What to do if you're a victim of a scam or a financial fraud – a guide

Wealth Management

Helping you recover from fraud and scams

Below is a checklist to help you report fraud and scams, as well as protective measures to take moving forward. Use the notes section at the end of this guide to document your actions, conversations, and any next steps.

General advice for fraud and scam victims

- ☐ Notify your RBC Dominion Securities Investment Advisor (IA)/RBC PH&N Investment Counsel Investment Counsellor (IC) and all financial institutions that facilitated transactions related to this scam or fraud.
  - — Report unauthorized or fraudulent activity immediately.
  - — Ask if you are able to file a claim or if the funds can be recalled or recovered.
  - — Seriously consider having a trusted contact person on file with your IA/IC as an extra layer of protection in case you can't be reached.
- ☐ Immediately cut off all contact with any scammers/fraudsters as they will have an explanation for everything and will keep harassing you. Once they obtain funds from a victim, they often come back with a new excuse, emergency, or request.
- ☐ Contact your local police service to file a police report.
- ☐ Contact the Canadian Anti-Fraud Centre (CAFC) to report. See the Reporting to the Authorities section on page 4.
- ☐ If your personal information or devices were hacked or compromised, follow the Recovering from identity theft or compromise checklist on page 3.

If the fraudsters made contact by phone

- ☐ Block the numbers they are calling from and don't answer calls from numbers you don't recognize.
- ☐ Contact your phone carrier to alert them to the issue, ask them to report the phone number and help you identify and filter out other potential scam numbers.
- ☐ If the calls continue, consider changing your phone number.

If the fraudsters made contact by email or over the internet

- ☐ Block the email address they are communicating from.
- ☐ Make your public profiles private and/or remove any personal details.
- ☐ Report scams, fraud and harassment to the company that owns the website or email provider.

Continue to be vigilant

Fraudster will often target the same individuals. The scammers often impersonate government agencies, fraud departments or attorneys and claim they can get your money back or ask you to secure additional money in safe accounts. If this happens to you, ask to meet in person at your local police station or at the financial institution named before giving any information or funds.

Helping you recover from identity theft and how to report to the authorities

It is critical to report fraud, scams, and identity theft to help investigators build cases against fraudsters and scammers and to stop them.

If you believe you have been a victim of an identity compromise or identity theft, follow the checklist below to help you recover. Also use the notes section at the end of this toolkit to document your conversations and any next steps.

- ☐ Notify your RBC Dominion Securities Investment Advisor (IA)/RBC PH&N Investment Counsel Investment Counsellor (IC) regarding any compromised personal information and review your account activity.
  - For phishing* attempts, report to phishing@rbc.com
  - Report any suspicious or unauthorized activity and cancel any compromised debit and credit card or chequing/ cheque book account numbers.
  - Make sure to have a trusted contact person on file with your IA/IC as an extra layer of protection in case you can't be reached.
- ☐ Change your online passwords and notify all of your financial institutions that your personal information has been compromised.
  - Follow proper password maintenance: Why Strong Passwords Matter – and How to Create Them
- ☐ To report a fraudulent communication, or if your identity was stolen as part of a scam, please contact the Royal Canadian Mounted Police's Phone Busters by email at info@phonebusters.com or call 1-888-495-8501.
- ☐ **Canadian Anti-Fraud Centre (CAFC):** Assists law enforcement through maintaining a central repository of information to assist with investigations.
  - Call 1-888-495-8501 or report a scam or fraud online at https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm
- ☐ Obtain a report of your banking account history and review it for unauthorized banking activity.
- ☐ Contact credit bureaus to place fraud alert notices or to freeze your credit:
  - **Equifax:** 1-877-323-2598 or https://www.consumer.equifax.ca/personal/contact-us/
  - **TransUnion:** 1-877-525-3823 or https://www.transunion.ca/assistance/fraud-victims-resources
- ☐ If any devices were hacked or compromised, consider having a professional cybersecurity service inspect your device for spyware/malware.
  - Make sure your device security software and internet browsers are up to date.

Continue to monitor for unauthorized activity

Review your accounts, credit reports and banking history and report any suspicious or unauthorized activity promptly.

***Phishing:** a cyberattack method where attackers pose as legitimate individuals, organizations, or entities to deceive people into revealing sensitive information such as passwords, credit card numbers, or personal details. Victim often thinks they are interacting with a trusted source, when in reality, they are providing information to malicious actors.

Additional resources

- ☐ Canadian Anti-Fraud Centre: https://www.antifraudcentre-centreantifraude.ca/
- ☐ Canada Revenue Agency: https://www.canada.ca/en/revenue-agency/services/forms-publications/publications/rc284/protect-yourself-against-identity-theft.html
- ☐ Office of the Privacy Commissioner of Canada – Identity Theft and Fraud: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/
- ☐ Canadian Resource Centre for Victims of Crime:
  - Elder Abuse: https://crcvc.ca/wp-content/uploads/2021/09/Elder-Abuse_-DISCLAIMER_-Revised-April-2022_-FINAL-1.pdf
  - Cyberstalking: https://crcvc.ca/wp-content/uploads/2021/09/Cyberstalking-_DISCLAIMER_Revised-Aug-2022_FINAL.pdf
- ☐ Government of Canada – Competition Bureau – Little Black Book of Scams: https://ised-isde.canada.ca/site/competition-bureau-canada/en/little-black-book-scams-2nd-edition
- ☐ RBC resources:

Updated Scams/ Frauds:

- Stay Informed on the Latest Cyber Scams: https://www.rbc.com/cyber-security/alerts/index.html
- Be Cyber Aware: https://www.rbc.com/cyber-security/index.html
- Privacy & Security Canada – Protecting Yourself: http://www.rbc.com/privacysecurity/ca/protecting-yourself.html

How to protect yourself:

- My Money Matters – Understanding Cyber Safety: https://www.rbcroyalbank.com/en-ca/my-money-matters/money-academy/cyber-security/understanding-cyber-security/
- Fraud Prevention: 5 Common Scams and How to Defend Against Them: https://discover.rbcroyalbank.com/fraud-prevention-5-common-scams-and-how-to-defend-against-them/
- The Vault – A cyber safety playbook: https://www.rbc.com/cyber-security/_assets-custom/pdf/cyber-playbook.pdf?_gl=1*1sslska*_ga*MjEyMTEyMjkzNC4xNjgxODMyMTQ1*_
- 5 Ways to Spot a Romance Scam: https://discover.rbcroyalbank.com/5-ways-to-spot-a-romance-scam/

Reporting notes

Use this page to take notes and track your progress. For your safety, do not write down usernames, passwords, PINs, or account numbers.

- ☐ Report any suspicious activity, unauthorized transactions or funds that went to suspected scams or compromised your personal information.
- ☐ If you were a victim of a scam or fraud, ask the relevant financial institution or agency if the funds can be recalled or recovered.
- ☐ Ask each agency/contact if there are any additional steps recommended to help you safeguard your information and assets moving forward.

Company/agency contacted	How to contact (phone number, email)	Contact person's name	Claim/case/ tracking number	Date/time contacted

If you suspect a scam always report it!

Strengthening your financial security

www.rbcwealthmanagement.com

RBC Wealth Management