Before you Sign

Fraud

Welcome to the Before You Sign podcast. This podcast was made to help you better know your legal rights in the province of Ontario. If you know your rights and responsibilities, you will be able to make choices that impact your life in Canada. It is important to know these podcasts are not legal advice for your situation, they give information about general legal topics that apply to your situation.

If you still have questions about this topic please consider going back to the service or agency who told you about these podcasts. If you have access to a computer, you can also go to stepstojustice.ca or settlement.org for more information. If you already know you need legal advice, support or representation please call Legal Aid Ontario at 1-800-668-8258 Monday to Friday from 8:00 a.m. to 5:00 p.m. (EST) for help in over 300 languages. This podcast is financially supported by The Law Foundation of Ontario, the YWCA St. Thomas-Elgin is solely responsible for the content.

Today we will be talking about fraud in Ontario. Fraud is when somebody does something knowing it is wrong or criminal. The criminal tries to trick another person into doing something that will result in financial or personal gain in some way for the criminal. This can happen in several different ways. In this podcast we will talk about identity theft and what to do if you become a victim.

Identity theft is the use of your information by another person, or group of people without your permission. It means the criminal has collected and used your personal information such as your name, date of birth, address, social insurance number, passport, banking information and other personal details for criminal purposes. A person, or group of people, may then use your personal information to pretend they are you and open a bank account, apply for loans or mortgages, obtain GST/HST rebates or refunds, benefit and credit payments, or income tax refunds, among many other things.

There are many ways for these dishonest people to gain access to your information. For instance, they could steal your purse or wallet. For this reason, you should consider limiting what you carry with you in your day to day life to just one piece of ID, like a driver's license for example. Items like your passport should be kept locked in a safe place and only carried when necessary. They could also go through your garbage. If you are not careful about how you get rid of your paper statements from your bank, credit card, and financial investments and just throw them out with your garbage, anybody could get your valuable information. If you are not careful when taking money out at the ATM somebody could be looking over your shoulder to see your your bank account PIN. You should always use your body and hand to cover up the PIN you are entering when doing banking at an ATM or paying for a purchase at a store. Data theft is when criminals steal your information from a computer or its network. This could happen from your private or work computer as well as the computer network of a business that you have dealt with. A very common form of fraud is called phishing, spelt P-H-I-S-H-I-N-G. The word phishing is used to describe fraud that is done using emails or phone calls and

pretending to be real companies in order to get you to share your personal information. They may send you an email message or call you on the phone claiming to be contacting you from what seems like a real business, such as a financial institution or government agency like the Immigration, Refugees Citizenship Canada or the Canada Revenue Agency. The email or phone call will say that there is a problem with the security for your bank account for example, or perhaps your immigration status is at risk at the IRCC, if you do not quickly reply confirming your personal information. It is important to know that no real business will ever request you share your personal information over email or the phone. If you receive an email that you are not sure about do not respond. Instead, look up the place of business or agency listed on the e-mail. Do not use the phone number or address listed in the email itself. Call, or visit in person, the place of business in question and explain what you have received. They can confirm for you if there are any real issues to be dealt with.

If despite your best effort's you do become a victim of identity theft, there are steps you need to take as soon as you become aware of it. Your first step is to call your local police. They will give you a police report number. Next, you should call your bank and credit card companies to tell them what has happened. Depending on how your identity has been used, it could affect your credit rating so you must also call Canada's two main credit reporting agencies. Equifax at **1-800-465-7166** and TransUnion at **1-800-663-9980** to ask them to put a "fraud alert" on your file. Phone Busters National Call Centre is run by the Royal Canadian Mounted Police and is responsible for tracking fraud trends and helps victims of fraud. You can contact them at **1-888-495-8501** for further support. If you suspect you may have been targeted by identity thieves, there are several important contacts to check. Sometimes the identity thieves might try to redirect your mail by changing your address with Canada Post so you should call them at 1-866-607-6301 to ensure nothing has been changed. Passport Canada can be reached at 1-800-567-6868. It is important to check with them and ensure that the criminals have not ordered a new passport in your name. Finally, you can call 1-800-622-6232 for information on where and how to replace identity cards such as your health card, driver's license or Social Insurance Number if necessary.

We hope you have found this podcast a good source of some basic legal information regarding what identity theft is, how to protect yourself and what to do if you do become a victim of it.