

1

## BE ON YOUR GUARD



## Fraud and Identity Theft: Recognize It. Report It. Stop It.

Identity theft occurs when someone uses your personal information, without your knowledge or consent, to commit a crime, such as fraud or theft. Frauds can involve credit cards, government documents or benefits, utilities, banks, or employment-related matters.

Fraud is increasing, and technology is making it easier. Telephone, fax and the Internet help criminals find victims all over the world. Chances are you know someone who has been a victim.

### Could You Be a Fraud Victim?

Take the following short quiz to test your knowledge of fraud and identity theft:

#### 1) My social insurance number (SIN) card is:

- In my wallet.
- In my bedroom.
- In my parents' safe.
- I have no idea!

#### 2) After I receive my bank statement, I:

- Quickly glance at it and throw it in the garbage.
- Lock it in a safe.
- Check to verify the transactions listed are correct.
- Leave it on the kitchen table.

## Contents:

- Fraud and Identity Theft .....pg 1
- Internet Shopping .....pg 7
- Employment and Job Opportunity Fraud .....pg 9

- 3) **A friend and I are having lunch together, but the restaurant is very busy. He offers to order lunch for both of us while I save a table. I would like to pay with a debit card, and he would like to pay with cash. Here is how I pay for lunch:**
- a) I give him my debit card and write my personal identification number (PIN) on a piece of paper for him.
  - b) I offer to order the lunches using my debit card and his cash while he saves the table.
  - c) I give him my debit card and call out my PIN from the table.
  - d) I give him my card. He already knows my PIN, and we do this every time we have lunch together.
- 4) **When I create an email password, I use:**
- a) My birth date.
  - b) The same password I use for my cell phone.
  - c) The name of my favourite band.
  - d) None of the above.
- 5) **When I pay with my credit card, I:**
- a) Sign the receipt without looking at it and shove my card in my pocket. I never carry a wallet.
  - b) Watch the cashier run my card through, read and sign the receipt, and look at my card before I put it back in my wallet.
  - c) Watch the cashier run my card through, read and sign the receipt, and put my card back in my wallet.
  - d) None of the above.
- 6) **I received an email from my bank asking me to verify my account by signing into my bank account online. I decide to:**
- a) Delete the email.
  - b) Click on the link provided in the email and follow the instructions.
  - c) Go to my bank's website and sign into my bank account.
  - d) Call my bank using the number provided in the email.

## Answers

1. The correct answer is c). Do not carry your SIN card with you unless you need it. Always keep it under lock and key at home, and if you do need to take it with you, leave a photocopy at home.
2. The correct answer is c). Be sure to carefully read all bank statements, pre-approved credit card offers and credit card statements. Contact your bank immediately if you find any errors. If you choose to dispose of any personal documents, such as financial documents, be sure to destroy them by using a shredder before throwing them into the garbage.
3. The correct answer is b). Never give your PIN to anyone. Writing it on a piece of paper is especially dangerous because it can easily get lost and fall into the hands of the wrong person.
4. The correct answer is d). Always choose a complex password of letters, numbers and symbols. Easy-to-remember passwords are also easy for thieves to guess.
5. The correct answer is b). Watch the cashier run your credit card through and check to make sure that you receive YOUR card when it is handed back to you. Also, read your receipt to make sure that you are being charged for the correct amount.
6. The correct answer is a). Delete this email right away. If your bank needs information from you, it will not send you an email. If you are concerned, call your bank to verify; however, never use the number provided in the email because the number may be fake and lead you instead to a criminal impersonating bank personnel.

## Who Are Fraud Victims?

People committing fraud don't care whom they target — victims can be young or old, educated or not. Some people are more vulnerable to fraud. You may have already taken the short quiz here, but for a more in-depth quiz and to find out your risk level, try Industry Canada's online **Fraud Quiz**, available at [www.ConsumerInformation.ca](http://www.ConsumerInformation.ca). Based on your answers, you will also get some tips about avoiding fraud.

## How Can You Stay on Guard?

The following checklist, available at [www.cmcweb.ca/idtheft](http://www.cmcweb.ca/idtheft), outlines what you need to know to help reduce the risk:

### *Guard Your Personal Information*

- Never give personal information by phone, the Internet or mail unless you initiate the contact.
- Be careful about sharing personal information and don't give out more than you need to.
- Shield your PIN, and never lend cards.
- Report missing credit or debit cards.
- Carry only the ID you need.
- Put other ID documents (SIN, birth certificate, passport) in a safe place.
- Shred documents with personal information.
- A SIN is only for employment and tax reporting.
- Ask about the security of your information at work, with businesses and charities.

### *Guard your Computer and its Information*

- Select a complex password of letters, numbers and symbols.
- Install firewall, anti-virus, anti-spyware and security software-update often.
- Don't try, don't buy and don't reply to spam or emails that ask for banking information.
- For online transactions, look for https://, a closed lock or an unbroken key icon.
- When disposing of hard drives, use overwrite software or destroy the drive.

Preventing fraud in the first place is much easier than trying to get your money or identity back later. Visit [www.cmcweb.ca/idtheft](http://www.cmcweb.ca/idtheft) to check out the entire *Consumer Identity Theft Kit*.

## What to Do If Your Identity Has Been Stolen

It is very important for anyone who has become a victim of identity theft to take action. Always call your financial institutions and local police first. Visit [www.cmcweb.ca/idtheft](http://www.cmcweb.ca/idtheft) for a more complete list of steps to follow that can minimize damage and help prevent further identity theft. This website includes information about whom to contact and an *Identity Theft Statement* form to help you provide written notice of the incident.

## Questions to Ask

It is difficult to know if you are being exposed to fraud. To avoid it, do your research and make sure you ask the right questions. The following questions are examples from *Personal Information and Scams Protection: A Student Practical Guide*, available on the RCMP website ([www.rcmp.ca](http://www.rcmp.ca)). Find it in the “Scams” section. It might help you.

- Who am I really dealing with?
- Why is he/she asking for more information than they actually need?
- Am I being rushed or pushed into making impulsive decisions?
- Is this person overly enthusiastic?
- Is this too good to be true?
- Is there anything unusual about this automated teller machine?
- Is a hidden camera / cellphone camera / person reading my PIN?
- Is this job offer legitimate?
- Is this website trustworthy/legitimate?
- Will this employer/organization protect my personal information?
- Why are they asking for a processing fee to give me a loan?
- How did they get my contact information?
- Am I broadcasting my personal information over the airway?
- Why does this stranger suddenly want to become my best friend?

## Dealing With Fraud

The first step in dealing with fraud is to **recognize it**. Keep in mind at all times the signs of fraud listed above. If you encounter fraud, **report it** immediately. Visit the websites listed below to find out how. Don't be a victim of fraud — **stop it**. Be on guard and save your money.

## More Information

The following websites offer up-to-date information on fraud prevention methods and current scams, including identity theft:

- Visit [www.ConsumerInformation.ca](http://www.ConsumerInformation.ca). Check out the *Spam IQ Test*, *Fraud Quiz* and other information available on fraud.
- The RCMP's website is available at [www.rcmp-grc.gc.ca](http://www.rcmp-grc.gc.ca).
- RECOL (Reporting Economic Crime On-Line), a website supported by the RCMP, is available to report Internet fraud ([www.recol.ca](http://www.recol.ca)).
- PhoneBusters, the Canadian anti-fraud call centre ([www.phonebusters.com](http://www.phonebusters.com)), is the central agency in Canada that collects information on identity theft, fraudulent telemarketing and advanced-fee fraud letters complaints. Please contact its call centre to report frauds or attempted frauds at 1-888-495-8501 or [info@phonebusters.com](mailto:info@phonebusters.com). For Nigerian letters, contact [waf1@phonebusters.com](mailto:waf1@phonebusters.com).
- *Privacytown* is available at [www.consumer.ic.gc.ca/privacytown](http://www.consumer.ic.gc.ca/privacytown).
- Consult the website of the Office of the Privacy Commissioner of Canada ([www.privcom.gc.ca](http://www.privcom.gc.ca)) to read the *Personal Information Protection and Electronic Documents Act*, which outlines the procedures that private sector organizations must abide by when collecting and using your personal information.
- Find provincial and territorial privacy offices at [www.privcom.gc.ca](http://www.privcom.gc.ca) by clicking on "Resource Centre" and then on "List of Provincial and Territorial Privacy Commissioners."

## 2 Internet Shopping

The Internet is a powerful tool and a great place to shop, but it is important to use it with caution. Criminals are using the Internet's speed, anonymity and hype to reach new markets with old and new scams. The best way to protect yourself is to know what the hazards are and what you can do to reduce the risk.

### Get the Details

Stay away from merchants who don't provide the details, i.e., who they are, where they are, how to contact them, what they are selling, all the costs involved and their privacy policy. Reliable merchants want you to know these details.

Use the *On-line Shopping Assistant*, available at [www.ConsumerInformation.ca](http://www.ConsumerInformation.ca), when you are considering making a purchase online.

### Spam Offers

Don't buy anything you hear about through spam (unsolicited emails). If you do get spam, don't reply to it, don't ask to be removed from the sender's mailing list, and don't take advantage of the spammer's offer to remove you from the list. These activities only serve to validate your email address. When it comes to spam, the solution is simple: delete, delete, delete.

You may wish to visit the U.S. Direct Marketing Association's (DMA's) website at [www.e-mps.org](http://www.e-mps.org) to have your email address removed from the marketing lists of member companies throughout Canada, the U.S., Australia, Belgium, Finland, Great Britain, Ireland and the Netherlands. Although the website is operated by a U.S. association, it also serves Canadians. You can also visit the RCMP website ([www.rcmp.ca](http://www.rcmp.ca)) and check out *Personal Information and Scams Protection: A Student Practical Guide*. There you will find some information about protecting yourself from scams.

### Phishing

Phishing refers to the imitation of a trusted person or organization in order to steal an individual's personal information, generally for the purpose of identity theft. For example, you may receive an email message that appears to be from a well-known bank asking you to visit a website to confirm your account details, but the website is actually controlled by someone looking to gather your personal information. Do not give out any information on these sites.

## Money, Security and Safety

It is usually safer to use a secure transaction website that shows either a closed padlock icon at the bottom of your screen or “https://” in the web address. If these aren’t in place, someone else could get your information and credit card number. Some provinces have Internet security legislation. Contact your provincial or territorial consumer affairs office to learn more (see “Reporting Internet Shopping Problems” below).

Make sure you know the total price for the goods you are buying, **including taxes, shipping and handling**. For out-of-Canada purchases, figure out the price in Canadian dollars using the currency converter at [www.ConsumerInformation.ca](http://www.ConsumerInformation.ca). Depending on the item(s), you may have to pay duty, GST or HST, plus a handling fee if the goods are mailed. It may be cheaper to buy low-cost items locally. For customs and duty information, contact the Canada Border Services Agency toll-free at 1-800-461 9999.

Be wary of purchasing from foreign sellers — it may be harder to get your money back if something goes wrong. If you paid by credit card and don’t get the goods, contact your credit card company to see if it can help. Also, contact your provincial or territorial consumer affairs office, as they may have Internet security legislation on the issue. If you have a problem with something you have purchased from a foreign seller, you may also wish to visit the website of the International Consumer Protection and Enforcement Network (ICPEN) at [www.icpen.org](http://www.icpen.org). ICPEN operates an informal dispute-resolution system to assist consumers in resolving disputes arising out of cross-border transactions.

Safety isn’t just a financial issue. Foreign products may not meet Canadian safety standards, and it’s up to you to make sure the product is safe. You should be particularly concerned with the potential chemical, mechanical and electrical hazards and the flammability of products. Be especially careful when buying things such as health or children’s products. Take the time to visit CSA International’s website ([www.csa-international.org](http://www.csa-international.org)) or Health Canada’s website ([www.hc-sc.gc.ca](http://www.hc-sc.gc.ca)) for product information.

## Quick Online Tips

- Remember, if the offer sounds too good to be true, it probably is.
- Read the contract, especially the fine print. Be sure to print out copies of important documents such as reference, confirmation and order numbers.
- Do not purchase anything on a website that asks you to send personal or financial information before you find out what’s for sale.

## Reporting Internet Shopping Problems

To report online fraud, contact RECOL (Reporting Economic Crime On-Line), supported by the RCMP, at [www.recol.ca](http://www.recol.ca).

To contact your provincial or territorial consumer affairs office, see the “Where to Get Help and Information” section of, *Am I Making the Most of my Money?*, in this series.

For problem transactions with a foreign seller, contact the International Consumer Protection and Enforcement Network at [www.icpen.org](http://www.icpen.org).

3



## Employment and Job Opportunity Fraud

We all want to find a job that is interesting and that pays well. However, there is a dark side to the world of job-hunting. There are lots of valid job advertisements and offers out there, but there are also plenty of criminals looking to capitalize on your need to find a job. If you can recognize a scam when you see one, you'll be able to keep your money in your pocket where it belongs and use your time to find a real job.

Phony job ads can be found in all forms of media. Be especially cautious when responding to ads on the Internet. Anybody anywhere in the world can create a website and pretend to be someone or somewhere else. Online jobs are generally posted either directly on company websites or on third-party job listing sites. It's a good idea to deal only with websites that you know are reputable.

## Types of Employment and Job Opportunity Fraud

**Work-at-home** jobs usually promise high incomes but often don't deliver. Most say that you need little or no investment or experience. However, you usually have to buy something such as a "starter kit" or a computer program before you start. Whatever it is, it could cost a lot of money. Work-at-home offers don't tell you that you may have to work many hours without any pay. If the work-at-home job involves selling, you may have to buy a large supply of the product up front. In most cases, if you can't sell it, you are stuck with it.

**Stuffing envelopes** is a common work-at-home promotion, but today's technology has made stuffing envelopes, addressing and mailing services almost obsolete. Don't fall for it.

Be wary of offers to **assemble or create products** for a company to sell. In many cases you will have to buy the company's production equipment and raw materials. They may also try to cheat you by telling you that you won't be paid because your final product doesn't meet their quality standards. (The company always sets the quality standards, of course.)

You may find ads offering **job training** or **job opportunities** that claim there are lots of high-paying jobs in the field, or even within the company that's offering the training. This training is often overpriced and uncertified. The jobs are often not available, and the training may not be recognized — or required — by other companies hiring in the same line of work.

**Pyramid selling** is a type of multilevel marketing that is illegal under the *Competition Act*. Pyramid selling incorporates the following deceptive practices:

- paying money for the right to recruit new members (who also pay money for the same right)
- requiring new recruits to buy products as a condition of participation
- selling unreasonable amounts of inventory to participants
- having an unreasonable product return policy

More information about pyramid selling can be found in the *Canadian Consumer Handbook*, available at [www.consumer.ic.gc.ca/handbook](http://www.consumer.ic.gc.ca/handbook).

Unscrupulous **model and talent agencies** take advantage of the fact that you don't know what standard industry practices are. You could end up paying a lot of money for unneeded classes and photographs, with no career in sight. The Acting Modelling Information Centre ([www.amisontario.com](http://www.amisontario.com)) has all the facts.

**Overseas teaching contracts** aren't generally fraudulent, but it is best to be sure. Some Canadians have found that promises made about salaries, bonuses and other amenities differ from what's available once you get there. The publications section of Foreign Affairs Canada's Consular Affairs website ([www.voyage.gc.ca](http://www.voyage.gc.ca)) has information worth reading on teaching English overseas. Click on "Publications."

## Identify Theft Potential

Be careful about applying for a job over the Internet. Online job offers may be a ploy to gather personal information to sell to the highest bidder. The highest bidder may be someone who wants to steal your identity.

Don't give out personal information (SIN, banking information, credit card numbers, etc.) online or in person unless you've been offered a job in writing, have received a copy of the contract, and have checked out the company.

## More Information

Visit [www.ConsumerInformation.ca](http://www.ConsumerInformation.ca) for information on safe job seeking, employment fraud, identity theft and other scams.

To contact your provincial or territorial consumer affairs office, see the "Where to Get Help and Information" section of, *Am I Making the Most of My Money?*, in this series.

For general information on working abroad, read *Working Abroad*, available on the Foreign Affairs Canada's Consular Affairs website at [www.voyage.gc.ca](http://www.voyage.gc.ca).

Check with your provincial or territorial department responsible for employment and training for more job-related information.

# CONSUMER ISSUES FOR THE YOUNG

Consumer protection remains an important part of the federal, provincial and territorial governments' agenda. In a spirit of co-operation and to improve efficiency on the consumer front, the Consumer Measures Committee (CMC) was created under Chapter Eight of the Agreement on Internal Trade. The Consumer Measures Committee has a representative from the federal government as well as every province and territory. The CMC provides a federal–provincial–territorial forum for national co-operation to improve the marketplace for Canadian consumers, through harmonization of laws, regulations and practices and through actions to raise public awareness.

