

# Protecting Your Identity

## Tips For Avoiding Identity Theft



Identity theft occurs when someone uses your name and personal information, such as a Social Security Number or credit cards numbers, for fraudulent purposes. It is a serious crime that can take months, even years, to resolve. You can protect yourself from identity theft by following these tips, watching for warnings signs and knowing what to do if your personal identity has been compromised.

### What's in Your Wallet?

- Do not carry your Social Security Card, passport or birth certificate in your wallet or bag.
- Remove your SSN, middle name and telephone number from voter registration records.

### Reduce Access to Your Personal Information

- Do not have personal checks pre-printed with your Social Security Number.
- Do not have personal checks sent to your home mailbox. Pick them up at the bank or a locked mailbox.
- Request a vacation hold on your mail if you won't be home for several days.
- Mail bills or other sensitive items at the post office rather than from your residence or local drop box.
- Remove your name from the marketing lists of the three credit reporting bureaus at [www.optoutprescreen.com](http://www.optoutprescreen.com).
- Put your number on the National Do Not Call Registry at [www.DoNotCall.gov](http://www.DoNotCall.gov).

### Credit Card Safety

- Cancel all unused credit cards since the account numbers are recorded in your credit report and could be used by thieves.
- Keep a list or photocopy of all credit cards, account numbers, expiration dates and telephone numbers of the customer service and fraud departments in the event your cards have been lost or stolen. Do the same with your bank accounts.
- Never give out your personal information over the phone unless you initiated the call and you have a trusted business relationship with the company.
- Never toss ATM receipts in public trash containers.
- Request in writing that the issuer of each of your credit cards remove your name from their marketing and promotional lists which they may sell to other companies.

### Personal Identification Numbers (PINs) and Passwords

- Memorize all passwords. Don't record them on anything in your wallet or handbag.
- Shield your hand when using your PIN at ATM machines or when making calling card phone calls.

### Safeguard Your Personal and Financial Information

- Always shred bills and other statements before throwing them away.
- Find out how the companies that you work with dispose of information. If you are not convinced that personal information contained on applications and forms are stored in locked files or shredded, take your business elsewhere.
- Carefully review your credit card and phone bills for unauthorized charges.

### Check Your Credit Report Annually

Order a free copy of your credit report once a year from each of the three national credit bureaus at [www.annualcreditreport.com](http://www.annualcreditreport.com). The three national credit bureaus are listed below.

**Equifax:**  
P.O. Box 740241  
Atlanta, GA 30374-0241  
800-685-1111  
[www.equifax.com](http://www.equifax.com)

**Trans Union:**  
P.O. Box 2000  
Chester, PA 19022-2000  
800-888-4213  
[www.transunion.com](http://www.transunion.com)

**Experian:**  
P.O. Box 2104  
Allen, TX 75013-2104  
888-397-3742  
[www.experian.com](http://www.experian.com)

**Stagger your requests for each of the free credit reports throughout the year so you will be informed about your current credit status all year long.**

## Iowa College Student Aid Commission

430 E. Grand Fl 3 • Des Moines IA 50309-1920

Phone: 877-272-4456 • Fax: 515-725-3401

Email: [info@iowacollegeaid.gov](mailto:info@iowacollegeaid.gov) • Website: [www.iowacollegeaid.gov](http://www.iowacollegeaid.gov)

## Secure Information Online

Be alert to impersonators. Don't give out personal information on the phone, through the mail or over the Internet unless you initiated the contact. Double check all websites to make sure the URL matches up exactly to avoid phishing scams.

## Encrypt Your Data

Keep your browser safe. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted.

## Safely Dispose of Personal Information

Use a wipe utility program to overwrite a computer's hard drive before disposing of it. Remove the memory in subscriber identity module (SIM) card before disposing of a mobile device. Also remove the phone book, list of calls, voicemail messages, web search history, apps with personal information and photos.

## Don't Overshare on Social Networking Sites

Limit what you post. An identity thief can find information about your life, use it to answer "challenge" questions in your accounts and gain access to your money and personal information.

## Watch for Warning Signs

Even after taking precautions, you need to watch for signs that indicate your personal information is being misused.

- You stop receiving certain bills or other statements in the mail.
- You receive credit cards that you didn't request.
- You are denied credit for no apparent reason.
- You get calls or letters about merchandise that you didn't purchase.
- You are notified that more than one tax return was filed in your name.
- You get notice that your information was compromised by a data breach at a company where you do business.

## Steps to Repair Identity Theft

If you think your identity has been stolen, follow these steps recommended by the FTC:

1. Contact the fraud departments of the three national credit bureaus and place a fraud alert on your credit report. It will last for 90 days and can be renewed.
2. You will be entitled to one free credit report from each of the three consumer reporting companies.
3. Close all of your accounts and credit cards that you believe have been misused. Talk to someone in the fraud department and follow up in writing.

## Steps *continued*

4. Submit a report to the FTC at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) and print a copy of the Identity Theft Affidavit. Save the complaint reference number that appears after you submit your information.
5. Forward a copy of the ID Theft Affidavit form and any supporting documentation you have to each company.
6. File a report with all police and sheriff's departments with jurisdiction in your area. Bring a copy of your FTC Identity Theft Affidavit.
7. Notify the U.S. Postal Inspector's Office in your state if you suspect that an identity thief has filed a change of address or has used the mail to commit bank fraud.
8. Check your social security statement with Social Security Administration to determine if your SSN is being misused for employment purposes. Create an online account at [www.ssa.gov/mystatement/](http://www.ssa.gov/mystatement/) to view your information at any time.
9. Contact the lender, or in the case of a defaulted loan, the Iowa College Student Aid Commission, if a federal student loan was falsely borrowed in your name.

## Resources

Contact the following resources for more information:

Iowa Attorney General Tom Miller  
Consumer Protection Division  
1305 East Walnut Street  
Des Moines, IA 50319  
Phone: 515-281-5926  
Website: [www.state.ia.us/government/ag/consumer\\_brochures/Identity\\_Theft.html](http://www.state.ia.us/government/ag/consumer_brochures/Identity_Theft.html)

Federal Trade Commission  
Identity Theft Clearinghouse  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
Phone: 877-IDTHEFT (438-4338)  
Website: [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

Social Security Administration  
Office of the Inspector General  
210 Walnut Street  
Des Moines, IA 50309  
Phone: 515-284-4345 or 800-772-1213  
Website: [www.ssa.gov](http://www.ssa.gov)

Credit Bureau Consumer Fraud Departments

**Equifax:**  
P.O. Box 740241  
Atlanta, GA 30374-0241  
800-525-6285

**TransUnion:**  
Fraud Victim Assistance  
P.O. Box 6790  
Fullerton, CA 92834-6790  
800-680-7289

**Experian:**  
P.O. Box 9554  
Allen, TX 75013  
888-397-374

