What to Do if You're a Victim of Financial Fraud

Moving billing and accounts online has made it easier for abusers to change account settings, stop payments, and impersonate survivors. Scams by strangers who misuse technology to gain access to financial information or trick people into sending them money are also increasingly common and hard to identify.

This info sheet provides some tips for survivors of financial fraud facilitated through technology.

Gather Important Information

If you are a victim of fraud, gathering critical details and preserving digital evidence are the first steps toward recovery. Make sure you have the following:

- All documents and receipts related to the fraud, such as credit card and bank account statements and/or credit report.
- Copies of emails, text messages, or other correspondence with the abuser.

For more information about how to preserve and document digital evidence such as emails, texts, and voicemails, check out our Preserving Digital Evidence Toolkit.

Contact Your Financial Institutions Immediately

Report the fraud to any financial institution that may be impacted. Many banks have ways for you to report fraud or dispute a transaction online or by calling them. Let them know as soon as possible so they can take action to protect your accounts.

Update Account Information to Prevent Further Access

- Flag all accounts by contacting your bank, credit card companies, and other places to put fraud alerts on your banking and credit accounts.
- Change passwords and PINs on all of your accounts.

- Notify Credit Bureaus by calling Equifax and TransUnion to report the identity theft and request a fraud alert on your credit profile.

Report the Fraud to the Police

Contact your local police department to provide an official report. Ask for a file number to update the report or refer to later if necessary.

Report to the Canadian Anti-Fraud Centre

Report fraud to the Canadian Anti-Fraud Centre by calling toll-free at 1-888-495-8501 or through the Fraud Reporting System, accessible online. They can offer support to safeguard your accounts to prevent further scams.

Report Specific Types of Fraud to Relevant Agencies

- **Online Fraud Through Websites:** Report fraudulent activity to the website administrator. Look for links labelled “Report Abuse” or “Report an Ad.”
- **Redirected Mail:** If you believe your mail was redirected without your permission, contact Canada Post.
- **Identity Theft with Service Providers:** Notify your cell phone, utility, and other service providers if your identity has been misused.
- **Immigration Documents:** Lost, stolen, or misused immigration documents need to be reported to Immigration and Citizenship Canada.
- **Lost or Stolen Passport:** If you lost your passport or it was stolen, contact Passport Canada and the police in your area. If you’re outside Canada, contact the nearest Canadian embassy or consulate office.

- **Stolen Social Insurance Number (SIN):** If you think your SIN may be being misused, take steps to protect it.
- **Lost or Stolen Provincial or Territorial IDs:** To replace birth certificates, driver's licenses, or health cards, contact the provincial or territorial issuing agency.

Protect Yourself from Future Fraud

Scammers often call, email, or text past victims with schemes to "help recover" their money. **Never pay recovery fees or share private information.**

Finally, keep in contact with the agencies involved – such as the Canadian Anti-Fraud Centre, your bank, and the police – to update them on any developments. Informing family, friends, and colleagues about what happened may prevent others from becoming victims.

By remaining calm and taking these steps, you can regain control of the situation and limit further damage.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support. For more information about digital financial abuse, see our full Digital Financial Abuse Toolkit.

Adapted for Canada with permission from Refuge's Tech Safety Project, based on their resource The Differences Between Identity Fraud and Coerced Debt.

This project was funded by TD Bank Group, through its corporate citizenship platform, the TD Ready Commitment.