Scams, Identity Theft & Other Fraud

Fraud is a growing crime in Canada. People of all ages are scammed, but especially older adults. Fraud victims nearly always lose money. The internet makes fraud easier to commit and to get away with. But you can protect yourself from fraud.

This publication explains the law in a general way as it applies in Nova Scotia, Canada. The information is not intended as legal advice. If you have a legal problem, contact a lawyer for advice about what steps you should take in your situation. We thank the Law Foundation of Nova Scotia, the Department of Justice Canada, and the Nova Scotia Department of Justice for providing core funding for our services, which makes publications like this possible.

I

Contents

©Copyright 2023

If you suspect that you may be a target of fraud, or if you have already sent funds, don't be embarrassed — you're not alone. If you want to report a fraud, or if you need more information, contact the Canadian Anti- Fraud Centre at antifraudcentre-centreantifraude.ca or 1-888-495-8501.

What is fraud?

Fraud is intentional deception. Fraud is a crime. Some types of fraud are referred to as **scams** or schemes. Fraud affects all age groups. Fraud usually causes financial loss for the victim. The internet has created new opportunities for fraudsters.

The person who is deceived is generally called the victim or mark. The person who does the deceiving is generally called a **fraudster**, a scam artist, a perpetrator, or a thief.

Fraud can be very profitable for criminals. Fraudsters are hard to catch because they are skilled at what they do, may manage to disappear before being caught, and they may not even be in Canada. Victims are often too embarrassed to tell anyone, and so many frauds do not get reported.

What is consumer fraud?

Consumer fraud is intentionally deceiving a person who buys a product or a service. For example, you are deceived into paying money for something that does not exist, is not accurately described, or is of little or no value. Another example is being deceived into providing information that allows a fraudster to steal from you.

Consumer fraud happens when a person, a group, or a company takes advantage of individuals, usually for monetary gain.

How does consumer fraud happen?

Fraudsters approach their victims in many ways:

- coming door to door
- calling on the telephone
- sending mail through the postal system
- sending emails, using social media, or other online services
- meeting in a coffee shop, club, place of worship or another place.

©Copyright 2023

They may attract you with a TV commercial, a magazine article, a newspaper advertisement, a website, a survey, or through social media.

A fraudster can cause you financial loss without having to make any personal contact with you. They are always thinking of new and different scams to take advantage of people.

What are common kinds of scams?

Unfortunately, there are so many types of scams they cannot all be listed here, and it is also difficult to guess what the next new scam will be. Examples of some of the more common consumer fraud scams include:

- **Identity Theft:** The fraudster uses your personal and financial information to steal from you. This is the top fraud across North America.
- **Advance Fee Fraud:** You are asked to make a payment or to give your personal or financial information before you receive a product or service.
- **ATM, Credit Card, and Debit Card Fraud:** The fraudster uses your pass codes and card numbers to withdraw cash from your accounts or to pay for purchases with your credit.
- **Counterfeiting:** The fraudster pays for purchases with fake money, cheques, or money orders.
- **Door-to-door frauds:** The fraudster comes to your door and says "I was driving by and noticed that your roof needs repair." Or "I have some left-over materials I can sell you at cost." Or "I'll need a 50% down payment to purchase materials." Always check with the Better Business Bureau or a neighbour who has used them before hiring any person to do work on or in your home.
- **Emergency:** The fraudster pretends to be someone close to you and tells you they need money right away due to a fake emergency, such as being arrested and needing bail money, being in a car crash, or having trouble travelling back to Canada. Grandparents are particularly vulnerable to this type of fraud, as the scammer may pretend to be a grandchild who claims to urgently need money.
- **False Charities:** The fraudster pretends to be a charity (sometimes by using a similar name, thanking you for your past support, or by trying to take advantage of a disaster such as a flood or hurricane). Sometimes the fraudster will go door to door pretending to collect donations for a charity.
- **Impersonation:** The fraudster pretends to be someone or something else for personal gain; for example, someone pretends to be a grandchild who needs money.

©Copyright 2023

- **Investment Fraud:** The fraudster misleads you into giving money for business ventures that promise unrealistic profits.
- **Misleading Job Opportunities:** The fraudster promises a large income for easy work, a fee or a start-up investment, or an almost guaranteed job after an expensive course.
- **Online Auctions, Lotteries, and Contests:** The fraudster tricks you into purchasing items of little or no value, or into buying tickets or prizes that do not exist or have little value.

Contact the Canadian Anti-Fraud Centre and Consumer Affairs Canada for more information about current scams, including COVID-19 scams. *See "Where can I get more information" at the end of this chapter for contact information.*

©Copyright 2023

Recognizing fraud

If it sounds too good to be true, it usually is. Here are some things you can look for that will sometimes point to a scam:

- contact from strangers looking to offer you a deal
- over-excited callers using a lot of pressure
- people pushing you for immediate answers or confirmation of a deal
- people who insist that you not tell anyone else about the deal
- people who discourage you from getting any advice or advice only from a person they suggest
- any deal in which what you earn will be based on how many people you involve in the deal
- people who will not send you any information until you give them money or information
- any deal where you must pay a fee or buy something before you receive a prize, credit, or product that you did not order
- prices so low they are unreasonable compared to their true value
- any reward, prize, or payment (usually very large) you are promised in exchange for your banking information
- contact from people, businesses, or creditors that you do not know
- people claiming to represent a charity that you do not know or that has a name very close to a charity that is well-known
- companies that try to sound like a well-known agency or company
- people contacting you for your credit card, calling card, banking information, or social insurance number
- any claim that you have won a prize for a contest you have not entered
- people saying they are calling from your bank and asking you to provide information about your account to help them catch a fraudster.

©Copyright 2023

What is identity theft?

Identity theft is getting your personal information and using it to steal from you. Identity theft is now the fastest-growing fraud.

Personal information might include your address, date of birth, social insurance number (SIN), credit card or bank card numbers, personal identification numbers (PINS) and pass codes, and driver's license numbers. If identity thieves get your personal information, they may:

- take money out of your bank accounts
- charge purchases to your credit cards
- apply for new credit cards or loans in your name
- buy expensive items on credit in your name.

In extreme cases, identity thieves not only collect personal information about you, but they may also watch you. They learn about your friends and family members, and learn your personal weekly routine. Then they decide how best to take advantage of you. Sometimes they pretend to be stranded family members who urgently need money. Sometimes they pretend to be you and arrange to mortgage or sell your house.

How do identity thieves get personal information?

Here are some of the ways identity thieves can get your personal information. They may:

- steal it from your wallet or purse, home, mailbox, workplace, vehicle, or computer
- go **phishing**, which means sending you an email threatening serious consequences if you don't update information on a website at once. This gets you to go to the website so that they can get personal information such as passwords and access codes from you.
- pretend to be someone entitled to request information (such as a government official, bank employee, landlord, creditor, or employer)
- collect it from your garbage. For example, bank and credit card statements, copies of credit or loan applications, financial statements, and tax returns.
- redirect your mail, open it, and then put it in your mailbox
- rig automated teller machines (ATMs) and debit machines so your debit or credit card number and PIN can be read

©Copyright 2023

- shoulder surf — hang around your shoulder to watch as you punch your access codes and passwords into ATMs, debit machines, telephones, and computers
- buy or trade customer mailing lists
- search obituaries, phone books, directories, and other public records
- place false advertisements for jobs to obtain your résumé and contact information
- pretend your personal details are needed to claim a prize or lottery winnings
- use letterhead that looks like it comes from a government department or financial institution to get personal information from you.

Protecting yourself from fraud

The best way to protect yourself from fraud is to be informed and alert.

- Protect your personal financial information. Do not give any of your banking or credit card information to anyone you do not know and trust. Do not write down your PIN.
- Cover the keypad or keyboard when you are entering your passwords and passcodes and look around you to make sure that no one is looking over your shoulder.
- Check before making purchases when you are not dealing face to face with someone you know, ask for a name and contact information, and make sure the person is who they claim to be.
- Get at least two written quotes for all repair work; ask for references and check them; check for complaints at the Better Business Bureau; and don't agree to pay all the money up front.
- Be aware that police and financial institutions never call or email you to ask for your bank card information, credit card details, or banking details.
- Do not provide more personal information than is necessary for your business.
- Only give your SIN when absolutely necessary, and do not carry your SIN card with you. Businesses such as stores should not be asking for your SIN number.
- Do not give your address and phone number unless there is a good reason.
- Carry only the documents and cards you need.
- Do not leave your purse or wallet unattended.
- If you are paying by debit or credit card, make sure that your card number does not appear on the receipt.

©Copyright 2023

- If you are paying with a debit or credit card in a restaurant, keep your card in sight. Arrange to pay at your table or go with the server to process the card.
- Shred receipts and copies of papers you no longer need such as bank statements, tax returns, credit applications and statements, receipts, insurance forms, and credit offers you get in the mail.
- Do not leave personal information sitting around at home, in your vehicle, at your workplace, or on your computer.
- Keep important documents such as your birth certificate, tax returns, and social insurance card in a secure place.
- When you receive renewal documents and cards, destroy the old ones and sign the new ones right away.
- Know when your credit card and financial statements and utility bills are supposed to arrive in the mail.

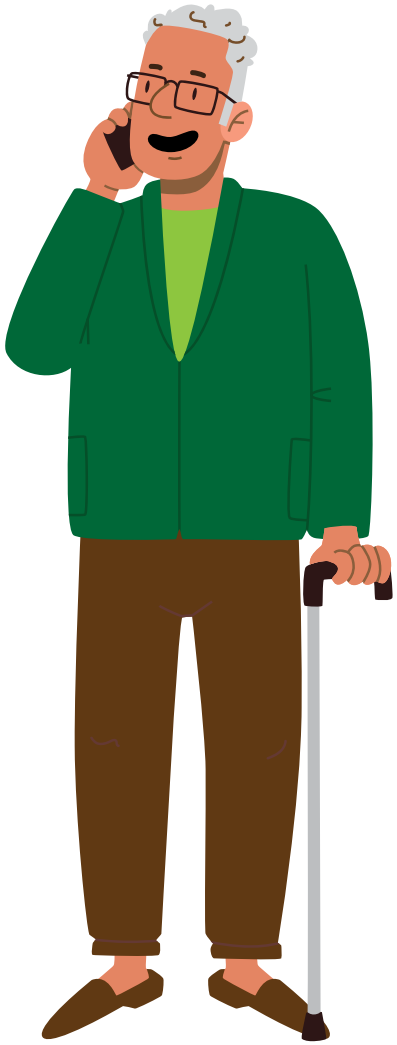
- Keep credit card, debit card, and ATM transaction records so you can match them to your statements.
- Check your bank and credit card statements carefully to make sure that there are no withdrawals or charges that you were not expecting.
- Update your credit cards to ones that have the latest security features, for example, “chip cards” which require a PIN because they are embedded with a micro-computer chip.
- Let your credit card company know when you are leaving the country. Your credit card company should contact you if there is unusual activity on your card such as stays at international hotels.
- Lock your mailbox.
- Pick up your mail promptly.
- Do not pick pass numbers (for your credit card, bank account, etc.) that refer to your personal information (like your birth date or SIN).
- Do not pick passwords that can easily be guessed such as the name of your pet.
- Use spyware filters, email filters, and firewall software on your computers.

©Copyright 2023

- If you use secure internet sites for financial transactions, follow security instructions when you enter and leave the site. Under the "Tools" section in your web browser, click "Clear Recent History" when you are done.
- Be sure all personal information is deleted before you sell, recycle, or discard your computer. You may have deleted files, but the information may still be on the hard drive.
- Consider signing up with the National Do Not Call List, which prohibits most businesses that you don't deal with from contacting you by phone.

What can I do if I think that I am the target of fraud?

If you suspect that you are the target of fraud, do not deal directly with the person you think is trying to deceive you. Do not agree to provide further money to get your first payments back or to keep a deal open.



You can contact your local police or RCMP detachment and the Canadian Anti-Fraud Centre. You may also report the crime online through some of the websites listed at the end of this section under "More Information".

You should also contact Equifax Canada and TransUnion Canada. They are credit reporting agencies. They can place an alert on your account so creditors must call you before opening any new accounts or changing your existing accounts. Also, ask them to send you a copy of your credit report so you can see if an identity thief has opened any new accounts or debts in your name. The Financial Consumer Agency of Canada has information about credit reports, and credit reporting agencies. *See "Where can I get more information" at the end of this chapter for contact information.*

©Copyright 2023

What if I am a victim of fraud?

If you have been the victim of fraud, you must contact the financial institutions and credit card companies where you have your accounts. Tell them what happened and have them freeze your accounts. If the fraud has affected your account, it must be closed. You will need to open new accounts.

You should contact the police or RCMP to report that you have been the victim of fraud, no matter how small your loss may be. They may start an investigation.

You should also contact Equifax Canada and TransUnion Canada. These credit reporting agencies can place an alert on your account so creditors must call you before opening any new accounts or changing your existing accounts. The Financial Consumer Agency of Canada has information about credit reports, and credit reporting agencies.

Report the fraud to the Canadian Anti-Fraud Centre.

If your government-issued documents were lost or stolen, contact the department, explain what happened, and ask for new documents. You will likely need to do that in writing. Contact Service Canada at canada.ca or 1-800-206-7218 if your social insurance number (SIN) has been stolen.

If you think your mail is being stolen or redirected, contact Canada Post at 1-800-267-1177 or canadapost.ca.

Quick Tips

- **Know the source.** This means checking into a website before handing over any personal information — especially personal financial information. This doesn't mean you can't shop or surf at unknown sites, but make sure you've done your homework before exchanging information.
- **Read your email carefully.** Many fraudulent offers come in the form of e-mails because the Internet makes it possible to send thousands at a relatively low cost. Use a mail program that allows you to screen out these mass mailings, and you'll spend less time with your finger on the delete key.
- **Deal only with reputable organizations**, and don't give out personal or financial information unless you are sure you're in a secure environment. Don't judge reliability by how nice or sophisticated the website may seem.
- **Be careful at auction sites**, one of the areas that generate a lot of complaints.

©Copyright 2023

- **Understand as much as possible about how the auction works**, what your obligations are as a buyer, and what are the seller's obligations.
- **Find out what the website/company does** if a problem happens and consider insuring the transaction and the shipment.
- **Learn as much as possible about the seller**, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where it is located. Examine the feedback on the seller. Remember because of the difference in laws, it may be much harder to solve a problem if the seller is located outside Canada.
- **Find out if shipping and delivery are included** in the auction price or are additional costs. If they are extra, find out exactly how much you'll be charged.
- **Don't give out your social insurance number or driver's license number.**
- **Don't give out your credit card number(s) online unless the site is secure and reputable.** Sometimes a tiny padlock appears on the screen. This symbolizes a higher level of security to transmit data. While not a guarantee, it may provide you with some assurance.
- **Don't invest in anything you are not absolutely sure about.** Do your homework on the investment to make sure that it is legitimate.
- **Be skeptical of individuals representing themselves as Nigerian or foreign government officials** asking for your help in placing large sums of money in overseas bank accounts.

©Copyright 2023

Where can I get more information?

- **The Canadian Anti-Fraud Centre** online at antifraudcentre-centreantifraude.ca or call 1-888-495-8501. The centre collects information and criminal intelligence on issues like mass marketing fraud (e.g., telemarketing), advance fee fraud (e.g., West African letters), internet fraud, identity theft, and COVID-19 frauds and scams
- **Investor Rights and Protection Guide** from the Legal Information Society of Nova Scotia, at legalinfo.org/guides/investor-rights-and-protection-guide/
- **The Financial Consumer Agency of Canada**: canada.ca/en/financial-consumer-agency.html or 1-866-461-3222. Information about identity theft, types of fraud, counterfeit money and other threats or scams; protecting yourself from fraud; reporting fraud.
- **The Spam Reporting Centre**, which oversees Canada's Anti-Spam law, at fightspam.gc.ca or 1-800-328-6189 also takes reports of suspicious or unsolicited emails (e.g., phishing, malware, deceptive marketing, etc.).
- **Get Cyber Safe**: Federal government site all about staying safe online for individuals and businesses: getcybersafe.gc.ca
- **CyberScan**: for information and help if someone is bullying you, sharing private images of you without your consent, or pretending to be you online or by text or email contact CyberScan at novascotia.ca/cyberscan/ or call 902-424-6990 or 1-855-702-8324.
- **Service Canada** at 1-800-206-7218 if your social insurance number (SIN) has been stolen.
- **Industry Canada's Office of Consumer Affairs**, a federal government department that gives consumers tips about how to protect themselves in various consumer situations: canada.ca/en/services/finance/consumer-affairs.html.
- **Competition Bureau of Canada**: A federal government agency concerned about competitive markets and consumer information. It investigates complaints and enquiries from the public about consumer issues such as deceptive product labelling and price fixing: competitionbureau.gc.ca. Their 'Little Black Book of Scams' is easy to use and can help you protect yourself against common scams.
- **National Do Not Call List** (Canadian Radio-Television and Telecommunications Commission): If you have complaints about a telemarketer or wish to register a number on the Do Not Call List. Website: lnnte-dncl.gc.ca, or call 1-866-580-3625. To use the National Do Not Call service, you must call from the phone number you wish to register.

©Copyright 2023

- **Service Nova Scotia consumer information**: Call 1-800-670-4357.
- **Better Business Bureau of the Atlantic Provinces**: Tips for consumers; lists of BBB-approved businesses and charities; complaints; information for businesses: visit bbb.org or call 1-877-663-2363.
- **Nova Scotia Registry of Joint Stock Companies**: 1-800-225-8227 (toll-free), or 902-424-7770.
- **Reporting Economic Crime On-line (RECOL)** An association that allows you to file fraud complaints online. www.recol.ca
- **To get a current copy of your credit report, contact Equifax Canada** — equifax.ca or 1 800-465-7166 or TransUnion Canada — transunion.ca or 1 800-663-9980
- **Nova Scotia Department of Seniors**:
  Email: seniors@novascotia.ca
  Information line: 1-844-277-0770 (toll-free in Nova Scotia)
  Website: novascotia.ca/seniors
- **211 information and referral service**. To learn about programs and services for Nova Scotia seniors, call 2-1-1 or visit their website, ns.211.ca.

General legal information

- Legal Information Society of Nova Scotia (LISNS)
  Legal Information Line
  902-455-3135
  1-800-665-9779
  Email: questions@legalinfo.org
  www.legalinfo.org

©Copyright 2023