University of Victoria

January 2013

Identity Theft Protection Checklist

The following checklist provides a set of steps you can take to protect yourself from identity theft and fraud.
It is based on advice on best practices provided by knowledgeable sources in the fields of information security and fraud prevention.

Part 1: Protecting Yourself from Identity Theft

If you are concerned about possible theft of your personal information you may want to consider the following steps:

	Steps	Information at risk
☐	Contact your financial institution(s) to have your bank account monitored (ask your bank about available options).	Banking information
☐	Call Canada's two main credit bureau agencies: Equifax: 1-800-465-7166 and TransUnion: 1-800-663-9980. • Ask to see a copy of your credit file and check it for suspicious activity (free service). • Have an alert placed on your credit file (free government-mandated service both agencies must provide) so that creditors know that your account is at risk. This will encourage creditors to take additional steps to validate your identity prior to opening a new account under your name.	Credit information
☐	Contact the Canada Revenue Agency (CRA) at 1-800-959-8281. • Ask to put a password on your account. This password will need to be verified if anyone calls to inquire about your account, along with the standard security questions to protect personal information. • Additional option: You may also request that the CRA disable all online access to your account. Online access can later be restored at your request. To disable your online account, call the CRA e-Services Helpdesk at 1-800-714-7257. Note that this will not impact your ability to file your taxes online using NETFILE.	CRA tax account(s)

Part 2: Ongoing Monitoring

We recommend that you continue to be vigilant about your financial accounts into the future. The following steps are ongoing ways to keep an eye on any activity associated with your accounts:

	Steps
☐	Be aware of "phishing" which is a scam where somebody with limited information about you attempts to obtain additional information about you by claiming to be from a bank or credit card company requesting information such as passwords, credit card numbers, date of birth and answers to other personal questions including security questions. Banks and credit card companies will under no circumstances initiate a call and ask for such information.
☐	**Frequently monitor your financial accounts, including credit cards and bank accounts, to ensure that all debt and activities are authorized.** Signs of fraudulent activity include: • Your bank statements show withdrawals or other transactions you didn't make. • You are denied credit even though you believe you have a good credit record. • Your credit report shows debts that are not yours.
☐	Monitor your mail for any disruption in delivery (contact Canada Post if your mail is missing): • Follow up with creditors if your bills do not arrive on time; • Follow up with financial institutions if your bank statements do not arrive on time; • Signs of fraudulent activity include: a. You no longer receive credit card statements or you notice that not all of your mail is delivered; b. You receive credit card statements or other bills in your name, which you did not apply for; and/or, c. A collection agency informs you they are collecting for a defaulted account established with your identity and you never opened the account; or about a bill you have already paid.
☐	**Monitor your credit activity at both credit bureaus and other credit-related activities:** • Be aware of telephone calls or letters that state you have been approved or denied by a creditor to which you never applied. • Request a free credit report on an annual basis from Equifax and/or TransUnion: http://www.equifax.com/ecm/canada/EFXCreditReportRequestForm.pdf http://www.transunion.ca/ca/personal/creditreport/consumerdisclosure/mail_en.page
	For additional information regarding best practices for managing your personal information please see the federal/provincial/territorial government Consumer Measures Committee's information for consumers on identity theft. http://cmcweb.ic.gc.ca/eic/site/cmc-cmc.nsf/eng/fe00170.html

Part 3: Responding to Suspected Identity Theft

If you have reason to believe that your identity has been compromised (e.g., accounts have been opened in your name or transactions are occurring that you did not authorize) you should take the following steps immediately:

	Steps
☐	File a complaint with the police. Ask for the case reference number, and the officer's name and telephone number. If your social insurance number (SIN) may have been involved, be sure to notify the police.
☐	Contact the Canadian Anti-Fraud Centre at 1-888-495-8501. The national anti-fraud call centre is jointly managed by the Royal Canadian Mounted Police, Ontario Provincial Police and Competition Bureau Canada. They provide advice and assistance regarding identity theft.
☐	Inform your bank and creditors by phone and in writing about any irregularities. Contact the fraud department of creditors (e.g., credit card companies, phone companies, banks and other lenders) for any accounts that have been opened or tampered with fraudulently.
☐	Report any irregularities in your mail delivery to Canada Post, (e.g., opened envelopes, missing financial statements or documents).
☐	If your Social Insurance Number (SIN) may have been involved, visit a Service Canada Centre and bring all the necessary documents with you proving fraud or misuse of your SIN. Also bring an original identity document (your birth certificate, or immigration or citizenship document). An official will review this information and provide assistance and guidance. Service Canada issues new SINs only in certain situations, such as when you have been the victim of fraud. If you can prove that your SIN was used fraudulently, you can ask for a new SIN. You should also notify the Canada Revenue Agency at the number provided above. If your SIN is being used fraudulently, you should bring the following information to Service Canada to assist in remediating the situation: • A printout of all the employers who issued a T4 slip for your SIN over the past three years. This printout can be obtained from the Canada Revenue Agency at 1-800 959 8281. Check for any employers for whom you have not worked. Service Canada will contact them on your behalf. • A clear photograph of yourself for every employer for whom you did not work. Photographs make it easier for a Service Canada official to confirm with the employer(s) that you didn't work for them. • A list of every address where you lived over the last 10 years. In addition, you should gather any available proof that someone else was using your SIN, for instance: • A copy of the application for credit filled in by someone else who used your SIN on the credit application. This application must show both your name and your SIN. • A letter from a creditor confirming that someone else used your name and SIN to apply for credit. This letter must include both your name and SIN and state that you are not responsible for any purchases made fraudulently using your information. • Note: Service Canada cannot correct a credit file. It is up to you to contact your financial institution(s), report any discrepancies and have them resolved. If Service Canada issues you a new SIN, you will need to contact all your financial institutions, creditors, pension providers and employers (past and current) to ask them to update your files.

Note: Even if you complete all of the above activities, you may still be the subject of identity theft. The above activities can help to reduce the risk of this occurring and, if identity theft does occur, assist you in identifying and addressing it as quickly as possible.