

## **IDENTITY THEFT**

### **What is identity theft**

Identity theft happens when a criminal obtains data that personally identifies you and then uses that for an illegal purpose – typically theft. The thief takes advantage of your good credit rating, and leaves behind bad credit in your name. Losses to consumers and businesses due to identity theft are enormous. Identity theft is now a Felony under Washington State Law (RCW 9.35.020).

### **The identity thief gets your information by:**

- Stealing your purse or wallet. They are frequently stolen from shopping carts in supermarkets.
- Stealing mail from your mailbox to obtain newly issued credit cards, bank and credit card statements, pre-approved credit card offers, or tax information.
- Accessing your credit report fraudulently by posing as an employer, loan officer, or landlord and ordering a copy.
- Dumpster diving in trash containers for discarded credit card receipts and loan applications.

### **How identity thieves use this information:**

- They open a new credit card account, using your name, date of birth, and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- They call your credit card issuer and pretending to be you, change the mailing address on your credit card account. Then, your imposter runs up charges on your account. Because your bills are being sent to the new address, you may not immediately realize there's a problem.
- They establish cellular phone service in your name.
- They open a bank account in your name and write bad checks on that account.

### **How to protect yourself:**

- Reduce the number of cards you carry. Don't carry your social security card, birth certificate or passport, except when needed.

- Shred, tear, or cut up papers with personal information, i.e.: charge receipts, bank statements, expired credit cards, and credit offers.
- Do not give out personal information over the phone unless you have placed the call and know the business. Even then find out how the information will be used and if it will be shared. Ask if you have a choice about the use of your information.
- Get a copy of your credit report at least once a year to check for errors. Follow up if problems are found. You can now get a free copy of your credit report once a year from all three credit reporting bureaus by connecting with [www.annualcreditreport.com](http://www.annualcreditreport.com)
- Carefully review your credit bills for any unauthorized charges.
- Password protect your accounts with something other than your mother's maiden name!
- Pay attention to your billing cycles. Follow up with creditors if bills do not arrive on time.
- Give your social security number only when absolutely necessary. Ask to use other types of identifiers when possible
- Guard your mail from theft. Deposit outgoing mail at the post office. Remove mail from your mailbox as soon as possible. Consider a locking mailbox; use a post office box for incoming mail.

### **What to do if you are a victim**

- Contact the fraud departments of each of the three major credit bureaus. Ask that a fraud alert be placed on your file; add a victim's statement to your report. ("My ID has been used to apply for credit fraudulently. Contact me at [at your phone number] to verify all applications.") Ask how long the fraud alert is posted on your file, and how you can extend if necessary.

Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Request a free copy of your credit report every few months so you can monitor any new fraudulent activity. Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers)

- Contact all creditors immediately with whom your name has been used fraudulently, by phone and in writing. (Creditors and include credit card companies, phone companies, and other utilities) You may be asked to fill out fraud affidavits. (New law requires these to be notarized at your own expense.) Ask that your account be password protected with something other than your mother's maiden name and social security number. Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request" (better than "card lost or stolen," because it can be interpreted as blaming you for the loss.)
- File a report with your local police or the police in the community where the identity theft took place. Give them as much documented evidence as possible. Make sure the police report lists the fraud accounts. Obtain a copy of all police reports, keep the phone number of your investigator handy and give to creditors and others who require verification of your case. It is a violation of federal law (18 USC 1028) and the laws of many states to assume someone's identity for fraudulent purposes.
- If you have had checks stolen or bank accounts set up fraudulently, report it to the appropriate check verification companies. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account. If your own checks are rejected at stores where you shop, contact the check verification company the merchant uses.
- If your ATM or debit card has been stolen or compromises, report it immediately. Get a new card, account number and password. Do not use your old password. When creating a password, don't use common numbers like the last four digits of your SSN or your birth date. Monitor your account statement. You may be liable if fraud is not reported quickly.

Further information may be obtained by linking to the following sites.

Federal Trade Commission identity theft [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/)

Washington State Attorney General [www.atg.wa.gov/](http://www.atg.wa.gov/)

U.S. Department of Justice [www.usdoj.gov/](http://www.usdoj.gov/)

Privacy Rights Clearinghouse [www.privacyrights.org](http://www.privacyrights.org)

