## Preventative Actions You Can Take

- Promptly remove mail from your mailbox after delivery.
- Deposit outgoing mail in a post office collection box, not your own mailbox.
- Never give personal information over the telephone, such as your social security number, date of birth, credit card number or any other personal information unless you initiate the phone call.
- Shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want before discarding them in the trash or recycling bin.
- Empty your wallet of extra credit cards and IDs, or cancel the ones you do not use and maintain a list of the ones you do. Never leave receipts at the bank machines, bank counters, trash receptacles, or unattended gasoline pumps.
- Memorize your social security number and all of your passwords. Do not record them on any cards or on anything else that is in your wallet or purse. Do not carry your (or your children or spouse's) social security card with you—put them in a safe place.
- Never loan your credit cards to another person. Never put your credit card or any other financial account number on a postcard or on the outside of an envelope.
- Be conscious of the normal receipt of routine financial statements and bills. Contact the sender if they are not received in the mail.
- If you applied for a new credit card (or checks) and it has not arrived in a timely manner, call the bank or credit card company involved.
- Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.
- Never leave your purse or wallet in your car!

## Internet and On-Line Services

- Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any web site or on-line service location unless you receive a secured authentication key from your provider. A secure web site will have the following in the address lines: https:\\www.(name of site). The "s" denotes a secured site. There will also be a padlock on the tool bar. Only provide your information to a site you have looked up; not one that was sent to you via e-mail. You may want to telephone the company instead to place an order.
- When you subscribe to an on-line service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number used to subscribe. Don't give them out.
- Beware of e-mail from someone who purports to be your ISP (internet service provider), bank, or other business informing you that your service or account will be suspended if you do not update your records. They are seeking personal information such as your social security number, bank account number and/or credit card number. Leave the site without responding. Your bank or ISP does not do business this way. Do not click on the site provided in the e-mail—it is most likely a fraudulent site. If you are uncertain, telephone the business after you have looked up the number. There are lots of scammers out there who want to use your identity and your money.

**Walla Walla Police Department**
**15 N. 3rd Avenue**
**Walla Walla, WA 99362**
**(509) 527-4434**
**Fax: (509) 525-5057**

# IDENTITY THEFT

## Quick Reference Guide 2009

Walla Walla Police Department

***RCW 9.35.020**: No person may knowingly obtain, possess, use, or transfer a means of identification or financial information of another person, living or dead, with the intent to commit, or to aid or abet, any crime.*

CITY OF WALLA WALLA

## What is Identity Theft?

Identity theft involves acquiring key pieces of someone's identifying information, such as a name, address, date of birth, social security number, and mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud which include, but are not limited to, taking over the victim's financial accounts, opening new bank accounts, purchasing automobiles, applying for loans, credit cards, and social security benefits, renting apartments, and establishing services with utility and phone companies.

**What to do if you become a victim:**

1. **Credit Bureaus**. Immediately call the fraud units of one of the three credit reporting companies: Experian, Equifax, or TransUnion. Report the theft of your credit cards, social security number, or any other identifying information. Ask that your account be flagged. At this time, ask for a copy of your credit report—because you may be the victim of identity theft, this should be free. If someone has tried to or has opened accounts using your personal information, ask for the names and phone numbers of the companies.

**Equifax:** PO Box 74021, Atlanta, GA 30374, 1-800-525-6285

**Experian:** PO Box 949, Allen, TX 75013 1-888-397-3742

**TransUnion:** PO Box 390, Springfield, PA 19064; 1-800-680-7289

One company will notify the others of the identity theft in order to put a flag on your name.

You may also want to notify the Federal Trade Commission Identity Theft Hotline at 877-438-4338, or on line at www.ftc.gov to file an on-line complaint.

2. **Creditors**: Contact all creditors immediately with whom your name has been fraudulently used. Ask that any fraudulent accounts be frozen immediately. Request replacement credit cards with new account numbers for your own accounts that have been fraudulently used.

3. **Law Enforcement**: Report the crime to your local law enforcement agency. Give them as much documented evidence as possible as this will greatly assist law enforcement in investigating the case. Creditors and banks will usually not provide information to law enforcement without a subpoena so it will be up to you to obtain as much information as possible. Get a copy of your police report. Keep it handy and give it to creditors and others who require verification of your case.

4. **Stolen Checks**: If you have had checks or an ATM card stolen or bank accounts set up fraudulently, report it to your bank immediately. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and open new accounts. When activating a new ATM card, do not use your old PIN, or common numbers such as your date of birth or part of your social security number.

5.**Social Security Numbers**: Call the Social Security Administration (800-772-1213) to report fraudulent use of your SSN. You can order a copy of your earnings and benefits statement to check whether someone has used your SSN to get a job or avoid paying taxes. Never carry your social security card in your purse or wallet. If your purse or wallet is stolen or lost, it will provide the perfect opportunity for identity theft.

**6. Mail Fraud/Change of Address:** If you suspect that someone has filed a change of address in order to divert your mail, contact you local Postmaster for a copy of the change of address form.

**7. Collection Agencies:** You may at some point receive letters or phone calls from collection agencies demanding that you pay a bill. Do not ignore these collection letters or calls. Call the telephone number listed on the collection notice and also write a letter similar to the example below:

Date

Dear (Creditor/Collection Bureau)

On (date) I received your letter demanding payment of $(amount). I did not open this account nor did I incur this unpaid balance. Someone, other than myself, wrongfully used my personal information to obtain a line of credit/service. Your company extended a line of credit/services to someone other than myself.

You are hereby notified that on (date) I filed an identity theft report with the Walla Walla Police Department. The incident report number is _____ _____, a copy of which is enclosed.

(Your name, address, and telephone number.)

It is imperative that you call and write a letter to the creditor or collection bureau. The police department cannot do this for you. Try to get as much information from the creditor/collection agency as possible, such as when the account was opened, what address was used, etc.