SCAMS, IDENTITY THEFT AND 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.

LEGAL INFO NOVA SCOTIA

If you think that you may be a target of fraud, or if you have already sent funds, don't be embarrassed—you are not alone. If you want to report a fraud, or if you need more information, contact The Canadian Anti-Fraud Centre (1-888-495-8501 (toll-free) or antifraudcentre-centreantifraude.ca).

What is fraud?

Fraud is when someone lies or tricks another person or a company to get money. Sometimes fraud is called a **scam** or a scheme. It is a crime that affects all age groups, and victims usually lose money. The person who tries to cheat someone out of money is called a cheat, a scammer, a scam artist, a con artist, a fraudster, or a swindler.

Victims are often too embarrassed to tell anyone, and so many frauds do not get reported. This makes it easier to get away with fraud.

What is consumer fraud?

Consumer fraud is tricking a person into buying a product or a service or into giving away valuable information. For example, you are tricked into paying money for something that does not exist, is not accurately described, or is of little or no value. Another example is being tricked into giving someone information that lets them steal from you.

How does consumer fraud happen?

Fraudsters approach their victims in many different ways. They might

- come to your door
- call you on the telephone
- send mail through the postal system
- send emails or use social media or other online services
- meet you in a coffee shop, club, church, or other place.

The scammer may attract you with a TV commercial, a magazine article, a newspaper advertisement, a website, a survey, or through social media. They can get money from you without contacting you in person. 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. As well, it is hard to guess what the next new scam will be. Some common consumer fraud scams are listed below.

Identity theft: Someone gets your personal and financial information to steal from you. This is the top fraud across North America. For example, someone looks through your trash bin and takes documents that have your private financial information.

Advance fee fraud: Someone asks you to pay for or to give your personal or financial information before you receive a product or service.

ATM, credit card, and debit card fraud: Someone uses your pass codes and card numbers to withdraw cash from your accounts or to pay for purchases with your credit.

Counterfeiting: Someone pays for purchases with fake money, cheques, or money orders.

Door-to-door frauds: Someone comes to your door and makes an amazing offer that they say your neighbour is taking, but that you don't have time to check out. Always check with the Better Business Bureau or with the neighbour.

False charities: Someone pretends to collect donations for a charity or for a recent disaster. The charity might have a similar name to a real 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, or they might pretend to represent a government and say you haven't paid your taxes.

Investment fraud: Someone misleads you into giving money for business ventures that promise unrealistic profits.

Misleading job opportunities: Someone promises a large income for easy work, if you pay a fee or a start-up investment. Or someone guarantees you will get a job after an expensive course.

Online auctions, lotteries, and contests: Someone tricks you into buying items of little or no value, or into buying tickets or prizes that do not exist or have little value.

Recognizing fraud

If it sounds too good to be true, it usually is. Here are some things that might point to a scam:

- contact from a stranger who wants to offer you a deal
- contact from people or businesses that you do not know
- an over-excited caller who uses a lot of pressure
- a person who pushes you to say yes right away to a deal
- a person who tells you not to tell anyone else about the deal
- a person who discourages you from getting any advice or encourages you to get advice only from a person they suggest
- any deal where what you earn will be based on how many people you involve in the deal
- a person who will not send you any information until you give them money or information
- any deal where you have to pay a fee or buy something before you receive a prize, credit, or product that you did not order
- a price that is too low compared to the true value
- the promise of a reward, prize, or payment (usually very large) in exchange for your banking information
- a person who says they represent a charity you do not know or that has a name very close to a charity that is well known
- a person who calls 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
- a person who says they are calling from your bank and to ask you for information about your account to help them catch a fraudster

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 includes your:

- address
- date of birth
- social insurance number (SIN)
- credit card or bank card numbers
- personal identification numbers (PINs)
- pass codes
- driver's license number.

If identity thieves get your personal information, they may use it to:

- take money out of your bank accounts
- apply for new credit cards or loans in your name
- buy expensive items on credit in your name or using your credit card

Sometimes, identity thieves might 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 need money right away. Sometimes they pretend to be you and arrange to mortgage or sell your house.

How do identity thieves get personal information?

Identity thieves have many ways to get your personal information. They might:

- 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 who has the authority to ask for personal 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
- shoulder surf—watch over your shoulder 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 they need your personal information 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 pass codes, and look around you to make sure that no one is looking over your shoulder.
- Before you buy online or on the phone, make sure the person is who they claim to be:
    - Check businesses with the Better Business Bureau.
    - Check charities with Canada Revenue Agency.
    - Check businesses or non-profits in Nova Scotia with the Registry of Joint Stock Companies.
- For any repair work:
    - Get at least two written quotes.
    - Don't pay all the money up front.
    - Ask for references and check them.
    - Check at the Better Business Bureau for complaints about the company.
- Remember that police and financial companies, like banks and credit card companies, never call or email you to ask for your bank card or credit card details.
- Do not give more personal information than is necessary for your business.
- Your social insurance number (SIN) is private. Give it only when you must, and do not carry your SIN card with you. Businesses such as stores should not ask for your SIN.
- Do not give your address and phone number unless there is a good reason.
- Carry only the documents and cards you need.
- Always keep your purse or wallet in sight—never leave it.
- If you are paying by debit or credit card, make sure that your card number is not listed on the receipt.
- If you are paying with a debit or credit card in a restaurant, keep your card in sight. Pay at your table or go with the server to pay.
- 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 get renewal documents and cards, destroy the old ones and sign the new ones right away.
- Know when your credit card, banking statements, and bills should arrive in the mail.
- Keep credit card, debit card, and ATM transaction records so you can match them to your statements.
- Read your bank and credit card statements to look for withdrawals or charges that you were not expecting.
- Update your credit cards to ones that have the latest security features, like microchips.
- Let your credit card company know when you are leaving the country. Your credit card company should call you if there is unusual activity on your card such as a charge for a hotel outside your country.
- Lock your mailbox.
- Pick up your mail right away each day.
- Do not use pass numbers (for your credit card, bank account, etc.) with your personal information (like your birth date or SIN).
- Do not use passwords that someone could guess, like your pet's name.
- Use spyware filters, email filters, and firewall software on your computers.
- 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 stops most businesses from contacting you by phone without your permission. It won't stop businesses you choose to deal with.

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

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

Call your local police or RCMP detachment. Call the Canadian Anti-Fraud Centre toll-free at 1-888-495-8501. You can also report a fraud at their website (antifraudcentre-centreantifraude.ca) or some of the websites listed at the end of this section under "More Information."

Contact Equifax Canada (toll-free at 1-800-465-7166 or online at equifax.ca) and TransUnion Canada (toll-free at 1-800-663-9980 or online at transunion.ca). 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 anyone has opened any new accounts or debts in your name.

The Financial Consumer Agency of Canada (canada.ca/en/financial-consumer-agency.html) has information about credit reports and credit reporting agencies, and how to contact them and correct errors on your credit report.

What if I am a victim of fraud?

If you have been the victim of fraud, you must call your banks or credit unions and the credit card companies where you have your accounts. Tell them what happened and ask them to freeze your accounts. If the fraud has affected your account, they will close it. You will need to open new accounts.

Call your local police or RCMP to report the fraud, no matter how small your loss may be. They may start an investigation.

Call the Canadian Anti-Fraud Centre toll-free at 1-888-495-8501. You can also report a fraud at their website (antifraudcentre-centreantifraude.ca) or some of the websites listed at the end of this section under "More Information."

Contact Equifax Canada (toll-free at 1-800-465-7166 or online at equifax.ca) and TransUnion Canada (toll-free at 1-800-663-9980 or online at transunion.ca).

The Financial Consumer Agency of Canada (canada.ca/en/financial-consumer-agency.html) has information about credit reports, credit

reporting agencies, and how to contact them and correct errors on your credit report.

If your government documents, like your driver's licence or your social insurance card—were lost or stolen, contact the department. Tell them what has happened and ask for new documents. You will likely need to do that in writing.

Call Service Canada at 1-800-206-7218 if your social insurance number (SIN) has been stolen.

If you think your mail is being stolen or redirected, call Canada Post at 1-800-267-1177 or visit canadapost.ca to report it online.

Quick tips

- Know the source. This means look into a website before you give any personal information—especially financial information. You can still shop or surf at unknown sites, but make sure you know who you are dealing with before you give any information.
- Read your email carefully. Many fraudulent offers come in the form of emails because the internet makes it possible to send thousands at a relatively low cost. Use an email program that lets you screen out these mass mailings, and you'll spend less time with your finger on the delete key.
- Deal only with organizations with a good reputation, and don't give personal or financial information unless you are sure you are in a secure environment. Don't judge reliability by how nice or sophisticated the website seems.
- Be careful at auction sites; they cause many complaints.
- Understand as much as you can about how the auction works; know what is expected of you as a buyer, and what the seller must do.
- Find out what the website or company does when there is a problem. Think about insuring the transaction and the shipment.
- Learn as much as you can about the seller, especially if you have only an email address. If it is a business, check the Better Business Bureau where it is located. Read the feedback on the seller. Laws are different in different countries: it may be much harder to solve a problem if the seller is outside Canada.
- Find out if shipping and delivery are part of the auction price or if they are extra costs. If they are extra, find out exactly how much they will cost.
- Do not give out your social insurance number or driver's license number.

- Do not give out your credit card number online unless the site is secure and reputable. Sometimes you can see a tiny padlock on the screen. This shows you that the site has a higher level of security. It is not a guarantee, but it may give you with some protection.
- Do not invest in anything you are not absolutely sure about. Do your homework on the investment to ensure that it is real.
- Stay away from people who say they are Nigerian or foreign government officials if they are asking you to help them put money in overseas bank accounts.

Where can I get more information?

- **Legal Information Society of Nova Scotia: Investor Rights and Protection Guide:** legalinfo.org/guides/investor-rights-and-protection-guide/
- **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, and identity theft complaints
- **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 ic.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, 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: consumerinformation.ca.
- **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

(competitionbureau.gc.ca under "Publications") 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.
- **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 (toll-free)
legalinfo.org
Email: questions@legalinfo.org

The Legal Information Society of Nova Scotia can also refer you to a lawyer or mediator.

Notes