How did I become a victim of identity theft?

- **Computer hacking**
- **Mail theft**
- **Inside theft**

We may never discover how this occurred but we will have a pretty good idea once the investigation starts. To give you a better understanding, lets identify the ways your personal information can be compromised.

Identity theft is when someone steals your personal information and uses it to commit fraud. They might access your bank accounts to steal money or open new accounts in your name. They might gain employment, buy a car, apply for a loan, all in your name; they are capable of using your identity in any way that they can for illegal financial gains. They might also use your identity to receive health insurance benefits, which could jeopardize your medical records. They will infiltrate anywhere personal information is stored.

The preferred ways of getting your information are:

Computer Hacking

Data stored on your computer or sent from your computer is vulnerable. Beware of potential viruses and put safeguards on your computer. Any entity you have done business with may have stored your personal information electronically, exposing you to the risk of a security breach.

Stolen Mail and Documents

Thieves love this, so shred, shred, shred. Any statement, report, bill, pre-approved credit card or document that divulges your personal information could be enough for an identity thief. They might go through your garbage, dumpsters or unlocked mailboxes to get it. Shred old credit cards, receipts, utility bills, bank statements and any information making you susceptible to fraud.

Stealing information from the inside

This involves accessing businesses that internally store personal data. Identity thieves infiltrate the workplace or imbed accomplices within a business with the sole purpose of stealing identities.

How did I become a victim of identity theft?

- **Imposters**
- **Medical ID Theft**
- **Financial ID Theft**

Imposters

Thieves will pose as loan officers, charity workers or any position that enables them to obtain vital information from you, either on the phone, by computer or in person.

They only need to steal a few pieces of your identity to create havoc with your credit, reputation and financial wellbeing. Thieves set up accounts with new addresses and the more they open successfully with the new address, the more they take control of your identity. They may also steal your identity with the view to getting medical attention and benefits in your name.

Financial identity theft

This variant occurs when a criminal steals your personal information, including any or all of the following: Social Security number; drivers license; passport; home address; mother's maiden name; bank PIN numbers; date of birth; credit cards (or credit card information); and/or personal phone numbers. Thieves use this information to either steal from your existing accounts or make purchases for themselves. They can create new accounts in your name that they control for fraudulent means. This may last for extended periods of time before you are aware to repair the damage. We will discuss preemptive ways of protecting yourself later.

Medical identity theft

This insidious form of fraud occurs when a criminal will steal your personal information and use it to obtain medical services. They will use your identity and insurance to seek medical attention, have expensive operations or, give birth — leaving the bill in your name. In doing so, they will have to changed your vital medical information (blood type, allergic reactions etc.) which can be potentially fatal to you. Always review your Explanation of Benefits (EOB) provided by your insurance company.

How did I become a victim of identity theft?

YOUR SSN IS PRECIOUS

Your Social Security number is precious. Protect it!

A Social Security number is the biggest prize to an identity thief. It unlocks bank accounts, credit cards and the rest of your fiscal being.

There are only limited circumstances justifying surrendering this information to someone; government tax agencies, banking and financial institutions would be appropriate examples.

Avoid giving your Social Security number on initial job applications, health provider offices (use the medical ID number off of your insurance card), or over the Internet.

Avoid carrying anything displaying your Social Security number. Most cards no longer detail SSN information to protect you and your identity.

How do I protect my family and myself?

- **Free credit Reports**
- **Your wallet**
- **Online shopping**
- **Protect your computer**

Take appropriate precautions

The federal FACT Act of 2003 entitles anyone to get a free credit report once a year from the three credit bureaus, which you should examine carefully for fraudulent activity.

To obtain your free annual credit report, either order online via www.annualcreditreport.com, or by telephone at (877) 322-8228.

For a copy of the mail-in form, go to: https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Avoid carrying personal information, if possible. Only carry the essential cards for everyday use. Wallets and pocket books are prime targets and their contents will make you vulnerable to identity theft if stolen. Do not leave in your vehicle and keep them safe at work and when travelling.

Keep your computer safe — we live in a world of viruses and hackers, so never open up unusual email from unknown sources. Install virus protection software, which will help protect from worms and viruses. Install a firewall to help stop hackers from stealing personal data. All stored data should be encrypted and password protected. When the time comes to dispose of your old computer, use software that securely wipes your hard drive, do not rely on the delete function to remove sensitive information.

When using the Internet for purchases be very conscious of the websites you are using. Be sure they are using secure data transmission and implement strong security and privacy policies.

How do I protect my family and myself?

- **Personal Mail**
- **Personal Documents**
- **Passwords**
- **Personal checks**

Take appropriate precautions

Keep your mail safe- many people now use commercial mail- boxes or P.O. mailboxes to safeguard their mail, on an everyday basis, even when away for extended periods of time.

Keep and store sensitive information securely, especially if you have roommates, employ outside help or you are having work done by outside contractors. Make copies of all accounts with expiration dates and customer service phone numbers and store securely, so you are ready for immediate action if the cards are lost or stolen.

Check all statements thoroughly for improper use, including Social Security, phone, bank accounts and credit card statements. Your Social Security statement is mailed about 3 months before the birthday.

Keep passwords and PINs safe — passwords to accounts should be alphanumeric (combination of letters and numbers). Thieves are looking for the easily guessed names and numbers. Children's, mother's maiden and pet names are predictable so avoid them. Easily guessed pass codes should be avoided, the last four digits of your Social Security number or birthdays, avoid using those. Create unusual passwords and keep a record of them in a safe place but never carry them with you. Set up additional passwords and security where allowed.

Keep your checks safe — mail payments inside post offices. Don't use drop boxes at work or your own mailbox for pick up. Stolen checks can be altered and cashed. Pick up your new checks from the bank, instead of having them mailed, and store-cancelled checks in a safe place.

How do I protect my family and myself?

Take appropriate precautions

Keep the number of credit cards to a minimum.

Cancelling credit cards can negatively affect credit scores, but keeping unused accounts gives another potential target to identity thieves. Track new or reissued cards that have been sent to you, contact the issuer if the card does not show up in two weeks.

- **Limit the number of credit cards you have**
- **Don't be careless**
- **Stop unsolicited marketing**

Don’t be careless.

Be mindful of where you keep your shopping receipts, although most receipts no longer have sensitive information on it. Be mindful of who is watching over your shoulder, when entering ATM codes. Never drop your guard even if nobody is standing behind you.

Stop unrequested marketing — there are many steps you can take to stop the annoying and unsafe marketing that you may encounter.

Call 1-888-5-optout to have the three credit bureaus remove your name from marketing lists permanently; this will limit the pre-approved credit offers you receive that can be used to obtain fraudulent credit cards in your name.

You can also visit www.donotcall.gov or call 888 -382-1222 and they will put your name on the National Do-Not-Call Registry. You can call your State office and add your name to the Do-Not-Call list, if they have one. Never allow any of your financial information to be shared with other financial institutions, credit card companies, insurance or investment firms.