Think You're Already a Victim? Follow These Seven Steps.

If you suspect ANY improper or illegal activity is taking place, follow these seven steps immediately:

Check Your Credit Report

Get a copy of your credit report to see if any new accounts or credit inquiries show up. Virtually all of your credit information is in your credit report. If someone is opening accounts in your name, it should show up there.

If you suspect you've been a victim of fraud (for example; you've had your mail stolen, lost your wallet, or been contacted by a collection agency for an account you've never heard of), you should contact the fraud department for each bureau. You are eligible for a free credit report sent via U.S. mail.

Place a Fraud Alert

Contact the fraud departments of each of the three major credit bureaus and report that you think your identity has been stolen. Ask that a "fraud alert" be placed on your file and that no new credit be granted without your approval.

If you're a resident of California, you can also apply to "freeze" your credit.

Start Your Research

Contact each company where you think you might have been a victim. Talk to their security or fraud department and explain what has happened. Review your account with them for any incorrect charges or a change of address. If you find something is wrong, you may need to close the account. If you open any new accounts, ask the company to put passwords (not your mother's maiden name) on the account.

The Federal Trade Commission has tried to make this process easier by creating an Identity Theft Affidavit. It's a document you can fill out once and use with each company investigation. Get it here (you will need a web plug-in called Adobe Acrobat), or go to the FTC web site to learn more.

File a Police Report

File a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank, credit card company, or others need proof of the crime later on. Also, make sure that the crime is reported under identity theft.

Document Everything

Make notes of everyone you speak with; ask for names, department names, phone extensions; record the date you spoke to them. Don't throw these notes away! Keep all notes and letters together in case they are needed in the future. Keep track of the time you spend documenting this information and lost hours at work. You will need this information if the perpetrator is ever caught. You can be reimbursed for the time spent and hours lost. One person I know reclaimed $3200 for her effort!

Talk to the Government Agencies

The Federal Trade Commission

File a complaint with the Federal Trade Commission (FTC). The FTC is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not have the authority to bring criminal cases, the Commission assists victims of identity theft by providing them with information to help them resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for further action.

If you're see that you're a victim of identity theft, you can file a complaint with the FTC by contacting their hotline.

By phone:
Toll-free 1-877-ID-THEFT (438-4338); TDD: 202-326-2502

By mail:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

Online:
Online ID Theft Complaint Form

The Post Office

Contact your local office of the Postal Inspection Service if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity.

The Social Security Administration

Contact the Social Security Administration with any allegations that involve the following:

- Buying and selling of counterfeit or legitimate SSN cards.
- Misuse involving people with links to terrorist groups or activities.
- Misuse of an SSN by someone else to obtain Social Security benefits.

The Internal Revenue Service

Contact the Internal Revenue Service If you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).

Talk to the Check Verification Companies

If someone is using checks they've stolen from you or has set up a bank account in your name, contact the major check verification companies. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses.

Is Identity Theft Going to Cost You?

It clearly is going to cost you time and money to clear up. But your liability for charges can be limited if you report any problems promptly. Here's the info:

Credit Cards

If you report the loss before the credit card is used, the card issuer cannot hold you responsible for any unauthorized charges. If a thief uses your credit card before you report it missing, the most you will owe for unauthorized charges is $50 per card. This is true even if the thief uses your credit card at an ATM machine to obtain a cash advance.

As your liability is limited to $50, beware of calls from telemarketers selling "loss protection" insurance. Some telemarketers may falsely claim that you will be responsible for all unauthorized charges made against your account if your credit card is stolen. Don't buy the pitch and don't buy the unnecessary insurance.

How to Contact Visa, MasterCard, and American Express
Visa - (800) 847-2911
Mastercard - (800) MC-ASSIST
American Express - (800) 554-AMEX

ATM and Debit Cards
Be aware that ATM and debit cards do not allow the same protections as credit cards. If you fail to report unauthorized charges within a timely manner, you could be held liable for the charges.

- If you report an ATM or debit card missing before it is used without your permission, your financial institution cannot hold you responsible for any unauthorized withdrawals.
- If you report your ATM or debit card lost or stolen within two business days of discovering the loss or theft, your liability is limited to $50.
- If you report your ATM or debit card lost or stolen after the two business days, but within 60 days after a statement showing an unauthorized withdrawal, you can be liable for up to $500 of what a thief withdraws.
- If you wait more than 60 days, you could lose all the money that was taken from your account after the end of the 60 days and before you report the card missing.

Checks
Most states hold the bank responsible for the losses from a forged check. However, you may be held liable for the forgery if you do not notify the bank in a timely manner that a check was lost or stolen, or if you do not monitor your account statements and promptly report an unauthorized transaction. Contact the major check verification companies to request that they notify retailers using their databases not to accept the lost or stolen checks, or ask your bank to notify the check verification service with which it does business.

What is a Fraud Alert?
A fraud alert is something that the major credit bureaus attach to your credit report. When you, or someone else, tries to open up a credit account by getting a new credit card, car loan, cell phone, etc., the lender should contact you by phone to verify that you really want to open a new account. If you aren't reachable by phone, the credit account shouldn't be opened.

A creditor isn't required by law to contact you, however, even if you have fraud alert in place.

How Do I Set Up a Fraud Alert?
It's pretty easy. Just contact the fraud department of one of the credit bureaus and ask them to flag your credit file for fraud. You'll probably talk to an automated voice response system and it should only take a few minutes.

What Happens When I Activate a Fraud Alert?

- Within 24 hours, an alert will be placed on your credit file at all three major credit bureaus. They now share data so when you call one of the bureaus, your alert request is sent to the other bureaus automatically.
- Your name will be removed from all pre-approved credit and insurance offers for two years.
- You will be sent a credit report from each of the three major credit bureaus by mail. Expect 1 - 2 weeks for delivery.

The fraud alert will remain in place for 3 months (Experian), 6 months (Equifax), 12 months (TransUnion). When the time runs out, you'll need to reactivate the alert. You can also apply for a 7-year victim statement that will keep the alert in place for, you guessed it, 7 years. For this, you will have to provide proof that you've been a victim of fraud.

What Are the Drawbacks of a Fraud Alert?
Activating a fraud alert will cause you a problem if you're used to walking into an electronics store, signing up for their amazing "don't pay anything until 2009" credit offer, and walking out of the store with a new big-screen TV. With a fraud alert active, you have to be available at either your work phone or home phone to approve opening the credit account. No big deal. It will just require a short delay in your instant gratification and a call-back to the credit company authorizing the new account.

If you can live with that, putting a fraud alert on your credit will help protect you in some situations.

On the **plus side**, a fraud alert won't cause any problems with using your credit card or checking accounts. It's focused on new credit accounts, not the ones you already have opened.

Rid Yourself of Junkmail and Pesky Telemarketers

Important News:
The Federal Trade Commission's national telemarketing Do Not Call list is live!

Junkmail and telemarketing is mostly a waste of time and resources. About 62 million trees and 25 billion gallons of water are used to produce a typical year's worth of junk mail in the United States. Worst of all, it puts you at greater risk for identity theft because each pre-approved credit offer that's sent to you is another invitation for someone to open a credit line in your name.

Here's how you slow the flow of junkmail and telemarketers:

Credit Bureaus Main Opt-Out Line

888 567-8688

This call will only take you about 30 seconds and it's well worth it. Just call and talk to the nice automated voice response system (they don't want you to talk to a human, it's too expensive!) and you can opt-out of all credit-related offers for two years, or permanently. You can also call back later and opt back in if you want the credit offers to start flowing again.

If you choose to opt out permanently, you will receive an additional form in the mail. Fill out this form and return it!!! If you don't, your lifetime opt out is reduced to 2 years. The form is unmarked and looks really generic. Don't let that bother you. Fill it out and opt out of these offers permanently.

Using this service will remove you from all pre-approved credit-related mail or phone offers coming from the credit bureau lists.

Experian Consumer Services

402 458-5247

This is a service unique to Experian (as far as I can tell) that removes your name from non-credit offers coming from Experian lists. That means stuff like samples, coupons, catalogs, and local or national promotional flyers. Once again, the call will take about 30 seconds as you talk to the nice automated response system. You just have to tell them your name, address, phone number and whether you want to opt-out of mail offers, phone offers, or both.

DMA - Direct Marketing Association Opt-Out

Mail Preference Service
Direct Marketing Association
P.O. Box 9008
Farmingdale, NY 11735

Or you can use the DMA Mailing List web form.
They charge $5 to send your request over the internet, or it's free to use their form and mail it in.

Telephone Preference Service
Direct Marketing Association

P.O. Box 9014
Farmingdale, NY 11735

Or you can use the DMA Telemarketing web form.
They charge $5 to send your request over the internet, or it's free to use their form and mail it in.

The DMA is an industry organization that the more reputable direct mailers belong to. One service they provide to member companies and others, is to distribute a list of people who want to opt-out of mail or telemarketing campaigns. The DMA updates the list every month or so, but a company might not update their list for three to six months. In other words, it's going to take a while before you see a big decrease in your junkmail.

List Brokers

These companies sell mailing lists to businesses and organizations. Write all of them and request that your name be removed from all their mailing and telemarketing lists. You're going to have to mail them by hand, but we've provided some labels to make it easier.

Dunn & Bradstreet
Customer Service
899 Eaton Ave.
Bethlehem, PA 18025

Metromail Corporation
List Maintenance
901 West Bond
Lincoln, NE 68521

R.L. Polk & Co. - Name Deletion File
List Compilation Development
26955 Northwestern Hwy
Southfield, MI 48034-4716

Database America
Compilation Department
470 Chestnut Ridge Road
Woodcliff, NJ 07677

Opting-out with the credit bureaus, DMA, and list brokers is a great start. It'll take a few months, but you should see a lot less mail and telemarketing calls before long. Here's what to do to stop the rest of the mail and telephone calls:

What to Do When a Telemarketer Calls

You must remember eight very important words. Write them down and stick them next to your phone.

"Put me on your do-not-call list."

Federal law requires telemarketers to keep a list of of consumers who don't want to be called. Confirm that the caller has placed you on this list each time you get a telemarketing call and you should reduce your calls over time. If you're even more serious about reducing your telemarketing calls, we've provided a script you can follow.

What to Do With Incoming Mail

First, directly contact those companies or organizations that currently send you junk mail. We've outlined four simple ways to do this:

1. Write to the company and ask that your name and address be removed from their mailing list. (print junkmail labels)

Identity Theft

SSA Publication, Revised August 2002

Identity theft occurs when a criminal uses another person's personal information to take on that person's identity. Identity theft is much more than misuse of a Social Security number-it can also include credit card and mail fraud

Identity Theft: What it is and what you can do about it

Every year, thousands of people are victims of identity theft.

While recent developments in telecommunications and computer processing make it easier for companies and consumers to reach each other, they can also scatter your personal information more widely, making life easier for criminals.

Identity theft is the unauthorized collection and use of your personal information, usually for criminal purposes.

Your name, date of birth, address, credit card, Social Insurance Number (SIN) and other personal identification numbers can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment, or accommodation, and even secure employment.

If this happens, you could be left with the bills, charges, bad cheques, and taxes.

How to fight identity theft

- Minimize the risk. Be careful about sharing personal information or letting it circulate freely.
- When you are asked to provide personal information, ask how it will be used, why it is needed, who will be sharing it and how it will be safeguarded.
- Give out no more than the minimum, and carry the least possible with you.
- Be particularly careful about your SIN; it is an important key to your identity, especially in credit reports and computer databases.
- Don't give your credit card number on the telephone, by electronic mail, or to a voice mailbox, unless you know the person with whom you're communicating or you initiated the communication yourself, and you know that the communication channel is secure.
- Take advantage of technologies that enhance your security and privacy when you use the Internet, such as digital signatures, data encryption, and "anonymizing" services.
- Pay attention to your billing cycle. If credit card or utility bills fail to arrive, contact the companies to ensure that they have not been illicitly redirected.
- Notify creditors immediately if your identification or credit cards are lost or stolen.
- Access your credit report from a credit reporting agency once a year to ensure it's accurate and doesn't include debts or activities you haven't authorized or incurred.
- Ask that your accounts require passwords before any inquiries or changes can be made, whenever possible.
- Choose difficult passwords — *not* your mother's maiden name. Memorise them, change them often. *Don't* write them down and leave them in your wallet, or some equally obvious place.
- Key in personal identification numbers privately when you use direct purchase terminals, bank machines, or telephones.
- Find out if your cardholder agreement offers protection from credit card fraud; you may be able to avoid taking on the identity thief's debts.
- Be careful what you throw out. Burn or shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc. Insist that businesses you deal with do the same.

Are you a victim of identity theft?

- Report the crime to the police *immediately*. Ask for a copy of the police report so that you can provide proof of the theft to the organizations that you will have to contact later.

- Take steps to undo the damage. Avoid "credit-repair" companies: there is usually nothing they can do, and some have been known to propose a solution — establishing credit under a new identity — that is itself fraudulent.
- Document the steps you take and the expenses you incur to clear your name and re-establish your credit.
- Cancel your credit cards and get new ones issued. Ask the creditors about accounts tampered with or opened fraudulently in your name.
- Have your credit report annotated to reflect the identity theft. Do a follow-up check three months after to ensure that someone has not tried to use your identity again.
- Close your bank accounts and open new ones. Insist on password-only access to them.
- Get new bank machine and telephone calling cards, with new passwords or personal identification numbers.
- In the case of passport theft, advise the Passport Office.
- Contact Canada Post if you suspect that someone is diverting your mail.
- Advise your telephone, cable, and utilities that someone using your name could try to open new accounts fraudulently.
- Get a new driver's license

.

According to the F.B.I., identity theft is the fastest-growing white-collar crime in the United States. Nowadays, when your purse or wallet gets stolen, the cash inside may not be the only thing a thief wants to steal. The most valuable items in your wallet are your Social Security number, ATM card, credit cards, bank checks, and any other items containing your personal information. Additionally, during the course of a busy day, you share this information when making transactions in person, over the telephone and online to buy goods and services. If this sensitive information falls into the hands of a criminal, it may be used to steal your financial identity.

Although it is impossible to guarantee that identity theft will never happen to you, this report provides information about how to reduce your chances of becoming a victim and what actions you can take if does occur.

What is Identity Theft?

Identity theft occurs when someone uses your name, Social Security number, credit card number or some other piece of your personal information to apply for a credit card, make unauthorized purchases, gain access to your bank accounts or obtain loans under your name. Unfortunately, most people do not know that they have been victims of identity theft until mysterious charges appear on their credit card bills or they are rejected for a mortgage because unpaid bills appear on their credit report.

Types of Identity Theft

Social Security Number

Your Social Security number is the most valuable piece of your personal financial information because it is your main identifying number for employment, tax reporting, and credit history tracking purposes. If your Social Security number falls in the hands of a thief, you could face serious problems as a result. A thief could use your Social Security number to obtain employment, open credit card accounts or obtain loans under your name. The best way to protect yourself is to guard your Social Security number and provide it to others only when absolutely necessary. Some businesses request your Social Security number for general record keeping. If they do, ask how your Social Security number will be used and whether you can use any other identifying number instead.

If your Social Security number is stolen, applying for a new one may not solve your identity theft problem. For example, a new Social Security number may not ensure a new credit record because credit bureaus may combine the credit records from your old Social Security number with your new one. Moreover, even when the old credit history is not associated with your new Social Security number, the absence of any credit history under your new Social Security number may make it more difficult to obtain credit.

Credit Cards

There are numerous ways in which an identity thief can make unauthorized charges on your existing credit card accounts, or open up new accounts under your name. An ordinary thief might steal your wallet or purse and try to make use of your stolen cards and checks. The more sophisticated thief can fill out a change of address form from the post office to get all your bills sent to another address. He or she can also call your credit card issuer and, pretending to be you, change the mailing address on your credit card accounts. The impostor then runs up charges on your account. Since your bills are being sent to a new address, you may not immediately realize the problem. An identity thief might also open new accounts under your name by stealing and completing a pre-approved credit card offer sent to you in the mail, using your name, date of birth and Social Security number, but a different address, on the application form. If this occurs, you may not discover that a new account has been opened under your name until the unpaid bills appear on your credit report.

Identity thieves can also obtain your credit card information from purchases you make at stores, over the telephone or online. For example, the credit card information you provide in person or over the telephone during a purchase can be improperly used to make unauthorized charges on your account. In addition, thieves can obtain your credit card number and other personal information through fraudulent or unsecured Web sites. No matter how professional looking the Web site, check the company’s reliability with

the Better Business Bureau before doing business with it, review the Web site's security policy, and be sure to use a secure browser if you are providing credit card information online. In the address window of your browser, check to see that the first part of the company's Web address changes from "**http://**" to "**https://;**" and also check the lower corner of the Web page to see whether a lock or key symbol appears, signifying security. Using a secure browser helps to ensure the safety of your personal data when it is being transmitted to a company's computers.

Before making online purchases, check the Web site's user agreement and privacy policy to find out how the company uses your credit card and other personal information. The user agreement and privacy policy will inform you whether the information you provide is stored in the company's database and whether you can opt out of being added to the company's mailing list or having the company share your personal information with a third party. Privacy Seal programs, such as the Better Business Bureau's BBBOnline program, provide seals for Web sites that have met certain standards for protecting the privacy of the consumer information that they collect.

Check Fraud

Identity thieves can drain your checking account by stealing your checks or your checking account number from your home or office and forging your signature, or by making counterfeit checks in your name, using a home computer. Some thieves even use cleaning solvent to remove what is already written on a check, making it payable to themselves. If your checks have been stolen or misused, immediately notify your bank, place a stop payment order, and close your checking account.

Be aware that identity thieves can also open checking accounts in your name using personal information such as your Social Security number. When they write bad checks on that account, those debts appear on your credit report.

Cellular Telephone Service

Identity thieves can establish new cellular telephone service in your name or make unauthorized calls that seem to come from, and are billed to, your cellular phone. Others make unauthorized charges by using your calling card and PIN. If this occurs, contact your service provider to close your existing account, and establish another one with a new PIN.

New Scams

Internet Account Updates

You may receive e-mail requests that seem to be from your Internet Service Provider stating that your "account information needs to be updated" or that "the credit card you used to sign up for service is invalid or expired and the information needs to be reentered to keep your account active." Such requests may come from scam artists seeking to obtain your personal information to commit fraud. If you receive this kind of request, do not respond without checking with your Internet Service Provider first.

Phony Identity Theft Prevention Services

The Federal Trade Commission warns that some companies that claim to be identity theft prevention services are guises for obtaining personal information from you such as your driver's license number, mother's maiden name, Social Security number and credit and bank account numbers. Remember, do not give out any personal information over the phone or online unless you are familiar with the business that is asking for it. If you are unsure about a firm, check it out with the Better Business Bureau.

Prevention

Although there is no method for guaranteeing that identity theft will never happen to you, below are tips than can help you minimize your risk:

- Carry only the cards you actually need. Minimize the identification information and the number of cards you carry in your wallet or purse. Do not carry your Social Security card unless you need it.

- Never put your account information on the outside of an envelope or on a postcard.

- Cut up old or expired credit cards. Close all inactive credit card and bank accounts. Even though you do not use them, these accounts appear on your credit report and may be used by thieves.

- For your ATM card, choose a Personal Identification Number (PIN) different from your address, telephone number, middle name, the last four digits of your Social Security number, your birth date or any other information that could be easily discovered by thieves.

- Memorize your PIN; do not write it on your ATM card or keep it written on a piece of paper somewhere in your wallet. Statistics show that in many instances of ATM card fraud, cardholders wrote their PINs on their ATM cards or on slips of paper kept with their wallets or purses.

- Keep personal information in a safe place. If you employ outside help or are having service work done in your home, keep your personal information out of sight.

- Give your Social Security number only when absolutely necessary. Ask to use another type of identifying number whenever possible.

- Do not give out personal information over the phone, through the mail, or over the Internet unless you have initiated contact or know the business with which you are dealing.

- Compare your ATM receipts and cashed checks with your periodic bank statements to check for unauthorized transfers or charges.

- Shared credit card statements, bank statements and pre-approved credit offers when you do not need them. Consider investing in a paper shredder.

- Decrease the number of unsolicited credit card applications that you receive. The fewer credit card applications you receive, the less likely it is that one will be stolen. Call (888) 5OPT-OUT to have your name removed from the marketing lists sold by the major credit bureaus for two years, or removed permanently.

- Ask your bank about its privacy policies and information practices. Find out the circumstances under which your bank would provide your account information to a third party.

- Order a copy of your credit report from the three credit reporting agencies at least once every year to review your file for possible fraud.

Detection

One of the most frustrating aspects of identity fraud is that you may not discover it until it has already occurred. Below are some of the warning signs:

- You receive bills for a credit card account you never opened, or you may notice unfamiliar and unauthorized charges on your bills. Collection agencies may contact you regarding the payment of such debts.
- A billing cycle passes without receiving your credit card statement — or other expected mail - because it has been sent to a different address.
- Bank statements include transfers or withdrawals you do not remember, checks are missing from your checkbook, or new checks do not arrive in the mail.
- You get turned down for a credit card, mortgage or other loan because your credit report includes debts you never knew you had.

Correcting the Problem

The most important thing to do when you discover identity fraud is to take action right away. Remember to keep records of all your telephone calls and other correspondence with companies regarding the identity fraud.

- File a report with your local police or the police in the community where the identity theft took place. Keep a copy of the police report and make note of the date of your report, in case your bank, credit card company or other company needs proof of the crime.

- If you suspect that your mail is being diverted to another address, check with your local post office to see whether an unauthorized change of address form has been filed under your name.

- Call your credit card issuers right away to check on the status of your accounts if your bills do not arrive on time. If necessary, close all your accounts. You should keep a record in a safe place, separate from your credit cards, of your account numbers, expiration dates, and the telephone numbers of each card issuer so you can report a loss quickly.

- Notify your bank at once if your ATM card has been stolen or if unauthorized transfers and withdrawals have been made on one or more of your accounts. Alert your bank if your checks are stolen or missing. When you open new bank accounts, ask that a password be used before any inquiries or changes can be made to the accounts and avoid using a PIN that may be discovered by a thief, such as your birth date or the last four digits of your Social Security number.

- Canceling your credit cards may stop impostors from using your existing accounts, but it does not stop them from opening new accounts under your name. To prevent this from occurring, if your cards may have been misused by an unauthorized party, contact the fraud departments of each of the three major credit bureaus and ask them to "flag" your file as one belonging to a possible fraud victim. This warning will include a statement that creditors should call to get your permission before approving new credit cards or loans in your name. After calling each of the three credit bureaus (listed in the Resources section of this report), you should follow up with them in writing. Keep copies of such written notices.

- Ask the credit bureaus for copies of your credit reports. You are entitled to a free copy of your credit report if you were recently denied credit or if your report is inaccurate because of fraud. Review your report carefully to make sure no unauthorized charges were made on your existing accounts and that no fraudulent accounts or loans were established in your name. In a few months, order new copies of your credit reports to verify that the inaccurate information has been removed and no new fraudulent activity has occurred.

- Contact each of the creditors for any accounts that were tampered with or falsely established in your name. Ask to speak with someone in the security or fraud department. According to the Fair Credit Reporting Act, you must follow up the calls with a letter to the creditor. When writing to a credit card company, be sure to send the letter to the address provided to report billing errors. Do not send it to the address where you send payments, unless you are directed to do so.

Liability

Credit Cards

If you report the loss before the credit card is used, the card issuer cannot hold you responsible for any unauthorized charges. If a thief uses your credit card before you report it missing, the most you will owe for unauthorized charges is $50 per card. This is true even if the thief uses your credit card at an ATM machine to obtain a cash advance.

As such liability is limited to $50, beware of calls from telemarketers selling "loss protection" insurance. Some telemarketers may falsely claim that you will be responsible for all unauthorized charges made against your account if your credit card is stolen. Don't buy the pitch and don't buy the unnecessary insurance.

ATM and Debit Cards

Be aware that ATM and debit cards do not allow the same protections as credit cards. If you fail to report unauthorized charges within a timely manner, you could be held liable for the charges.

1. If you report an ATM or debit card missing before it is used without your permission, your financial institution cannot hold you responsible for any unauthorized withdrawals.
2. If you report your ATM or debit card lost or stolen within two business days of discovering the loss or theft, your liability is limited to $50.
3. If you report your ATM or debit card lost or stolen after the two business days, but within 60 days after a statement showing an unauthorized withdrawal, you can be liable for up to $500 of what a thief withdraws.
4. If you wait more than 60 days, you could lose all the money that was taken from your account after the end of the 60 days and before you report the card missing.

Checks

Most states hold the bank responsible for the losses from a forged check. However, you may be held liable for the forgery if you do not notify the back in a timely manner that a check was lost or stolen, or if you do not monitor your account statements and promptly report an unauthorized transaction. Contact the major check verification companies (listed below) to request that they notify retailers using their databases not to accept the lost or stolen checks, or ask your bank to notify the check verification service with which it does business.

National Check Fraud Service: 1-843-571-2143

SCAN: 1-800-262-7771

TeleCheck: 1-800-710-9898 or 1-800-927-0188

CrossCheck: 1-707-586-0551

Equifax Check Systems: 1-800-437-5120

International Check Services: 1-800-526-5380

Resources

Contact each of the three major credit bureaus if you discover that you are the victim of identity fraud. You are entitled to a free copy of your credit report if you are unemployed, on welfare, were recently denied credit or if your report is inaccurate because of fraud. Otherwise, there is a small fee for your credit report. When contacting the credit bureaus, you need to provide your Social Security number, date of birth, phone number, current address, any previous addresses over the past two years, and the name of your current employer.

Equifax

To report fraud by mail, contact Equifax at

P.O. Box 740256
Atlanta, GA 30374.

To order your report by telephone, contact 1-800-685-1111.
To report fraud over the telephone, contact 1-800-525-6285.

You can also access Equifax's Web site at www.equifax.com.

Experian

To order your report by mail, contact

P.O. Box 2002
Allen, TX 75013.

To report fraud by mail, contact

P.O. Box 9532
Allen, TX 75013.

To order your credit report or report fraud by telephone,
contact 1-888-EXPERIAN (397-3742).

You can also access Experian's Web site at www.experian.com.

Trans Union

To order your report by mail, contact

P.O. Box 1000
Chester, PA 19022.

To order your report by telephone, call 1-800-888-4213.

To report fraud by mail, contact

Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834.

To report fraud by telephone, call 1-800-680-7289.

You can also access Trans Union's Web site at www.tuc.com.

The Federal Trade Commission (FTC) is the federal clearinghouse for identity theft complaints. Although the FTC does not have the authority to bring criminal cases, it helps victims of identity theft by providing them with information to help resolve the financial and other problems that result from identity theft. The FTC also may refer victims' complaints to other appropriate government agencies and private organizations for action.

Contact the FTC by calling its toll-free hotline at 1-877-IDTHEFT (438-4338), by writing to

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 2058

or by accessing its Web site at www.consumer.gov/idtheft. The FTC also provides very detailed information about identity theft through this Web address: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

The Social Security Fraud Hotline should be contacted if your Social Security number is being misused. Contact the Social Security Fraud Hotline by mail at

P.O. Box 17768
Baltimore, MD 21235

by telephone at 1-800-269-0271, by fax at 1-410-597-0118

and by e-mail at oig.hotline@ssa.gov.
You can also access its Web site at www.ssa.gov

The Office of the Comptroller of Currency regulates national banks, which can usually be identified because they have the words "national" or "national association" in their titles or the letters N.A. or NT&SA following their titles. If you are unable to resolve a complaint with the bank yourself, contact the
Office of the Comptroller of Currency Consumer Assistance Group at

1301 McKinney Street, Suite 3710
Houston, TX 77010.

You can also contact this agency by telephone at 1-800-613-6743 (business days 9:00 a.m. to 3:30 p.m. CST)

by accessing its Web site at www.occ.treas.gov
or by e-mail at Customer.Assistance@occ.treas.gov.

The Office of Thrift Supervision regulates savings banks and savings and loan banks having the word "Federal" in their name or which use the initials FSB (federal savings bank) or FSLA (federal savings and loan association). You can contact this agency by writing to the

Office of Thrift Supervision, Northeast Region
Consumer Affairs
10 Exchange Place Centre, 18th Floor
Jersey City, NJ 07302.

You can also contact this agency by telephone at 1-800-842-6929

by accessing its Web site at www.ots.treas.gov
or by e-mail at consumer.complaint@ots.treas.gov.

The U.S. Postal Inspector can assist if an identity thief stole your mail to get new credit cards, bank and credit card statements, pre-screened offers, tax information, or if a thief has falsified change-of-address forms. Contact your local post office for the phone number for the nearest postal inspection service or check the Postal Service Web site at www.usps.gov/websites/depart/inspect.

The Federal Bureau of Investigation (FBI) is one of the federal criminal law enforcement agencies that investigates cases of identity theft. Local field offices are listed in the Blue Pages of your telephone directory. You can also access the FBI's Web site at www.fbi.gov.

The Better Business Bureau Serving Metropolitan New York (BBB) can be contacted if you would like to check the Reliability Rating of a company or if you have a problem resolving fraudulent charges.

The BBB can be reached in a number of ways.

To file a complaint with the Better Business Bureau through this Web site, click here: http://www.bbb.org/bbbcomplaints/Welcome.asp

For immediate assistance, call 212-533-6200. The charge is $3.80 plus applicable tax, charged to a major credit card. Consumers may also call 1-900-555-4BBB. The charge is 95 cents per minute; the average call costs $3.80.

For free information or to file a complaint by mail, write to

257 Park Avenue South
New York, NY 10010-7384

or fax your information to 212-477-4912.