GOVERNMENT AGENCIES

Canadian Anti-Fraud Centre;
www.antifraudcentre.ca
1-888-495-8501

Competition Bureau of Canada;
www.competitionbureau.gc.ca
1-800-348-5358

Consumer Protection Ontario;
www.ontario.ca/consumers/comsumer-protection-ontario
1-800-889-9768

Police Non-Emergency
416-808-2222

Working Together to Prevent Crime

SP 917-E, 2015/02

Fraud- Know it Before it Knows You

www.torontopolice.on.ca/financialcrimes

GRANDPARENT SCAM

The "Grandparent Scam" is a scam where a grandparent receives an unexpected telephone call from a person claiming to be their grandson or granddaughter. The caller will say it is an emergency and ask that you send money immediately.

The call usually starts off with "Hi, Grandma/Grandpa". When the grandparent says "hi" the caller would then say "Do you know who this is". It is at this point, the grandparent says a name which is usually a name of one of their grandchild.

The caller would then request that the grandparent to send money ASAP, with the grandchild indicating that they are either in jail or in the hospital, and to not tell their parents.

With the grandparent wanting to help, they would send money by either Western Union or Money Gram, as they can pick it up quickly in cash.

If the money has not been picked up, it can be retrieved. If it has, the money is gone.

How do these scammers choose who to contact? They obtain your information from marketing lists, social networking sites, and telephone listings.

How do these scammers know the names of your grandchild? They do not. Sometimes one will mention it, or from the obituary; again social networking sites.

How to Protect Yourself: If you get a telephone call from someone claiming to know you and asking for your help, check to confirm that it is legitimate before you send any money. Ask questions that would be hard for a stranger to answer. **DO NOT** send money unless you are certain it is the real person you know.

IF YOU HAVE BEEN SCAMMED

If you think you may be a victim of a fraud or scam, there are some key steps you should take immediately to reduce your risk of losing more money, and to avoid being scammed again:

⇒ Stop all communication with the scammer;

⇒ Stop making any major financial decisions until your accounts are secured;

⇒ Gather all records you have of the scam;

⇒ Notify your financial institution and other companies where you have an account that may have been affected;

⇒ Change all your passwords to your accounts including social media sites;

⇒ Protect your devices such as: computer, laptop, tablet if you used it to communicate with the scammer;

⇒ Ensure security software on your device is up to date;

⇒ Install anti-spyware protection;

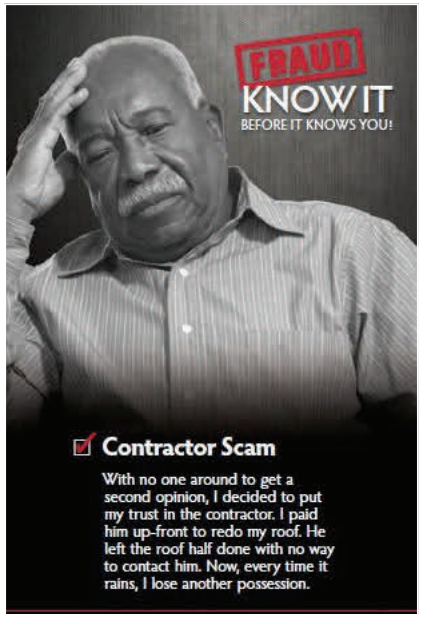
⇒ Scan your hard drive and files;

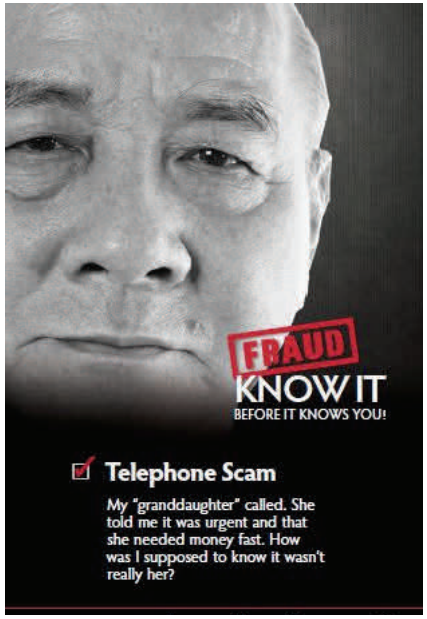
⇒ Never send your personal, credit card or online banking details through an email; and

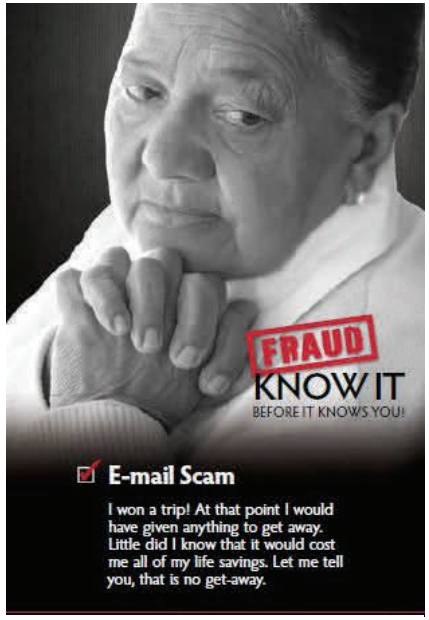
⇒ Put an alert on your credit report by contacting Equifax Canada or TransUnion Canada;

To report any banking and credit card scams, contact your local bank's or financial institution(s).

To report Spam Emails and SMS, visit www.fightspam.gc.ca for information on Canada's anti-spam legislation.







IDENTITY THEFT

Identity theft occurs when someone has taken possession of your credit card information, drivers licence, social insurance number, bank account or other personal information. Once an identity has been "stolen" in this manner, the thieves can go on a shopping spree, leaving you to deal with the financial, legal and psychological costs.

Your personal information can be reproduced to access your bank accounts, open new bank accounts, apply for loans, credit cards, make purchases, obtain passports and receive government benefits.

How to Protect Yourself: If any key documents are lost or stolen, **IMMEDIATELY** notify the issuer and the police. Shred all your sensitive personal documents before tossing them into the garbage. Always protect your PIN and never give it to anyone else. Carry only documents you absolutely need.

If you suspect or know that you are a victim of identity theft, contact your local police service and file a report. Regularly check your credit with Equifax Canada, Toll Free: 1-800-465-7166 or TransUnion Canada, Toll Free: 1-877-525-3823.

INVESTMENT/PONZI SCHEME

A Ponzi Scheme is a fraudulent investment where the scammer pays returns to its investors from new investors, rather than from profit earned by the operator. New investors are usually enticed by offering higher than normal returns than other investments, in the form of short-term returns. A Ponzi Scheme requires increasing flow of money from new investors to sustain the scheme.

Ponzi's are attractive to investors because of above-market investment returns. As new money stops flowing into the Ponzi, old investors cannot cash out, causing a cash crunch and the eventual demise of the scheme.

How to Protect Yourself: **"**If it sounds too good to be true, it probably is". An investment opportunity can look like a sure thing, but investors must always think rationally rather than emotionally. Guarantees of high annual returns are unrealistic, as markets fluctuate. Choose an investment manager carefully. Experience and skill should be considered, rather than personality or charisma.

PHISHING SCAMS

Phishing Scams are typically fraudulent email messages appearing to come from legitimate sources (e.g., your internet service provider, your bank). The e-mail usually directs you to a spoofed website in an attempt to get you to divulge private information (e.g., passwords, credit card numbers). The message is designed to induce panic in the reader.

An example of a common phishing attempt is, an email message stating that you are receiving it due to fraudulent activity on your account and asking you to "click here" to verify your information.

CHEQUE OVERPAYMENT SCAM

Overpayment Scam is the type of fraud where the person receiving the cheque is actually owed money for goods sold. The seller receives a counterfeit cashier's cheque, personal cheque or corporate cheque from the "purchaser" in an amount in excess of the amount owed; is asked to deposit the cheque and wire the excess funds immediately back to the sender/purchaser or the purchaser's agent or shipper; and, the deposited cashier's cheque is subsequently returned as counterfeit and charged back to the seller's account.

Anyone selling goods should be suspicious of any cheque, especially if it is for more than the agreed selling price. Consider an alternative method of payment, such as an escrow service or online payment service. Talk to your bank about the safest way to receive funds from overseas.

To protect yourself against this sort of scam, never agree to a deal in which the payer wishes to issue an amount for more than the agreed price and expects you to reimburse the balance. The scammers use a variety of excuses to explain the overpayment, but any such excuse should be treated with the utmost suspicion.

How to Protect Yourself: Know who you are dealing with; independently confirm your buyer's name, street address, and telephone number. Never accept a cheque for more than your selling price. Never agree to wire back funds to a buyer. A legitimate buyer will not pressure you to do so, and you have limited recourse if there is a problem with a wire transfer. Resist pressure to "act now."

delivery. In addition to stressing the urgency and confidentiality of a transaction, these letters will also stress the importance of trust and honesty in order to make the reader believe that there is validity to the letter. For instance, the writers of these letters will commonly claim to be a doctor and/or a corporate entity with a major corporation of Nigeria. There will also be some mention of government involvement.

Typically, after receiving a letter a consumer would respond either by phone, fax, or email. The response would be a request for further information on the requirements and procedure for the transaction. Once contact is established, the writer of the letter will normally ask for an up front processing fee, and in some cases arrange for a meeting to discuss the transfer of funds. Most letters come with a breakdown of the percentage of money each party involved will receive once the transaction is final. For instance, many letters received at CAFC offer the following breakdown:

1 30% for the account holder;
1. 60% for me and my partners; and
2. 10% to be used in offsetting taxes and all local & foreign expenses.

How to Protect Yourself: Do not open unsolicited emails. Spam usually means scam and the message may contain a virus that can damage your computer.

Phishing Scams are all about tricking you into handing over your personal and banking details to scammers. The emails you receive might look and sound legitimate, in reality genuine organizations like a bank, or a government authority will never expect you to send your personal information by an email or online.

Do not just assume an email you receive is legitimate, if the email is asking you to visit a website to "update", "validate" or "confirm" your account information, be skeptical.

How to Protect Yourself: Do not reply to spam emails, do not click on any links or call any telephone number listed in a spam email(s). Call your bank(s) or financial institution(s) to inquire the email you received is legitimate.

DATING AND ROMANCE SCAMS

Dating and Romance Scams try to lower your defences by appealing to your romantic and compassionate side. Common examples - scammers on legitimate dating sights, will build a relationship with you over a few emails and eventually give you a story about a sick family member, or a story of despair. They will ask you directly or more subtly for money, to help them in their situation.

Once they get what they want, they disappear. In other cases, you slowly get lured with gifts or flowers. The scammer will tell you about a large sum of money they need to transfer out of their country, or that they want to share with you. They will then ask for your banking details, money for an administrative fee, or tax that they claimed needs to be paid to free up the money.

How to Protect Yourself: Never send money, give credit card or online account details to anyone you do not know and trust.

RENOVATION/UTITLTY FRAUD

This scammer will come to your door claiming to be in the neighbourhood and offering a "discount, today only". They appear friendly and knowledgeable, will offer you a service regardless if you need it. This Scam often targets seniors by convincing them they need something (e.g., paved driveway or a new roof) Charging more than fair market prices, and often taking a hefty deposit; sometimes never doing the work or only partially completing it.

Be assured, their true intention is to convince you to sign a contract and to line their own pockets, while they politely empty yours.

How to Protect Yourself: Always be cautious of those who come to you door. Do not leave anyone alone to roam your home. Do not be in a rush. Take your time and be an educated consumer.

proves you for a loan, then calls or emails you demanding a fee before you can receive the money, it is most likely a scam. Ads that promise loans generally appear in classified sections of local and national newspapers, magazines and tabloids.

Remember: simply advertising through recognized media outlets does not ensure the legitimacy of the company behind the ad.

ANTI-VIRUS SCAM

Generally, this Scam involves company representatives calling individuals and stating, for example, that it is Microsoft calling and that their computer is running slow or has viruses. They offer to repair the computer over the internet, which can involve the installation of software or the customers allowing the representatives remote access to their computer.

How to Protect Yourself: Allowing a third party to download software or remotely access a computer carries inherent risks. Keyloggers or other malicious software could be installed to capture sensitive data such as online banking user names and passwords, bank account information, identity information, etc.

419 ADVANCED FEE LETTER SCAM

Throughout Canada and the United States letters concerning the "request for urgent business transaction" usually the transfer of millions of dollars, are being sent out to consumers and business" via mail, email and fax transmission. These letters are commonly referred to as Nigerian Letter Scams or West African Fraud Letters.

The scheme begins once a consumer receives a letter. The preferred method of sending these letters is via email . The Canadian Anti-fraud Centre (CAFC) has seen an increase in email

countable to pay for the funds he/she wired.

Another similar "mystery shopper" Scam, the victim answers an ad for a job. The "employer" sends the victim a cheque for $1200 and is told to cash the cheque and keep $200. The scammer tells the victim to "mystery shop" at a particular gas station, with the remaining funds. The victim is instructed to purchase $1000 worth of merchant gift cards. The victim is told to pay attention to the cleanliness of the shop and to rate customer service. The victim calls the "employer" and gives him/her the gift card numbers. Again, the victim later finds out that the cheque is counterfeit and is now accountable for the funds to his/her bank.

How to Protect Yourself: ***Never pay to become a mystery shopper!*** This includes never accepting a cashier's check in exchange for you wiring or sending money to a person or company. Again, it never costs money to get assignments or to become a shopper.

ADVANCE FEE LOANS SCAM

Some companies claim they can guarantee you a loan even if you have bad credit or no credit. They usually request an up front fee, which may range from hundreds to thousands of dollars. Once you send your money to these companies, you never get your promised loan and you cannot get your money back. If you cannot get a loan through traditional lending institutions, it is unlikely that you'll get one in response to a classified ad. Ask the loan company to take the amount of their fee off of the total amount of the loan that was promised you. In most jurisdictions, it is illegal for a company to request an up front fee prior to obtaining a loan.

How to Protect Yourself: Do not pay upfront. If a lender ap-

CALL DISPLAY SPOOFING

Most of us make use of call display features on our personal and business phones. We believe that the phone number displayed is actually that of the caller, or is associated to the place the caller is calling from.

Unfortunately, call display features can display inaccurate information via the use of **"call spoofing"** services. Such services enable the caller to cause any phone number that they desire to appear as the number they called from on a person's call display. Some call spoofing services offer the option to the caller of using a male, female, or "garbled" voice.

Call spoofing is a technique used by "fraudsters" to falsify the telephone number and or name that appears on a person's caller ID. These "fraudsters" then try to trick you into giving your personal information such as your social insurance number, passwords, address, and last name over the telephone, allowing them to gain access to your accounts. The unfortunate truth is that we cannot rely on call display information to be accurate.

How to Protect Yourself: Never give out personal information in response to an incoming call. Fraudsters are clever; they often pose as government agencies, credit card companies, and bank representatives to get people to reveal their personal information. If you are in doubt about the identity of a person who is calling you, ask appropriate questions. Never assume that the caller is who he/she claims to be, based upon the call display information alone.

SOCIAL ENGINEERING

Social Engineering is a method used by fraudsters in support of the various forms of identity theft. Social Engineering can be online or offline activities which are all associated with one motive in mind to glean personal information from, or related to intended victims. Personal information that is valuable to fraudsters (identity thieves) includes, but is not limited to the following types of identity information:

- Name;
- Date of birth;
- Address;
- Phone number(s);
- Employment information;
- Financial Information, including credit card numbers, loan information, mortgages held, etc.;
- Information on family members;
- Potential password information such as mother's maiden name;
- Social Insurance Number;
- Drivers Licence Number; and
- Citizenship information/Immigration information.

Often, the above information is held by persons other than the intended victim. Employers, banks, government institutions, insurance companies, and many other entities have access to such materials. In a typical scenario, persons with legitimate access to identity information will be contacted by fraudsters posing as the intended victim.

A conversation ensues, and the holder of the identity information is convinced to "let their guard down." Trickery is used to convince the holder of the information that it is safe to release the identity information to the fraudster. (Often, but not always over the phone).

False Charities cont'd;

that help children who are ill. All registered charities in Canada are overseen by the Canada Revenue Agency, and are listed in a database. You can also contact your local Better Business Bureau to inquire if they have any information about the organization. If the charity is genuine and you want to make a donation, get the charity's contact details from the telephone book or a trusted website, source.

How to Protect Yourself: If you have any doubts at all about the person asking for money, do not give them any cash, credit card or bank account details. Never give out your personal, credit card or online account details over the telephone unless you made the call and the telephone number came from a trusted source. Search the Canada Revenue Agency database to check that the charity that has approached you is genuine.

MYSTERY SHOPPER

Any false, deceptive or misleading solicitation offering employment and requesting an advance fee to secure the job, or obtain the materials to perform the job, or any job offer involving money transfer or wiring funds related to cashing monetary instruments.

The "Mystery Shopper" the victim answers an enticing ad to become a mystery shopper. The "employer" sends a letter, with mystery shopping tasks to be completed, and a cheque to help the victim fulfill his/her mystery shopping tasks. The victim will likely cash the cheque he/she was given first. One of the tasks will be to use a money transfer company and wire a large portion of the money to a name provided, in order to test the company's procedure and customer service skills. The victim will find out later that the cheque is counterfeit, thus making the victim ac-

mate product or providing a service. Pyramid Schemes inevitably collapse and you will lose your money. In Canada, it is a crime to promote a pyramid scheme or even to participate in one.

How to Protect Yourself: Never commit to anything at high pressure meetings or seminars. Don't make any decisions without doing your homework. Research the offer being made and seek independent advice before making a decision.

FALSE CHARITIES

Charity Scams take advantage of people's generosity and kindness by asking for donations to a fake charity or by impersonating a real charity.

With Charity Scams the scammers can approach you in many different ways, on the street, at your home, over the phone, or on the Internet. Some emails and collection boxes are mark with the logos "genuine charities".

Often the scammer would use a recent natural disaster or famine to exploit for money claiming that it is a charity. Other scammers play on your emotions by pretending to be from charities

Once that information falls into the hands of fraudsters, it may be used to apply for loans, credit cards, bank accounts, tax refunds etc. Your Identity Information is treated like a commodity. Identity information is bought and sold between groups of fraudsters, based on their needs. Extreme care must be taken when asked by any person to provide your identity information or that of another person to a third party.

How to Protect Yourself: Never give out any confidential information whether it is over the phone, online, or in-person, unless you can first verify the identity of the person asking and the need for that person to have that information. If you receive a telephone call from your credit card company saying your card has been compromised. Hang up and call the number on your credit card rather than speaking to whoever called you. Always remember financial institutions will never ask for your password or other confidential information over the telephone.

BLACK MONEY

"Black Money" may appear in support of a variety of fraudulent scams. Any scam where a victim is eventually offered cash may involve the use of black money at some point in the process. Black Money describes paper sheets that have been bundled to appear as genuine currency that has been blackened by a "special compound." Typically, victim is told that the money is

related to foreign government deposits, and that the currency has been blackened with a substance that is nearly impossible to remove in order to prevent the money from being used by persons who should not have it.

Victims are further advised that only a very expensive compound can remove the black substance from the bills. A supposedly random bill is selected from the bundle, and the compound is applied to the bill. The black substance is removed, revealing a genuine $20, $50, or $100 bill.

The problem is that the bill selected was not random. Usually, it's the only genuine bill in a large bundle. The rest of the "bills" are worthless paper. The genuine bill is black because it was run through an inkjet printer, and the "special compound" is actually ink solvent or a similar substance. Victims are encouraged to pay thousands of dollars for access to the special compound that will supposedly allow them to wash the entire bundle of currency.

How to Protect Yourself: There is no such thing as painted money recovery. Never strike a deal in a parking lot. It is important to remember to be vigilant when approached with "too good to be true" opportunities.

THE AFFINITY METHOD

"Affinity Fraud" occurs when a fraudster convinces an unwitting third party to use their personal connections of family, friends, and co-workers to "do their dirty work." This is especially prevalent in Investment Scams, and Pyramid Schemes. A well intentioned person is convinced to "buy in" to a financial proposal, or business transaction. The proposed transaction is entirely fraudulent, but the person is unaware of this.

Convinced that they are about to make their friends, relatives, and co-workers wealthy, the person begins to aggressively market the proposal/transaction to their network. The fact that the "sales job" is being performed by a friend/relative/co-worker causes potential victims to feel at ease with the proposed transaction, and buy into it and/or market it themselves.

What makes this method so devastating is that once the whole scheme collapses and financial losses are endured, relationships between friends and family are shattered forever.

How to Protect Yourself: Affinity Fraud is one of the most difficult scams to protect yourself against because being suspicious of your family or friends can be difficult. Loyalty within the group can also make it difficult for law enforcement officials to detect affinity fraud. Some groups refuse to believe that fraud has occurred. Be cautious of a "too good to be true" proposal.

PYRAMID SCHEMES

Pyramid Schemes promise a large financial return for a relatively small cost. Pyramid schemes are illegal and very risky and can cost you a lot of money. In a typical Pyramid Scheme, unsuspecting investors are encouraged to pay large membership fees to participate in money making ventures. The only way for you to ever recover any money is to convince other people to join and to part with their money as well. People are often persuaded to join by family members or friends, there is no guarantee that you will recoup your initial investment.

Although pyramid schemes are often cleverly disguised, they make money by recruiting people rather than by selling legiti-