IDENTITY THEFT

How Can You Reduce Your Exposure To Identity Theft?

- Guard your Social Insurance Number (SIN). Never put your SIN on checks, do not use your SIN or any part of it as a password at work or anywhere else, and only give it out when you believe it to be of absolute necessity.
- Create passwords and PINs that are difficult to guess for all accounts and change them periodically.
- Consider buying a shredder to adequately destroy personal financial documents that you are throwing out. So-called "dumpster diving" in your trash is a way for criminals to obtain information about you.
- Never give out any confidential information (account numbers, passwords) over the phone to an unsolicited caller who is stating that they represent your financial institution or similar creditor. This person could be anyone! Get their name, location and telephone number, and reason that they are calling. Call them back at the phone number printed on your billing statements.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances. Report and challenge any questionable charge regardless of dollar amount. A small charge could be a first warning sign of a larger problem.
- Go through your wallet or purse. If it were lost or stolen, how much information would a thief obtain? Do not carry your Social Insurance card, birth certificate or passport with you unless absolutely necessary. Do not carry extra credit cards either.
- If you are denied credit find out why. It could be due to errors on your credit report that you are unaware of.
- Be alert to red flags. If you ever receive a call from a merchant, creditor or collection agency in what seems to be a case of mistaken identity, be on alert. Find out exactly who they are and details of why they are calling you. This may be your first and only warning that you are a victim of identity fraud.
- Watch for people who try to eavesdrop and overhear the information you give out orally. Keep a watch out for people standing near you at retail stores, restaurants, grocery stores, etc., that have a cell phone in hand. With the new camera cell phones, they can take a picture of your credit card, which gives them your name, number, and expiration date.

Email and “Phishing” Identity Theft prevention tips:

Phishing is when criminals lure people to surprisingly realistic websites that they have created to trick people into disclosing their account numbers, passwords, social security numbers or other sensitive information. The thieves then use the information to pilfer bank accounts or go on a spending spree with stolen credit card numbers.

- Don't trust email headers, which can be forged easily.
- Avoid filling out forms in email messages. You can't know with certainty where the data will be sent and the information can make several stops on the way to the recipient.
- If you want to do business online, don't click on links in an unsolicited email. Go to the company's Web site yourself and fill out information there.
- Be wary of any email message asking you to verify or re-enter account information that you have already given to an organization you do business with. Do not provide

information that is supposed to be secret, like a PIN for an ATM card. Think twice before entering credit card numbers for offers that appear too good to be true, like merchandise with an unusually low price or a contest that requires you to pay a small handling fee to receive a prize.

- If there is any reason to doubt the authenticity of an email message from a company you do business with, do not click on any link or button in the message. Instead, type the Internet address of the company into your browser, log in as you usually do, and examine your account information.
- Look for the padlock icon on the bottom of the browser window that indicates that the site is using security features meant to protect confidential information. If a site is asking for personal information and is not using this security method, it is suspect. But the padlock, in itself, is no assurance a site is legitimate.
- Telephone a company to ask if an email is legitimate. Let any organization being impersonated know of the scam.
- If you have any reason to suspect that you have inadvertently provided information to a phisher, contact your bank and credit card companies immediately. Also, change any online passwords that you may have revealed to the phishers. If you provided information that could be used for identity theft – like a Social Insurance number – contact the two major credit bureaus to put a fraud warning on your credit file.
- If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you know to be genuine.
- Avoid emailing personal and financial information.

What Should You Do If Your Identity Is Stolen?

- Call both of the major credit bureaus and place a fraud alert on your name and Social Insurance number. An alert is a signal to any company looking to open a credit line that you are a victim and it must contact you before issuing any new credit.

Equifax can be reached at 1-800-465-7166
Trans Union can be reached at 1-866-525-0262

- While you are on the phone with the bureau, tell them you want a free report. Victims are allowed to obtain free copies of their credit reports.
- Cancel your credit cards and any false accounts you find on your credit report.
- File police reports. File one in your city or town and also file one in the cities or towns where your stolen identity was used. Get copies of the reports. You will need these to show creditors that you are a victim.
- After a month or two, order more copies of your credit report to verify that the companies removed the false entries and check to see that no new false accounts were opened (the reports should still be free).