COMPANION RESOURCE · APPENDIX D

Scam Response Checklist

What to do in the first hour, and the red flags to watch for

From *Holiday Money Without the Regret* by P.J. Whitfield, Cogitent Press. Print as many copies as you need for your own use.

If you think you have been scammed

Act quickly. Every hour can matter.

1. **Stop all contact** with the scammer. Do not reply, click, or call back.
2. **Call your bank or credit card issuer immediately.** Use the number on the back of your card or on the official website, not a number the scammer gave you. Ask them to block the transaction, freeze or replace the card, and monitor the account.
3. **If you paid with a gift card,** contact the card issuer with the card number and any receipt, and ask whether the funds can be frozen.
4. **If you sent an e-transfer,** contact your financial institution at once. Recovery is difficult, but a fast report gives the best chance.
5. **If you shared passwords,** change them now, starting with email and banking. Turn on two-factor authentication.
6. **If you gave out personal information,** such as your Social Insurance Number or ID details, contact Equifax Canada and TransUnion Canada to place a fraud alert on your file, and consider reviewing your credit reports.
7. **If you clicked a link or installed something,** run a security scan on your device and change your passwords from a different, secure device.
8. **Keep evidence:** screenshots, messages, receipts, phone numbers, website addresses, and payment details.
9. **Report it** to your local police and to the Canadian Anti-Fraud Centre at 1-888-495-8501 or through its online reporting system. Report even if you lost no money.
10. **Forward scam texts** to 7726 (SPAM).
11. **Tell someone you trust.** Scammers rely on shame and secrecy.
12. **Do not pay anyone who offers to recover your money.** That is a second scam.

The red-flag list

Stop and verify if any of these are true.

- You were contacted out of the blue.
- You are told to act immediately, or to keep a secret.
- You are asked for payment by gift card, cryptocurrency, wire transfer, or e-transfer.

- The price, prize, or return is too good to be true.
- A message contains a link to "verify" or "claim" something.
- The caller threatens arrest, account closure, or legal action.
- You are asked for passwords, PINs, or one-time codes. Real organizations do not ask for these.
- The "relative" in trouble cannot be reached any other way.

Numbers to know

Who	Contact
Canadian Anti-Fraud Centre	1-888-495-8501
Report spam text messages	Forward to 7726 (SPAM)
Equifax Canada	Search the official site for the fraud alert page
TransUnion Canada	Search the official site for the fraud alert page
Your bank or card issuer	The number on the back of your card
Local police	Non-emergency line, or 911 if you are in danger

© 2026 Cogitent Inc. P.J. Whitfield is a pen name of Cogitent Inc., published under Cogitent Press. General information only; not personal financial, tax, or legal advice. Figures and rules checked as of October 2026 and may change. Confirm anything that affects your money with the Canada Revenue Agency, the Financial Consumer Agency of Canada, or a qualified professional.