

## What is personal information?

Any combination of the following information can be enough for identity theft to occur:

- Name
- Address
- Phone Number
- Email Address
- ATM Pin
- Date of Birth
- Social Security Number
- Mother's Maiden Name
- Financial Account Numbers

## The basics of safeguarding your information

### • Guard your social security number

Do not carry your Social Security card with you and do not ever use your social security number as a PIN or password. Limit the number of identification cards you carry. Many medical cards contain your Social Security number. Do not carry it with you if you do not need it.

### • Shred, shred, shred

Shred bills, bank statements, receipts, medical billings, credit card offers, and any other items that contain personal or financial information.

### • Protect your mail

If you are going to be out of town have the post office hold your mail. Place outgoing mail in an official mailbox not your own.

### • Never give out your personal information

Legitimate companies or agencies do not call or email asking for personal information. Never give out personal information unless you initiated the contact.

### • Sign up for the Do Not Call Registry

Register your home and mobile residential numbers on the Wisconsin Do Not Call Registry at no cost by visiting [www.donotcall.gov](http://www.donotcall.gov) or by calling 1-888-382-1222; you must call from the phone number you wish to register.

### • Keep a list of all financial accounts

Keep a list of all credit card and bank account numbers, phone numbers, and expiration dates. This information as well as other sensitive documents should be kept in a safe place, such as a safe.

### • Stop pre-approved credit card offers

Stop pre-approved credit card offers by calling 1-888-567-8688 or visiting the Opt Out website at [www.optoutprescreen.com](http://www.optoutprescreen.com)

### • Check your bills and bank statements

Look at your statements as soon as you get them to see if there are any unauthorized charges or inaccuracies. If there are, report them right away.

### • Pay attention to internet security

Make certain you have a firewall and updated virus and spyware protection on your computer. Check your browser security settings to make certain that they are not too low.

### • Use two-factor authentication if offered

Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.

### • Check your credit report regularly

Obtain your credit report FREE from each of the three major credit reporting agencies each year. You can get your free credit report from Equifax, Experian, and TransUnion by calling 1-877-322-8228 or online at [www.annualcreditreport.com](http://www.annualcreditreport.com)

## What to do if it happens to you

### • Contact your bank

Let your bank know that your identity has been stolen even if the thief has not used your bank accounts or ATM/debit card. Consider closing and reopening new accounts with new numbers

and obtaining a new ATM/debit card with a new PIN. In addition, you may want to ask your bank if you can place a password on your accounts.

### • Contact your creditors

If an identity thief has opened a new account or credit card in your name contact the creditor to close the account and explain what happened as soon as possible.

### • Report the theft to the police

Your local police department is required to prepare a report of identity theft even if the theft might have occurred at some other place. Be sure to obtain a copy of the report for yourself. It can be a vital tool to working through recovering from the identity theft.

### • Put a Fraud Alert on your credit report

A fraud alert is a notation that requires a business to take extra reasonable steps to verify a person's identity before issuing a line of credit or offering services. The fraud alert will be active for 90 days and can be renewed. You only need to contact one of the three agencies below and they will notify the other two on your behalf.

### • Put a Security Freeze on your credit report

A freeze is stronger than a fraud alert because it remains in place until you release it and requires that you be alerted if an account in your name is requested. The freeze must be requested by contacting each of the three credit reporting agencies directly. Unless a police report is provided, the fee is \$10 for each agency. You will be given a pin number to temporarily lift the freeze in order for you or a creditor to access your credit report. There may be a \$10 fee each time you need to lift the freeze.

#### Experian

PO Box 9701  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

#### Equifax

PO Box 105069  
Atlanta, GA 30348  
1-800-349-9960  
[www.equifax.com](http://www.equifax.com)

