

# To You.



- 5. File a police report.** Without one, many companies will refuse to take your case seriously. Some companies may also require you to file the identity theft affidavit available at [www.UnionPlus.org/IDTheft](http://www.UnionPlus.org/IDTheft).
- 6. Start a file.** Keep notes of every phone conversation, piece of correspondence and copies of your credit reports. Write down each person's name, title, and phone number in case you need to re-contact them or refer to them in future correspondence.
- 7. Close compromised accounts and dispute fraudulent charges in writing.** Keep in mind that closing accounts may hurt your credit score, however, so you may want to close only those accounts that have been involved in the theft.
- 8. Review your credit reports.** When you place an extended fraud alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. You may also want to subscribe to a credit monitoring service so you'll be notified quickly of any new activity.
- 9. Get help.** Check with your insurance companies and employer to learn whether your benefits include identity theft resolution services or expense reimbursement.



## *Union Plus cares about helping you build and keep good credit*

**These exclusive union member resources can help!**

**Identity Theft Prevention and Resolution**  
[www.UnionPlus.org/IDTheft](http://www.UnionPlus.org/IDTheft)

**Credit Reports and Scores**  
[www.UnionPlus.org/CreditScore](http://www.UnionPlus.org/CreditScore)

**Credit Counseling:**  
[www.UnionPlus.org/CreditCounseling](http://www.UnionPlus.org/CreditCounseling)

**Credit Management:**  
[www.UnionDebtHelp.org](http://www.UnionDebtHelp.org)

**Homeowner Help**  
[www.UnionPlus.org/SaveMyHome](http://www.UnionPlus.org/SaveMyHome)  
1-866-490-5361, 24 hours a day

**Credit Bureau Contact Information:**  
Equifax: 1-800-525-6285  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742)  
[www.experian.com](http://www.experian.com)  
P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289  
[www.transunion.com](http://www.transunion.com)  
Fraud Victim Assistance Division,  
P.O. Box 6790, Fullerton, CA 92834-6790



**Union Privilege**  
1125 15th Street, NW  
Suite 300  
Washington, DC 20005  
[www.UnionPlus.org](http://www.UnionPlus.org)

(O)C-BR 0708



## Your identity is one of your most important assets.

# Protect it!



# If It Happens

## *If you think or know your personal information has been misused, act quickly.*

- 1. Monitor your financial accounts closely.** Most credit card companies, credit unions and banks allow you to monitor your accounts online. You can often set up e-mail or cell phone alerts to notify you in case of unusual activity.
- 2. Report fraudulent charges immediately.** Even small charges can indicate big problems. Crooks often make small charges to check if a credit card is valid, or make purchases of less than \$100 each on many different credit and debit cards to avoid attracting attention.
- 3. Place a fraud alert or credit freeze on your credit reports.** If you notice fraudulent activity, contact one of the three major credit bureaus to place a fraud alert or credit freeze on your credit reports; whichever one you contact is required to contact the others on your behalf. With a fraud alert, businesses will be able to review your credit report, but will be alerted to verify your identity before issuing you credit. With a credit freeze, businesses will not be able to access your credit file unless you provide a PIN number.
- 4. Know your rights under the Fair Credit Billing Act for credit card loss or fraudulent charges.** Your maximum liability for unauthorized use of your credit card is \$50. If the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use.

To learn more, visit  
[www.UnionPlus.org/IDTheft](http://www.UnionPlus.org/IDTheft)

# Identity Theft

*Identity theft can happen to anyone, even those who don't use credit often. According to the Federal Trade Commission, some of the most common ways personal information is stolen include:*

- **Dumpster Diving:** ID thieves love trash when it contains billing statements or other items with personal information.
- **Skimming:** While you are making a purchase, the thief uses a special storage device to capture your credit/debit card number to use later.
- **Phishing:** Fake copies of legitimate websites and e-mails warning you to “verify your account” can be so convincing that you reveal your personal information.
- **Outright theft:** Many cases begin with a stolen wallet or purse, as well as bills, tax documents, credit cards or new checks plucked from mailboxes.
- **Insider jobs:** Employees steal customer files, sometimes after being bribed by ID thieves.
- **Pretexting:** There are two variations on this scam. Thieves may call you pretending to work for your credit card company or a business, and trick you into revealing personal details. Or, they may pretend to be you in order to convince employees at your utility providers, financial institutions etc. into sharing your information with them.



## Take These Steps to Help Protect Yourself

### Secure Your Personal Information

- Use a cross cut shredder to turn documents containing personal and financial information into confetti.
- Lock up your wallet or purse at work, and never leave it in your vehicle.
- Avoid giving out any personal information over the phone unless you initiated the call, even if the person calling seems to have detailed information about your accounts.
- Don't carry identification that includes your Social Security number (SSN). If a business requests your SSN, question whether it is really necessary. If they insist, ask if you can provide only part of the number, such as the last four digits.
- Don't print your driver's license number, phone number or SSN on your checks.
- Read privacy notices from your financial institutions for instructions on how to say “no” to information sharing.



### Secure Your Mail

- Install a locked mailbox or use a post office box to receive your mail, especially if it arrives while you are not home.
- Stop paper bills. Receive and pay your bills online instead.
- Place outgoing mail in an official US Postal Service mailbox. These mailboxes are locked and tend to be more tamper proof than your personal mailbox.

### Secure Your Computer

- Use only a secure Internet connection to access websites where you store or provide any personal information, whether at home or on the road. Look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a web site that begins with “https” (the “s” stands for secure).
- Install and run anti-virus and anti-spyware programs, and use a firewall. Keep them up-to-date.
- Install the latest security patches for your computer. Your operating system may offer free software patches to close holes in the system that thieves could exploit.
- Create difficult passwords that include a combination of letters, numbers and special characters – not your name, address, birth date, or anything that would be easily guessed.
- Don't store passwords on your computer or write them down where others may easily find them. Keep them somewhere secure – hide them in a locked drawer, for example.
- Never respond to e-mails requesting personal information, or click on links to popular websites asking you to verify your information. Type in the correct web address and go directly to those sites to log in instead.

### Secure Your Credit

- Review your credit reports for free once a year at AnnualCreditReport.com or by calling 1-877-322-8228.
- Consider using a credit monitoring service to notify you of changes to your credit information.
- Monitor your financial accounts online and set up e-mail or cell phone alerts for unusual activity.

*For resources to help detect, prevent and resolve identity theft, visit*  
**[www.UnionPlus.org/IDtheft](http://www.UnionPlus.org/IDtheft)**

## Identity Fraud Tip-Offs

*ID thieves are sneaky. What may seem like an innocent mix-up could be a clue that your personal information has been compromised. Clues to watch out for:*

- Your credit report lists aliases (variations on the spelling of your name), addresses at which you have never lived, accounts you have never held, and/or inquiries from companies to which you have not applied for credit, insurance or a job.
- You don't receive your credit card or bank account statement. A thief may have changed your address in order to use your bank accounts without raising suspicion.
- You receive bills for accounts you didn't open, such as a cell phone or credit card.
- You receive medical bills or health insurance benefit statements for medical procedures you've never had.
- A debt collector calls about a bill that doesn't belong to you.
- Your annual Social Security statement lists income you didn't earn.
- Someone calls to “confirm” information about one of your accounts or warn you about fraud, and asks for personal information or account details, such as your Personal Identification Number (PIN) or the three-digit security code on the back of your credit card.