CANADIAN ANTI-FRAUD CENTRE
CENTRE ANTIFRAUDE DU CANADA

Fraud Trends – First 6 Months of 2026 2026-08-27

FRAUD: RECOGNIZE, REJECT, REPORT IT LA FRAUDE: IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

The Canadian Anti-Fraud Centre (CAFC) continues to see significant financial losses associated with fraud in 2026. In the first six months of the year, Canadians reported approximately $351 million in losses to the CAFC. While investment fraud continues to account for the highest reported dollar loss, several fraud types are showing notable activity when compared with 2025, including spear phishing, bank investigator fraud, extortion and recovery fraud. These figures represent only reported incidents; the CAFC estimates that only 5% to 10% of fraud is reported, meaning the actual impact is likely much greater.

Fraudsters continue to use impersonation, urgency, convincing communications and established trust to obtain money or personal information. In many cases, criminals impersonate financial institutions, businesses, government or law enforcement, employers, service providers, or individuals known to the victim. Canadians should be cautious of unexpected requests involving money, changes to payment instructions, investment opportunities, account security concerns or claims that previously lost funds can be recovered.

Trends standing out in the first half of 2026

<u>Investment fraud</u> - approximately $139.6 million reported lost
Remains the fraud type with the highest reported financial losses in the first six months of 2026. Fraudsters may use social media, online advertisements, messaging applications or impersonation to promote fraudulent investment opportunities, including cryptocurrency-related investments. Victims may initially see fake account balances or returns designed to encourage additional deposits.

<u>Spear phishing</u> - approximately $57.7 million reported lost
Continues to cause significant losses. In all of 2025, reported losses exceeded $68 million, while approximately $57.7 million has already been reported during the first six months of 2026. These frauds often involve compromised or spoofed communications and may target businesses by impersonating executives, suppliers, contractors or other trusted contacts to redirect payments or change banking information.

<u>Bank investigator fraud</u> — approximately $28.6 million reported lost
Continues to stand out in 2026. Reported losses were approximately $28.3 million in 2025, compared with approximately $28.6 million in only the first six months of 2026. Fraudsters may impersonate a financial institution, police or another trusted organization and claim a victim's account has been compromised. Victims may then be instructed to transfer money, provide banking information or participate in a supposed investigation.

Extortion — approximately $25.5 million reported lost
Losses to extortion frauds during the first half of 2026 have already exceeded the approximately $23 million reported during all of 2025. Extortion can take many forms, including threats, impersonation and false allegations designed to pressure victims into sending money quickly. Fraudsters may also impersonate law enforcement and threaten arrest, deportation or other legal consequences if payment is not made.

Recovery fraud — approximately $13.7 million reported lost
Victims who have already lost money to fraud may be targeted again. Fraudsters may claim to represent law enforcement, government agencies, financial institutions or recovery organizations and promise to recover previously lost funds in exchange for fees, taxes, deposits or other payments. Approximately $13.7 million was reported lost to recovery fraud in the first six months of 2026, compared with approximately $25.9 million during all of 2025. The CAFC has also warned that fraudsters may impersonate the CAFC itself when carrying out recovery fraud.

Warning signs

- Unexpected requests to send, transfer or withdraw money
- Pressure to act immediately, secretly or outside normal procedures
- Requests to change banking or payment information
- Unsolicited investment opportunities promising high or guaranteed returns
- Calls claiming your bank account is compromised and asking you to assist with an investigation
- Requests to pay fees or taxes to recover money previously lost to fraud
- Communications that appear to come from a trusted organization but contain unusual instructions
- Requests for passwords, verification codes, remote access or sensitive financial information

How to protect yourself

- Slow down and independently verify unexpected requests before taking action.
- Contact businesses, financial institutions and government agencies using contact information you locate yourself.
- Never transfer money to a so-called safe account at the direction of an unexpected caller.
- Verify changes to payment or banking information directly with the person or business involved using a known contact method.
- Be cautious of investment opportunities received through social media, online advertising or unsolicited messages.
- Never pay someone upfront to recover funds you previously lost to fraud.
- Do not provide passwords, verification codes or remote access to your devices.
- Talk to a trusted person before sending money when you are being pressured or threatened.

If you believe you have been a target of fraud, contact your financial institution immediately and report the incident to your local police and the Canadian Anti-Fraud Centre.