



## Increasing Your Fraud Awareness

### Fraud Prevention Forum

The Fraud Prevention Forum, formerly the Deceptive Telemarketing Prevention Forum, is a concerned group of private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations committed to fighting fraud aimed at consumers and businesses. Credit Union Central of Canada has been representing the Credit Union System on this initiative.

It has developed a wide reaching public awareness campaign based on an analysis of existing research on the profile of fraud victims, a quantitative study on the scope of the problem in Canada and focus testing of messages which resonate with the public. The Competition Bureau chairs the Fraud Prevention Forum which has developed new tools and information that will empower Canadians to recognize, report and stop fraud such as deceptive telemarketing, lottery and prize scams and identity theft. There are many known scams, and new ones are invented every day.

### Prize Pitch

One of the most common scams is the "prize pitch". Consumers are told they have been specially selected to win a prize, or have been awarded one of three or two of five prizes. These prizes usually include cash or a vehicle. You must purchase a product and pay in advance to receive your prize. These products may include "coin collections", personalized pen sets, etc. The products are generally cheap or overpriced, but may sound valuable over the phone.

**Remember, in a legitimate contest you do not have to purchase a product to qualify for a prize.**

You may also encounter the "sweepstakes scam". After entering a fake sweepstakes contest in the mail, you will receive a call within two to four weeks from a fraudulent telemarketer. This person will usually identify themselves as a lawyer, judge, customs agent or other official. They will represent themselves as an agent for a particular company. You will be told that you have won a large cash award, but money must be sent up front for taxes, etc.

### Recovery Pitch

If you buy into any of the Prize Pitch schemes, you are likely to be called again by someone promising to get your money back for you. Be careful not to lose more money to this common

practice.

Here are two examples of the stories you may be given over the phone:

A caller claiming to be a law enforcement officer tells you that money has been seized, and that their records indicate that you have lost money to the company or companies. They will help you recover the money you have lost for a small fee. **DO NOT BELIEVE THEM.** If money is seized, you will be advised by a police agency but they will never request money in advance for any reason.

The caller may claim that they have bought out a particular company that promised you prizes that were never sent to you. They are an honest company, and they are eager to get those prizes right out to you if you can pay some related costs. **DO NOT BELIEVE THEM! HANG UP AND CALL PHONEBUSTERS!**

## **Advanced Fee Loans**

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.

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.

## **Travel**

By simply filling out a ballot to win a vacation at a home, boat or auto show, you may be set up for "suckers lists". Shortly after filling out this ballot, you may be contacted over the phone by someone claiming to offer you a "free" or "low cost" vacation. They will ask for your credit card number and personal information in order to hold the vacation for you, or they may request money in advance.

**Don't give out your credit card information over the phone.** If you want to check out the value of these promises, seek out the advice of a legitimate travel agency in your area. If you have provided credit card information to the telemarketers, be aware that most companies have policies that allow you to cancel your reservation within 30 days. **Do not let anyone pressure you into committing to any agreement over the phone.**

## **False Charities**

In Canada we have a long and honourable tradition of voluntary giving to those in need, often through charity organizations. But if an unfamiliar charity organization contacts you - by mail, phone, or Internet - be careful.

Bogus charities often use names that are very close to the names of legitimate and respected charities. The end of the year is the peak season for charity appeals. It also is the peak season for the bogus charity appeals.

### **Warning signs**

- High pressure or threatening telemarketers who want you to contribute immediately.
- Someone calls and thanks you for a pledge you don't remember making.
- Copycat names. Names that might be misleading or deceiving.

### **What you can do**

- If you receive a telephone call, ask for the information to be sent to you in writing. Ask how much of your gift will be used directly for the charity. Ask how much will go toward administrative costs. Legitimate charities have no problem giving you this information.
- Remember on an incoming call a person could be misrepresenting a legitimate charity.
- Never give out your personal / financial information out over the phone, or at the door. You may wish to make out a cheque payable to the charity. You can mail the cheque later.
- Call the charity. Find out if they know about the appeal and have authorized it and what percentage of your donation they will receive from your donation. Perhaps there is a better way to give, where 100% of your donation will reach the charity.
- Ask if charity is registered. Contact Revenue Canada at 1-800-267-2384. Ask them to give you the charitable tax number of the charity. Question any discrepancies.
- At the beginning of each year decide which charities you can afford to donate to - send your cheques directly to their head office, and feel good about giving. When approached you can say that you have already given and leave it at that. Perhaps you will consider their appeal next year when you decide on the charities you can afford to give to.
- To file a complaint call your local police and **PhoneBusters 1-888-495-8501**.

## **Pyramid Schemes**

Pyramid schemes are frauds that are based on recruiting an ever-increasing number of investors. The initial promoters (those at the peak of the pyramid) recruit investors who are expected to bring in more investors, who may or

may not sell products or distributorships. Recruiting newcomers is more important than selling products.

No new money is created in pyramid schemes. Investors who get in early take their profits from investors who join later. At some point, no new investors can be found and as a result the last investors, who are at the bottom of the pyramid, lose their money. They also face prosecution, as pyramid schemes are illegal.

Before you invest any money in a multi-level company that could be a pyramid, get all the facts about the company, its officers and its products. Get written copies of the company's marketing plan, sales literature, contracts and prospectus (a legal document that gives prospective investors information about the company). Avoid promoters who fail to clearly explain their plans. Have a lawyer or accountant explain anything you do not understand. Find out if there is a demand for the product, or if there are similar products on the market.

Remember that the greater the promised return, the greater the risk.

**Pyramid schemes are illegal under the Competition Act, and serious charges may be brought against you if you are operating or affiliated with one of these schemes.**

Effective January 1, 1993, Industry Canada made amendments to the Competition Act, Section 55. A multi-level sales procedure is a pyramid if:

- There is compensation paid for recruiting a new salesperson
- There is inventory loading, that is, the recruits must purchase an unreasonable quantity of product
- Purchases are required as a condition of entry. (You may, however, be required to pay for a sample kit, but this kit must be at cost.)

## **Advanced Fee Letter Fraud (West African / Nigerian Letters)**

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. Letters are sent by mail, fax transmission and email, while email transmission being the preferred method of delivery for the letters. PhoneBusters has seen an increase in email 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 the letter is valid. 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 PhoneBusters offer the following breakdown,

1. 30% for the account holder
2. 60% for me and my partners
3. 10% to be used in offsetting taxes and all local & foreign expenses.

Copies of the letters can be directly forwarded to PhoneBusters via fax at (888) 654-9426 or by email at [waf1@phonebusters.com](mailto:waf1@phonebusters.com)

### **How Can I recognize a Scam?**

#### **It sounds too good to be true**

- You've won a big prize in a contest that you don't recall entering. You're offered a once-in-a-lifetime investment that offers a huge return. You're told that you can buy into a lottery ticket pool that cannot lose.

#### **You must pay or you can't play**

- "You're a winner!" but you must agree to send money to the caller in order to pay for delivery, processing, taxes, duties or some other fee in order to receive your prize. Sometimes the caller will even send a courier to pick up your money.

#### **You must give them your private financial information**

- The caller asks for all your confidential banking and/or credit card information. Honest businesses do not require these details unless you are using that specific method of payment.

#### **Will that be cash... or cash?**

- Often criminal telemarketers ask you to send cash or a money order, rather than a cheque or credit card. Cash is untraceable and can't be cancelled. And, crooks also have difficulty in

establishing themselves as merchants with legitimate credit card companies.

### **The caller is more excited than you are**

- The crooks want to get you excited about this “opportunity” so that you won't be able to think clearly.

### **It's the manager calling**

- The person calling claims to be a government official, tax officer, banking official, lawyer or some other person in authority. The person calls you by your first name and asks you a lot of personal or lifestyle questions (like how often do your grown children visit you).

### **The stranger calling wants to become your best friend**

- Criminals love finding out if you're lonely and willing to talk. Once they know that, they'll try to convince you that they are your friend – after all, we don't normally suspect our friends of being crooks.

### **It's a limited opportunity and you're going to miss out**

- If you are pressured to make a big purchase decision **immediately**, it's probably not a legitimate deal. Real businesses or charities will give you a chance to check them out or think about it.

## **What can I do to protect myself?**

Remember, legitimate telemarketers have nothing to hide.

- However, criminals will say anything to part you from your hard-earned money.
- Be cautious. You have the right to check out any caller by requesting written information, a call back number, references and time to think over the offer.

Legitimate business people will be happy to provide you with that information. After all, they want the "bad guys" out of business too. Always be careful about providing confidential personal information, especially banking or credit card details, unless you are certain the company is legitimate. And, if you have doubts about a caller, your best defense is to simply hang up. It's not rude – it's smart.

If you're in doubt, it's wise to ask the advice of a close friend or relative, or even your banker. Rely on people you can trust.

Remember, you can **Stop Phone Fraud - Just Hang Up!**

**I suspect that a relative or friend is being targeted by unscrupulous telemarketers. What can I do?**

Watch for any of these warning signs

- a marked increase in the amount of mail with too-good-to-be-true offers
- frequent calls offering get-rich-quick schemes or valuable awards, or numerous calls for donations to unfamiliar charities
- a sudden inability to pay normal bills
- requests for loans or cash
- banking records that show cheques or withdrawals made to unfamiliar companies
- secretive behavior regarding phone calls.

If you suspect that someone you know has fallen prey to a deceptive telemarketer, don't criticize them for being naïve. Encourage that person to share their concerns with you about unsolicited calls or any new business or charitable dealings. Assure them that it is not rude to hang up on suspicious calls. Keep in mind that criminal telemarketers are relentless in hounding people – some victims report receiving 5 or more calls a day, wearing down their resistance. And, once a person has succumbed to this ruthless fraud, their name and number will likely go on a "sucker list", which is sold from one crook to another.

## **Identity Theft: Could it Happen to You?**

Maybe you never opened that account, or ordered an additional card, but someone else did....someone who used your name and personal information to commit fraud. When an imposter co-opts your name, your Social Insurance Number (SIN), your credit card number, or some other piece of your personal information for their use - in short, when someone appropriates your personal information without your knowledge - it's a crime, pure and simple.

## **Are you a Victim?**

The signs can be many, but typical indicators that your identity is being used include:

- A creditor informs you that an application for credit was received with your name and address, which you did not apply for.
- Telephone calls or letters state that you have been approved or denied by a creditor that you never applied to.
- You receive credit card statements or other bills in your name, which you did not apply for.
- You no longer receive credit card statements or you notice that not all of your mail is delivered.
- A collection agency informs you they are collecting for a defaulted account established with your identity and you never opened the account.

## **Identity Theft Statement - What is it?**

If you have been a victim of identity theft, the Identity Theft Statement helps you notify financial institutions, credit card issuers and other companies that the identity theft occurred, tell them that you did not create the debt or charges, and give them information they need to begin an investigation. A copy of the Identity Theft Statement is available at your branch of Trico Credit Union.

If you suspect that your personal information has been hijacked and misappropriated to commit fraud or theft, take action immediately and keep a record of your conversations and correspondence. The following basic actions are appropriate in almost every case.

- Start a log of dates, person(s) that you spoke with and exactly what they said.
- Contact the fraud departments of each of the two major credit bureaus.
- Equifax: (800) 465-7166 and Trans Union: (877) 525-3823
- Request that a "Fraud Alert" be placed in your files. At the same time order copies of your credit reports.
- Contact the fraud department of creditors for any accounts that have been opened or tampered with fraudulently. This may include credit card companies, phone companies, banks and other lenders.
- File a report with your local Police or the Police in the community where the identity theft took place.
- Contact PhoneBusters National Call Centre. PhoneBusters is currently central sourcing all pertinent information on Identity Theft to identify trends and patterns, information is also used to assist law enforcement agencies in possible investigations.

**Remember:** There is no reason to be paranoid; there's just reason to be careful. If someone wants desperately to target you, they can probably get a lot of information about you -- so you just need to minimize the criminal's opportunities to get that information. You can make yourself a harder target and that's the best defense. If you are a victim, do not panic, you will not be out any money. The losses will be attributed to the banks and or companies associated with the fraud.

## **Minimize The Risk**

While you probably can't prevent identity theft entirely, you can minimize your risk. Identity theft is on the rise and it can happen to anyone. It can happen to you. By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft.

## **Identity Theft: Tips that will help minimize your risk.**

1. Before you reveal any personal identifying information, find out how it will be used and if it will be shared.
2. Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time.
3. Guard your mail. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after delivery. Ensure mail is forwarded or re-routed if you move or change your mailing address.
4. Utilize passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SIN or your phone number.
5. Minimize the identification information and number of cards you carry.
6. Do not give out personal information on the phone, through the mail or over the internet unless you have initiated the contact or know with whom you're dealing.
7. Keep items with personal information in a safe place. An identity thief will pick through your garbage or recycling bins. Be sure to tear or shred receipts, copies of credit applications, insurance forms, physician statements and credit offers you get in the mail.
8. Give your SIN only when absolutely necessary. Ask to use other types of identifiers when possible.
9. Don't carry your SIN card; leave it in a secure place.

## **Phishing**

The word phishing comes from the analogy that Internet scammers are using email lures to 'fish' for passwords and financial data from the sea of Internet users.

Phishing, also called "brand spoofing", is the creation of email messages and

Web pages that are replicas of existing, legitimate sites and businesses. These Web sites and emails are used to trick users into submitting personal, financial, or password data. These emails often ask for information such as credit card numbers, bank account information, social insurance numbers, and passwords that will be used to commit fraud.

The goal of criminals using brand spoofing is to lead consumers to believe that a request for information is coming from a legitimate company. In reality it is a malicious attempt to collect customer information for the purpose of committing fraud.

### **Tips on how to spot and avoid phishing scams**

- Protect your computer with anti-virus software, spyware filters, email filters and firewall programs.
- Contact the financial institution immediately and report your suspicions.
- Do not reply to any email that requests your personal information.
- Look for misspelled words.

Always report phishing or 'spoofed' emails.

If you've received one of these suspicious emails, report it to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org) or the financial institution that it appears to be from.

**You can report any suspicious calls to PhoneBusters at the same toll free number in Canada or the United States.**

**Toll Free:**

1-888-495-8501

**Overseas and Local:**

1-705-495-8501

**Toll Free Fax Number:**

1-888-654-9426

**Fax Number (Overseas and Local):**

1-705-494-4008

**Mailing Address:**

Box 686

North Bay, Ontario P1B 8J8

**E-mail:** [info@phonebusters.com](mailto:info@phonebusters.com)

**Nigerian Letters Only:** [waf1@phonebusters.com](mailto:waf1@phonebusters.com)