

# Identity Theft

You're probably heard about it in the news.

It may even have happened to someone you know.

The FBI calls identity theft one of the fastest growing crimes in the United States and estimates that 500,000 to 700,000 Americans become identity theft victims each year.

Identity theft is a federal crime. It occurs when one person's identification (which can include name, social security number, or any account number) is used or transferred by another person for unlawful activities.

**This information will help you understand what identity theft is, how it happens, how to protect yourself, and what steps to take if your identity is stolen.**

## How Identity Theft Can Affect You

The consequences of identity theft can be staggering. Victims spend extensive time closing bad accounts, opening new ones, and fixing credit records. There can be high out-of-pocket expenses related to clearing your name. You could be denied loans and jobs - and, though unlikely, you could even be mistakenly arrested as a result of crimes committed in your name.

### What Identity Thieves Do with Your Information

Identity thieves frequently open new accounts in your name. They often apply for new credit cards using your information, make charges, and leave the bills unpaid. It is also common for them to set up telephone or utility service in your name and not pay for it. Some victims have found that identity thieves applied for loans, apartments, and mortgages. Thieves have also been known to print counterfeit checks in a victim's name.

Thieves also often access your existing accounts. They may take money from your bank accounts, make charges on your credit cards, and use your checks and credit to make down payments for cars, furniture, and other expensive items. They may even file for government benefits including unemployment insurance and tax refunds.

Unfortunately, thieves often use a stolen identity again and again. It is very common for victims to learn that thieves have opened and accessed numerous accounts, often over a long span of time.

## How Identity Theft Happens

Four out of five victims have no idea how an identity thief obtained their personal information. Among those who think they know what happened, many believe the identity theft occurred when their purse or wallet was stolen or lost. Thieves also steal identities from the trash - this is called "dumpster diving" - and it can occur at home, at work, or at a business. Mail can be stolen from your home mailbox, from a drop-box, at businesses, and even directly from postal workers. Home computers can be infected with viruses that transmit your data to thieves.

Group identity theft has become a major problem for consumers. A thief gains access to a place that keeps records for many people. Targets have included stores, fitness centers, car dealers, schools, hospitals, and even credit bureaus. Thieves may either use the stolen identities themselves or sell them to other criminals.

"Pretexting" is a method of identity theft that is on the rise. The identity thief poses as a legitimate representative of a survey firm, bank, Internet service provider, employer, landlord, or even a government agency. The thief contacts you through the mail, telephone, or e-mail, and attempts to get you to reveal your information, usually by asking you to "verify" some data.

Victims of identity theft often find that someone they know has committed the crime. Roommates, hired help, and landlords all have access to your home, and it is possible for them to access private information. Identity theft within families is also fairly common. This causes particular difficulties, because victims may be reluctant to notify the authorities or press charges. People are especially vulnerable when ending relationships with roommates and spouses.

Identity theft often goes undetected. Within a month of being committed, half of the crimes still remain unnoticed. One in ten stays hidden for two or more years. Identity thieves may change "your" address on an account so that you won't ever receive the bills with the fraudulent charges on them. They will often pay the minimum balances on accounts they have opened, so as to avoid calling attention to the account and having it cut off. They may even use the identities of children or persons who are deceased, so that the crime is less likely to be noticed.

## **Steps to Prevent Fraud**

Think about taking care of your identity on a regular basis just like you take care of your health. Some activities you do every day, like brushing your teeth and taking vitamins. Other actions should be taken once or twice a year, like getting dental check-ups and an annual physical.

### **Change Your Daily Routine**

#### **At Home**

In the home, keep personal information safe, especially if you have roommates or are having any work done in your home. Don't keep Personal Identification Numbers (PINs) near your checkbook, ATM card, or debit card.

Shred any papers with confidential information before you throw them out - even the junk mail. Anything with an account number can be used in identity theft. This includes prescreened credit card offers, receipts, canceled checks, bank statements, expired charge cards, doctors' bills, and insurance documents.

Since many identity thefts are traced to having a purse or wallet stolen, carry as few cards with identification and personal information as possible. Don't take your social security number, and bring as few credit cards as you can. Think about putting different cards in different parts of your purse or knapsack.

You should be wary of any mail, telephone, or Internet request for information - it could be "pretexting." Unless you initiated the contact with a business, don't give out any confidential information - such as your credit card number, social security number, PIN, birth date, or even your mother's maiden name. Also be careful of unexpected e-mails that look as if they are from a legitimate company asking you to enter some information at a linked web site; sometimes phony web sites can look real. Make sure your family members also know not to give out any information to others.

Check your banking and credit statements soon after you receive them and make sure there is no unexplained activity. Keep track of when in the month each of your bills usually arrives. If a bill does not arrive on time, call the company to make sure no changes have been made to your account. Often, identity thieves will change the address of a bill so that it will take you longer to figure out the scam. If you're careful, you may notice the theft earlier.

#### **Out of the Home - Shopping and Services**

When you sign a credit card slip, avoid putting your address, telephone number, or driver's license number on it. Also, be sure to take your receipts with you to shred at home because "dumpster diving" is very common at large retail areas, such as malls. This will help to minimize how much personal information about you is floating around out there.

Be particularly wary of giving out your social security number. Few institutions - businesses granting you credit, employers filling out tax forms for you, or government agencies - have any reasonable

cause to know your social security number. However, a business may refuse to serve you if you do not give them the information they request. It is up to you if you still want to do business with the establishment.

## Get Your Check-ups

### Your Credit Report

Many people don't realize they are victims of identity theft until long after the initial crime occurred. Identity thieves often try to hide the crimes for as long as possible so that they can access more money. To stop the crimes as soon as possible, make sure you carefully check your credit reports regularly. Your credit reports are important tools for limiting the amount of damage a thief can cause.

Contact each of the three major credit [reporting agencies](#) to order a copy of your credit report at least once each year. Your credit report will generally contain information on where you work and live, the credit accounts that have been opened in your name, if you own a home, if there are any liens against your home, how you pay your bills, and whether you've been sued, arrested, or have filed for bankruptcy.

Consider canceling credit cards you haven't used in a long time. You can also consider adding a "fraud alert" to make it harder for thieves to open new accounts without your knowledge. With a fraud alert, the credit agency has to call you to confirm any request it receives to open a new account in your name. If you decide you want this service, just contact the credit reporting agencies.

#### How to Read Your Credit Report

1. Check to make sure you are aware of all accounts listed, and balances are what you expect them to be.
2. Look for anything suspicious in the section that lists who has received a copy of your credit history. Some identity thieves "pretext" by posing as a landlord or employer.
3. Make sure no inquiries have been made about loans or leases you didn't apply for.
4. Check for addresses where you have never lived.
5. Check for typos in your social security number.
6. If there is any incorrect information in the records, contact the credit bureau, creditor, employer, or government agency immediately. Follow up with a letter describing what actions were taken. Your protections are usually stronger if you report the problem quickly and in writing.

### At Work

The newest trend in identity theft is to hit groups of people, and workplaces can be vulnerable. Find out if your company has a policy about protecting its employees from identity theft. Make sure your employer stores your personal information in a safe place. Also, find out which other employees have access to your personal information.

### Companies and Agencies with Which You Do Business

Identity theft can occur through records maintained by your bank, credit card companies, the Department of Motor Vehicles, utilities, insurance companies, and phone companies. Try to have as little information as possible printed on any cards these groups may issue. If you want, ask these companies about their policies with regard to sharing your information. You can stop many components of information sharing.

When choosing a PIN, use one that is hard to guess. Avoid the last 4 digits of your social security number, your mother's maiden name, birth dates, names of pets, or even the name of your hometown baseball team. Try to mix numbers, letters and symbols.

Make it harder for thieves to use your accounts. Put passwords on credit card, bank, and phone accounts. Get credit cards with your picture on them. Call the companies that issue the accounts and find out what security options they offer.

Don't print your social security number or phone number on your checks. Don't have your checks delivered to your home - go and pick them up yourself at your bank.

**Try not to use your social security number for an identifier:**

- Check your drivers license to make sure you aren't using your social security number as identification - few states require this any more.
- If a school, employer, health insurer, or other institution needs to give you an identification number, often they simply use your social security number. Find out if they can use another number instead.
- The only places you must use your social security number are on government and financial forms, such as tax forms and most credit applications.

**Your Mail**

Reduce the circulation of your information through the mail. Stop receiving prescreened credit offers by calling **1-888-5OPTOUT**. You can also reduce direct mail marketing and telemarketing by contacting the Direct Marketing Association. Notify each of the three major credit bureaus that you do not want personal information about you shared for promotional purposes. (This will also reduce unsolicited mail.) Consider putting a lock on your mailbox.

**Identity Theft Insurance**

Home insurance policies can include "identity theft insurance" as an option. But know that if you are a victim, insured or not, you should be able to get out of paying all fraudulent bills.

**What to Do If You're a Victim of Identity Theft**

There are several steps you can and should take to protect yourself if you are a victim of identity theft.

**Make Sure to Document Your Actions**

Begin documenting the time and money you spend on straightening out identity theft. In some states, any person found guilty of financial identity theft will be ordered to pay restitution to the victim for any financial loss, including lost wages.

- Keep copies of correspondence and documents related to the theft.
- Write records of all telephone calls, including the date and time of your call and the name and title of the person who assisted you.
- Write letters to confirm all phone conversations. Include the date, the name of the person you spoke with, and what actions were taken.
- To be extra careful, send documents and letters Return Receipt Requested and keep the postal receipt with your copy.

Consider using the ID Theft Affidavit to avoid having to complete different forms. This form can assist you in disputing inaccurate information that appears on your credit report as a result of fraud. It's available on [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). Keep copies of all affidavits that you send.

### **Contact the Police**

Immediately call the police to file a report with your local law enforcement. If your identity was stolen when you were away from home, you may need to contact the police in that jurisdiction, too. Opening a police case accomplishes two things: First, the police can start investigating the crime. Second, you will need information from the police report to help you straighten out your credit and accounts after the crime. When you talk to the police, make sure you get the police report number and information on how to reach the investigator. Give this information to all the companies you contact in getting your credit cleared up after the crime.

### **Stop the Damage**

After you call the police, contact the credit bureaus. Next, contact any credit card companies and banks where your accounts may be at risk.

### **Credit Bureaus**

Contact the fraud departments at each of the three credit bureaus.

**Equifax:** (800) 525-6285  
**Experian:** (888) EXPERIAN (397-3742)  
**TransUnion:** (800) 680-7289

- Get all three agencies to flag the accounts with a "fraud alert." Find out from each credit reporting agency how long the fraud alert will remain on your report, and how to extend that time, if needed. Ask that all creditors contact you at a phone number you provide to verify all future applications.
- Add a "victim's statement" to the report; include your name, state the problem, and provide a telephone number where you can be reached.
- Have each credit bureau send you a copy of your report. These reports will guide you in tracing where and when any fraud occurred to your accounts.
- In a few months, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred. Unfortunately, identity thieves often strike the same accounts again and again. Because of this, it is very important to continue to monitor your credit reports very closely for a while after the initial crime. Even with a "fraud alert," thieves may still find ways to open new accounts. Ask the credit bureaus if they will supply you with free reports every few months.

### **Credit Card Companies**

If a thief has gained access to a credit card, contact the security department of that credit card company.

- Close any affected accounts so that they're registered as "closed at customer request."
- Get new account numbers, and protect the accounts with passwords.
- Follow up with a letter documenting the date, the name of the person who helped you, and what actions were taken.

Just because one card has been compromised, you may not want to close all of your credit accounts, and you may want to hold on to some cards. You may want to get counseling about this decision from a victim assistance group. (Some useful nonprofit groups are listed below.)

### **Banks**

Inform your bank if your wallet or purse was stolen or lost. Tell them what bank account information, including account numbers, ATM cards, or checks it contained.

- Cancel checking and savings accounts and open new ones.
- Stop payments on outstanding checks.
- Get a new ATM card, account number, and PIN or password.

### **Contact the Government Authorities**

It is also good to contact other authorities that specialize in identity theft. The Federal Trade Commission (FTC) runs the ID Theft Hotline and the ID Theft Data Clearinghouse.

**FTC Identity Theft Hot Line:** (877) IDTHEFT (438-4338)

If mail service was used in the fraud, contact the U.S. Postal Inspection Service. This agency is helpful if any fraudulent utility bills or apartment leases show up on your credit report.

**U.S. Postal Inspectors:** (800) 372-8347

### **Identity Theft Resources**

#### ***Credit Agencies***

##### **Equifax**

P.O. Box 740241  
Atlanta, GA 30374

[www.equifax.com](http://www.equifax.com)

Report Fraud:

(800) 525-6285

Order a Credit Report:

(800) 685-1111

##### **Experian**

P.O. Box 2002  
Allen, TX 75013

[www.experian.com](http://www.experian.com)

Report Fraud:

(888) EXPERIAN (397-3742)

Order a Credit Report:

(888) EXPERIAN (397-3742)

##### **TransUnion**

P.O. Box 1000  
Chester, PA 19022

[www.transunion.com](http://www.transunion.com)

Report Fraud:

(800) 680-7289

Order a Credit Report:

(800) 916-8800

#### ***Federal Government Resources***

##### **Federal Trade Commission**

Identity Theft Clearinghouse  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

Report Fraud:

(877) IDTHEFT (438-4338)

**U.S. Postal Inspection Service**

475 L'Enfant Plaza SW  
Washington, DC 20260  
[www.usps.gov/postalinspectors](http://www.usps.gov/postalinspectors)  
Mail Fraud Complaint Center:  
(800) 372-8347

***Nonprofit Resources***

**Identity Theft Resource Center**

P.O. Box 26833  
San Diego, CA 92196  
(858) 693-7935  
[www.idtheftcenter.org](http://www.idtheftcenter.org)

**Privacy Rights Clearinghouse**

3100 - 5th Ave., Suite B  
San Diego, CA 92103  
(619) 298-3396  
[www.privacyrights.org](http://www.privacyrights.org)

**Victims Assistance of America, Inc**

P.O. Box 33752  
Washington, DC 20033  
(502) 292-2456  
[www.victimsassistanceofamerica.org](http://www.victimsassistanceofamerica.org)

***Direct Marketers***

**Direct Marketing Association**

Mail Preference Service  
P.O. Box 643  
Carmel, NY 10512  
[www.dmaconsumers.org/offmailinglist.html](http://www.dmaconsumers.org/offmailinglist.html)