

# IDENTITY FRAUD

Anyone that has any form of personal identification documents, like a social insurance card, birth certificate, or passport, can fall victim to identity fraud and not even know it.

Identity fraud can be described as someone else using your personal information to make transactions on your behalf. These transactions can include opening new credit cards, taking money out of your bank accounts, and ordering items online, just to name a few.

'Phishing' is the practice of sending fake emails in an attempt to 'fish' or get your passwords and financial data. Typically, these fake emails try to trick people into clicking on the link provided to get the user to update personal information. Another example of identity fraud is 'vishing', which is the telephone version of 'phishing'. It starts with a phony email that gives a false number to call where 'customer service' will ask for the user to update personal information. The goal of using 'phishing' or 'vishing' techniques is to make people believe that the request for the information is coming from a valid company.

According to a recent consumer survey published by McMaster eBusiness Research Centre (Sproule & Archer, 2008), 1.7 million Canadian adults were victims of identity fraud in the past year. More than \$150 million was spent to resolve the problems caused by these frauds. Most victims (57%) did not know how their personal information was obtained. Therefore, it is very important to do what you can to protect yourself.

## PROTECT YOURSELF

Tips to help protect you against identity fraud:

### PERSONAL DOCUMENTS

- Only share personal information with companies you know well and can trust.
- Keep important documents, like your social insurance number or birth certificate in a safe place, not in your wallet.
- Don't leave your personal information lying around at home, work, or in a vehicle.
- Always destroy old identification documents when you renew or replace them.
- Shred all documents with personal information.

### CREDIT/DEBIT CARDS

- Keep your wallet or purse close to you at all times.
- When using your credit or debit card, keep the card in sight; make sure it's your card when it is returned.
- Look closely at the bank machine that you are using to verify the card reader has not been tampered with.

### TRANSACTIONS

- Don't give personal information over the phone or by email.
- Carefully review emails and check for misspelled words.
- Make sure the website you are using is secure before inputting personal information.
- Keep your computer firewalls and spyware up to date.

# PREVENT IT

Tips to avoid identity fraud:

## PERSONAL IDENTIFICATION NUMBERS (PIN)

- Memorize your PIN; never write it down or share with anyone.
- Always cover the keypad when entering your PIN.

## CREDIT/DEBIT CARDS

- Make a list of the cards you have in your wallet, their account numbers, and customer service contact information. Keep this in a safe place.
- Check your monthly statements to make sure they are your transactions.
- Report lost or stolen cheques, credit cards, and identification documents as soon as possible.
- Order a free copy of your credit report at least once a year.

# REPORT IT

If you think that you are a victim of identity fraud, contact your financial organization right away. It is also important to report fraud to your local police. If the financial organization holds you responsible, contact the Financial Consumer Agency of Canada to find out your rights and responsibilities.

There are consumer protection policies that are in place to help protect you from identity fraud. For example, the **Zero Liability Public Commitment** policy protects consumers if their credit card or credit card number has been used in a false transaction, even if it was in a store, on the telephone, or online. However, this policy does not apply to automated bank machine (ABM) transactions when using your PIN. **Visa E-Promise** is another policy that can add extra protection for Visa cardholders when shopping online, by mail, or by telephone.

### KEY REFERENCES:

Financial Consumer Agency of Canada. (2007). *Protecting yourself from fraudulent e-mails and telephone calls*. Ottawa: ON: Author.

Sproule, S. and Archer, N. (2008). *Measuring identity theft in Canada: 2008 consumer survey working paper #23*. Hamilton, ON: University of McMaster, McMaster eBusiness Research Centre.



# RECOGNIZE IT

There are many scams out there designed to alarm consumers and to force an instant response. Here are some warning signs to look for:

- The offer sounds too good to be true. (For example, you don't remember entering this contest in which you have won the prize.)
- You must make a payment before the delivery of service.
- You must give private financial information even if it is not required.
- You can only pay with cash. Note: cash can not be traced nor can the payment be cancelled.
- It's a limited time offer and you are going to miss out.
- The person that you are dealing with wants to be your new best friend.

# WEBSITES & RESOURCES

## PHONE BUSTERS

Information on false telemarketing pitches

[www.phonebusters.com](http://www.phonebusters.com)

1-888-495-8501

## FINANCIAL CONSUMER AGENCY OF CANADA (FCAC)

Provides financial services information

[www.fcac.gc.ca](http://www.fcac.gc.ca)

1-866-461-3222

## REPORTING ECONOMIC CRIME ONLINE (RECOL)

To make a fraud complaint

[www.recol.ca](http://www.recol.ca)

## EQUIFAX CANADA

Learn about your personal credit rating

[www.equifax.ca](http://www.equifax.ca)

1-800-465-7166