

Newcomer Finances Toolkit

Fraud

Worksheets



Ottawa Community Loan Fund • Fonds d'emprunt Communautaire d'Ottawa
22 O'Meara St., Causeway Work Centre, Ottawa, ON K1Y 4N6 Tel: 613-594-3535 Fax: 613-594-8118

www.oclf.org

Table of Contents

<i>Fraud</i>	<i>1</i>
<i>Identity Theft</i>	<i>2</i>
<i>Protect Your Identity</i>	<i>4</i>
<i>Spot the Fraud</i>	<i>6</i>
<i>Scams</i>	<i>7</i>
<i>Problems with Fraud</i>	<i>9</i>
<i>Protecting My Identity</i>	<i>10</i>

Fraud

Fraud is lying or stealing to get money.
Fraudsters may tell you something **false** to get you to send them money.
They may steal your personal information to take your money.

There are many kinds of fraud.
Some happen when you believe a lie.
Some can happen without you doing anything.

Fraudsters will say anything to trick you.
They are usually polite and friendly.
They will keep pushing until you say yes.



Identity Theft

Identity theft happens when someone else pretends to be you.

They may get a loan or a credit card in your name, or take money from your bank account.

They use your information, such as your Social Insurance Number (SIN) or your credit card number, to pretend they are you.

It can take years to fix your credit if identity theft happens to you.



Usually identity thieves get their information from you.

They trick you into giving them your credit card number, expiry date, bank account numbers, passwords, or SIN.

They may pretend to be your bank, the government, a store, an online auction site like eBay, or your credit card company.

If you are looking for a job, they may pretend to be an employer.

Identity thieves can hide their real number and even make it look like they are calling from a real company or government office on your call display.

They may call you or leave a voice message (**vishing**).

They ask you to tell them your personal information or to use your telephone keypad to enter your SIN, credit card number, or bank password.

They may send you a letter or an email (**phishing**). They may make a fake website that looks like the real website.

They may put an ad in the newspaper or on a website.

An email from an identity thief may have a link in it. When you click on the link, it takes you to a website and asks you to put in your information.

It may have a telephone number for you to call.

Often fake emails have a warning that your account will be closed or someone has used your account.

They may promise that you will get a refund or a payment if you respond.

They may have spelling mistakes or have a logo that looks strange.

Identity thieves may take mail out of your mailbox, such as your credit card statement or a new set of cheques from your bank.

They may take papers out of your garbage or recycling, such as a “pre-approved” credit card application.

They may steal your purse or wallet. This often happens at work, in crowds, or on public transportation.

They may use an electronic machine called a skimmer to take the personal information from your credit card at a restaurant or a bank machine. They use this information to make a fake credit card.

They may watch you to get your PIN.

They may change your address with creditors or utilities to get your information sent to them.

They can pretend to be you and sell your house or get a mortgage on your house or another property (**title fraud**).



Protect Your Identity

You can protect your identity.

Keep the amount of personal information in your purse or your wallet to the minimum.

Don't carry extra credit cards, your SIN card, birth certificate, or your passport unless you need them on that day. Keep them in a safe place.

Only give your SIN when it is necessary. Ask to use other ID if you can.

PIN

Don't use numbers that are easy to guess for your PIN, and don't write it down anywhere. Change your PIN and passwords often.

Use your hand or your body to keep other people from seeing the numbers for bank machines, direct payment machines, or long-distance telephone cards.

If you think someone else knows your PIN, change it.

Debit and Credit Cards

When you get a new card, sign the back right away.

When you use your debit card or credit card, watch the person doing the transaction.

Check when you get the card back to make sure it is yours. Sometimes fraudsters keep your card and give you a fake card.

When you travel, keep your cards with you or in a hotel safe.

Receipts and Statements

Always take credit card and bank machine receipts. Put them into your wallet or purse, not in the shopping bag where they can fall out.

Check your bank and credit card statements carefully every month.

If you see transactions you don't remember, tell the bank or credit card company right away.

Get your credit reports from Equifax and TransUnion at least once a year.

Check them for credit you didn't **authorize**.

Shredding

Shred any documents with personal information like your signature, your name and address, statements, receipts, utility bills, credit card applications, and insurance forms before you put them in the garbage.

When you get a new document that has identity information (like a driver's licence or vehicle registration), shred the old one.

If your bills don't arrive when you expect them, call the company to make sure they still have the right address.

Telephone Calls

Don't give personal information to anyone who calls you. Tell the caller you are going to check the number and call back yourself.

Only give information if **you** call the number you got from your bill, the back of your bank card or credit card, or from the telephone book.

If a bank, government, or credit card company calls you, they will ask for you by name and they will already know your account information and SIN. They will **not** ask for your SIN, account number, PIN, password, credit card number, expiry date, or security code on the credit card.

They may ask you some questions to check if you are their customer.

Online

Be careful when shopping online. Buy from stores you know and trust.

Watch for the closed lock or unbroken key symbol in the browser window before you put in your personal information.

If you don't see the lock or key symbol, or if the lock is open or the key is broken, someone else on the Internet can get your information.

After you put in personal information, log off the website, clear the browser cache, and close the browser window.

Get anti-spam and anti-virus software on your computer, and install a firewall. Keep them up-to-date.

Be careful reading emails with attachments, or downloading files or programs from the Internet.

Don't email personal or financial information. Other people can get access to your email.

Don't give your personal information in a link from an email.

Mail

If you are going to be away, ask a neighbour to pick up your mail.

If you don't have someone you can ask to pick up the mail, go to the post office and tell them to hold your mail. You have to pay for this.

Spot the Fraud

Here is a sample email that says it is from the Canada Revenue Agency. It looks like it is a real CRA email. How can you tell that it is a fraud?



Dear Tax Payer,

You are entitled to your tax refund now. The tax refund is \$241.34. You are required to follow the link below to login to our secure Epass site with your Social Insurance number and complete the required information in order for your refund to be processed.

<http://www.cra-arc.gc.ca/gol-ged/gov/confirmtaxrefund?REF128328-1h28877a>

Yours sincerely,

Gilles Dompiere, Department of Revenue, Canada

Does the organization have my email address?

The CRA doesn't have your email address. It isn't on the tax form.

Is the email addressed to me?

The email is addressed to Tax Payer, not you.

Does the email tell me I will have a problem if I don't act now?

The email says you can only get your refund if you log in.

Does the email ask for information that the organization already knows or wouldn't ask?

No website should ask for your social insurance number to log in.

Are there mistakes in the email?

At the bottom, it says "Department of Revenue" instead of the right name, Canada Revenue Agency.

Scams

Many **scams** promise you something that is too good to be true.

If it sounds too good to be true, then it is probably a scam.

If you answer the letter, email, telephone call, or ad, the scammers ask you for a fee, an advance payment, or your bank account information.

The scammers take your money and you never get what they promise.

Prizes

They may tell you that you won a big prize, but you have to pay taxes or a fee to get it.

If you win a lottery or a prize, you **never** have to pay taxes or fees on the money you won.

You may fill out a ballot for a contest or draw that is a fraud. The information on the ballot will be used to contact you.

Money Deals

The scammers may say you can get a guaranteed loan at a low interest rate, even with no credit history or a poor credit history.

They may say they need someone to help with a business deal.

They may say they have lots of money that they need to transfer to Canada.

They may say you can buy an investment that will make a lot of money with no risk.

Jobs

The scammers may offer you a job. Part of the job is to put payments through your bank account.

If you are putting payments through your bank account, the money may come from crime.

They may say you can “earn easy money” or get rich quickly.

They may offer a lot of money to work from home.

They may say that you can make a lot of money by selling door-to-door or to friends and family.

If you need to buy lots of **inventory** (things to sell) at the beginning or if they say you make money by getting other people to join, be careful.

There may be people who say how much money they made, but they are part of the scam.

Fake Cheques

If you are getting payment for something you are selling or renting, only accept a cheque that is for the right amount.

Scammers may send or give you a cheque for a higher amount and ask you to give the extra money back in cash or send it by money order or wire transfer.

If their cheque bounces, you would lose your money.

If their cheque is fake, your money is gone by the time you find out.

When you deposit the fake cheque in your bank, you become **liable** for the amount of the cheque too, so you have to pay the bank back.

Threats

They may say that you need to answer now or you will lose your chance.

They may say that you will lose your account if you don't answer.

Sometimes they pretend that they need the money to help someone who is very sick.

Safety Tips

Never click on the link in a scam email, since your computer could be attacked by a fraud website.

Don't answer the scammer.

If it is a telephone call, just hang up.

Never send any money or valuables.

Don't fill out ballots for contests or draws if you don't know the company.

Be careful when you meet people on the Internet. You don't know who they really are.

If you get a cheque that you think may be a fraud, give it to the police. For example, if someone sends you a cheque and asks you to send part of it back by money order or wire transfer, give the cheque to the police.

Don't sign a contract in a hurry. Take time to think it over.

Problems with Fraud

If you are a **victim** of fraud or identity theft, call your bank or credit card company right away.

You can also call the credit-reporting agencies to let them know. They will put a fraud alert on your file.

Report it to your local police.

Keep notes on what happened and the names of the people you tell about the fraud. Keep any papers about the fraud.

If the bank or credit card company says you are responsible, call the Financial Consumer Agency of Canada at 1-866-461-3222.



If you get a fake email or telephone call, you can tell the organization and the police.

You can contact the Royal Canadian Mounted Police (RCMP) at 1-888-495-8501 or at www.phonebusters.com.

You can tell the provincial or local police.

If it is an international scam, you can contact a partnership of international and Canadian police at www.recol.ca.

If you get a fake email or telephone call, you can check to see if the organization has a warning about fraud on its website.

Open a new browser window and use the organization's name or a web address from your statement, agreement, bill, or the Yellow Pages.

They may have examples of phishing and vishing.

The website will tell you what to do if you have given your personal information to a fraudster.

Protecting My Identity

1. I leave extra identity cards at home.
2. I only give my SIN when it is needed.
3. I have a PIN that is difficult to guess.
4. I don't write my PIN down anywhere.
5. I use my hand to block other people from seeing my PIN.
6. I sign the back of any new card right away.
7. I watch my card when I use debit or credit.
8. I keep credit, debit, and bank machine receipts.
9. I check my bank and credit card statements.
10. I check my credit reports once a year.
11. I shred documents with personal information.
12. I don't give personal information on the phone unless I called.
13. I look for the closed lock or unbroken key on websites.
14. I log off, clear the cache, and close the browser window.
15. I have anti-spam and anti-virus software and a firewall.
16. I don't email personal information.
17. I look out for phishing and vishing scams.
18. I get someone to take care of my mail when I am away.