

## Identity Theft

What is identity theft?  
How it happens?  
What to do if it happens to you?  
How to prevent it?

## What Is Identity Theft?

Identity theft occurs when a person's identity is stolen for the purpose of opening credit accounts, stealing money from existing accounts, applying for loans, even renting apartments or committing crimes.

Victims of identify theft often aren't aware that they've been targeted until they find unknown charges on their bank or credit card statements, are called by a collections agency or are denied credit.

## How Identity Theft Happens

Here are some of the most common ways identity thieves can gain access to your information. They:

- Steal wallets and purses containing your identification, credit and bank cards
- Steal your mail, including bank and credit card statements, phone bills and tax information
- Complete a "change of address form" to divert your mail to another location
- Steal or illegally purchase personal information you share on the Internet
- Call you claiming to be a well know reputable company, asking for personal information.
- Send you an email, which appears to be from a reputable company, asking to respond or

go to a web site and provide your personal information. This practice is know as "phishing" (pronounced "fishing")

- Set up bogus web sites that look like familiar legitimate sites and ask you to provide personal information. This practice is known as "spoofing" .

## This Guide

This guide will help you take action to protect yourself against identity theft. If you've already been victimized, this guide will provide information about restoring your credit profile and minimize the potential for any future occurrences of identify theft.

## What To Do If You've Become A Victim Of Identity Theft?

1. Contact one of the three credit bureaus to request that an initial 90-day fraud alert be added to your personal file. By requesting a 90-day fraud alert, anyone seeking credit in your name will have to have their identity verified. The credit bureau you contact will forward the fraud alert to the remaining two credit bureaus automatically. Once you place the fraud alert in your file you are entitled to a free credit report. The information for each of the three bureaus is as follows:

Equifax  
(800) 525-6285  
Post Office Box 740241  
Atlanta, GA 30374-0241  
<http://www.equifax.com>

Experian  
(888) 397-3742

Post Office Box 9532  
Allen, TX 75013  
<http://www.experian.com>

TransUnion  
(800) 680-7289  
Fraud Victim Assistance Division  
Post Office Box 6790  
Fullerton, CA 92834-6790  
<http://www.transunion.com>

2. Notify your bank(s) and ask them to flag your account, contact you regarding any unusual activity and take the following actions in the event of such activity:

If checks were stolen, place stop payments on them.

If bank accounts were set up without your consent, close them.

If your ATM card was stolen, issue a new card, account number and PIN.

3. Notify the issuers of the credit cards you carry. If unauthorized charges appear on your legitimate credit cards or if unauthorized cards have issued in your name:

Request replacement cards with new account numbers.

Monitor credit card bills for new fraudulent activity. If found, report it immediately to the credit card issuers and credit reporting agencies.

4. Check with any online accounts, merchants or payment services that you use for any fraudulent activity against your account.
5. Contact your local police department to file a criminal report.

6. Contact the Social Security Administration's Fraud Hotline (800) 269-0271 to report the unauthorized use of your personal identification information.
7. Notify the Department of Motor Vehicles of your identity theft. Check to see whether an authorized license number has been issued in your name.
8. File a complaint with the Federal Trade Commission. Visit the Federal Trade Commission website at <http://www.consumer.gov> or call 1-877-438-4338 to review the information available in the "Take Charge: Fighting Back Against Identity Theft" brochure or to file a complaint.
9. Contact the local office of the United States Postal Service or go to its website [www.usps.com/websites/department/inspect/](http://www.usps.com/websites/department/inspect/) and file an "Identity Theft via US Mail" complaint form with the Postal Inspector.
10. Document the names and phone numbers of everyone you speak to regarding the incident. Follow up your phone calls with letters. Keep copies of all correspondence.

### **Additional Ways To Protect Your Identity**

There are some simple precautions you can take to minimize the chance of your identity being stolen.

1. Check your credit report regularly. Additionally, consumers are entitled under federal law to get one free comprehensive disclosure of all of the information in their credit file from each of the above three national credit bureaus once every 12 months. You may request your free annual credit report by visiting <http://www.AnnualCreditReport.com> or calling (877) FACTACT.

2. Shred your confidential mail.
3. Keep account numbers, Person Identification Numbers (PINs), credit and bank cards and checks in a secure location.
4. Don't select a PIN that has personal significance, such as a birthday or address and change your PIN frequently.
5. Memorize your PIN and do not share your account numbers or PINS with friends or family.
6. When conducting transactions on the Internet make sure the web sites you visit are secure and reputable. Also, utilize anti-virus software to detect malicious messages and firewalls to prevent hackers attempting to take control of your computer.
7. Always take your receipts with you from the ATM or store.
8. Never give your confidential information, including your account number and social security number to callers claiming they are from your financial institution or claiming that you have won a prize or to people unknown to you.
9. Delete unsolicited or unknown email.

### **The Middlefield Banking Company Wants to Help**

The unauthorized use of someone's identity is a serious matter to The Middlefield Banking Company. If you're a victim of identity theft or account fraud, you should call your The Middlefield Banking Company customer service representative immediately or contact The Middlefield Banking Company at <http://www.middlefieldbank.com>. The Middlefield Banking Company will work with you to correct all unauthorized transactions in your The Middlefield Banking Company accounts and correct any incorrect reports submitted by The Middlefield Banking Company to credit bureaus, and will attempt to protect you from any future identity theft or account fraud with The Middlefield Banking Company.

### **Important Numbers If You Are A Victim Of Identity Theft**

#### **Credit Bureaus**

Equifax	(800) 525-6285
Experian	(888) 397-3742
TransUnion	(800) 680-7289
TeleCheck	(800) 710-9898

**Federal trade Commission ID Theft Hotline**  
(877) 438-4338

**Social Security Fraud Hotline**  
(800) 269-0271

**United States Postal Service online**  
[www.usps.com/websites/depart/inspect/](http://www.usps.com/websites/depart/inspect/)