear in you. Do not fall for their tactics; take control of the situation by taking time to think about the information presented to you.

4. Be cautious

- If you have been contacted about a loan you did not apply for, it is likely a scam. Ignore the communication and do not provide personal or banking information.
- Be wary of lenders who promise access to loan funds, provide approvals with no credit checks required, and request for advance fees or upfront payments before receiving loan funds.
- If it sounds too good to be true, it probably is! If you feel suspicious of a loan offer, it's best to reject it altogether.

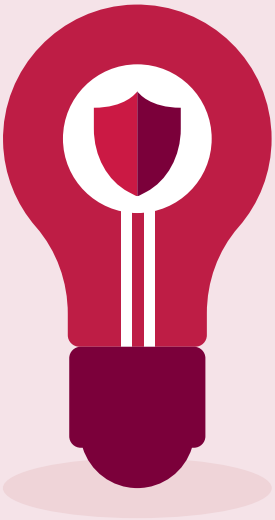
5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on the loan offer presented to you, and whether they are familiar with the name or reputation of the lender. If you remain unconvinced or uneasy about the terms of the loan, reject the offer and stop all communication with the lender.

Know your fraud, before it knows you

We would like to remind you that you must immediately report any actual or suspected fraud and unauthorized activity on your accounts and debit and credit cards, the loss or theft or cards, and if your card details or PINs are compromised. You must immediately replace your debit card or credit card and change your PINs and banking passwords.

To learn more about resources available to you or how CIBC can help if you are a victim of fraud, please refer to the information below or visit **cibc.com/fraud**.



Stay in the know, wherever you go

Stay on top of your purchases, credit card activity or other transactions that seem out of place with CIBC Alerts via the mobile banking app. By setting up custom alerts tailored to you, we notify you in real-time by text, email or phone if a transaction seems unusual. If it is fraud, we will connect you to a fraud specialist.

Interested in signing up or learning more? Visit our **CIBC Alerts page**.

How CIBC can help

Please contact CIBC at **1 800 872-2422** or email us at **fraud@cibc.com** immediately if you believe you have been a victim of fraud, your accounts have been compromised, or your identity has been stolen.

If you receive fraudulent emails and text messages or would like to report fake websites posing as CIBC, please email us at **fraud@cibc.com** describing the fraudulent incident and attach or include any fraudulent emails or website links you encountered for analysis.

Additional resources

To report fraud, contact the Canadian Anti-Fraud Centre at **1 888 495-8501**, or visit **AntiFraudCentre.ca**.

For the Better Business Bureau (BBB)'s Scam Tracker and Scam Tips, visit:
BBB.org/ScamTracker or **BBB.org/ScamTips**

For more fraud tips, visit:

Competition Bureau Canada	**CompetitionBureau.gc.ca**
Royal Canadian Mounted Police	**RCMP-GRC.gc.ca**