

2. BE VIGILANT

» Guard your computer and its information. Online chats, shopping and banking add a lot of convenience to our lives but, if you don't have appropriate security settings for your computer, your personal and financial information could be at risk.

» Only shop and bank online with trusted merchants. Make sure that the website is legitimate. Fraudsters can create a fake website ("brand spoofing") to trick consumers into revealing personal and financial information. Check that the URL is correct – including the domain.

Before giving your credit card number or other financial information to a business, make sure the merchant has a secure transaction system. Most Internet browsers indicate when you are using a secure Internet link. To check to see if a website is secure, look for a website address that starts with https://, a closed lock or an unbroken key icon at the bottom-right corner of the screen.

» Paying attention to financial details can help you watch for signs that you may be a victim of identity theft.

» Keep credit card, debit card and automatic banking machine (ABM)

transaction records so you can match them to your statements.

» Report any discrepancies on your statements to your financial institution right away, whether it is transactions that appear which you have not made, or transactions that you know you have made, but do not appear.

» Pay attention to credit card expiry dates. If your replacement hasn't arrived, call the company. Someone may have taken it from your mail or changed the mailing address.

» Once a year, or if you think your personal information has been stolen, get a copy of your credit report from each of the major credit reporting agencies. The tells you what information the bureau has about your credit history, financial information, judgments and any collection activity. It also shows who has asked for your information.

ARE YOU A VICTIM?

» Report the crime to the police immediately. Ask for a copy of the police report so that you can provide proof of the theft to the organizations that you will have to contact later.

» Cancel your credit cards and get new ones issued. Ask the creditors about accounts tampered with or opened fraudulently in your name.

» Have your credit report annotated to reflect the identity theft. Do a follow-up check three months after to ensure that someone has not tried to use your identity again.

» Close your bank accounts and open new ones. Insist on password-only access.

» Get new bank machine and telephone calling cards, with new passwords or PINs.

» Advise your telephone, cable and utilities that someone using your name could try to open new accounts fraudulently.

» Get a new driver's licence.

The message is clear: Do everything you can to avoid identity theft. And you certainly don't want to do anything to help someone steal your identity.



Vicky Tan is a Mortgage Agent with The Mortgage Providers. Visit her online at www.themortgageproviders.ca or e-mail your questions to vt@themortgageproviders.ca

Trust the Experts

Michael Volpentesta, AMP

Agent License # M08002906

Telephone: **416.398.1323**

E-mail Address: mv@themortgageproviders.ca



FSCO License #10533

The Mortgage™ PROVIDERS

The Mortgage Providers For Today's Personal & Business Needs

www.themortgageproviders.ca

3500 Dufferin St., Suite 205, Toronto, ON M3K 1N2

Tel: 416.398.1323 | Fax: 416.398.1324 | Toll-Free: 1.866.398.1323