WHAT SHOULD I DO IF MY WALLET OR PURSE IS LOST OR STOLEN?

24-Point Recovery Checklist

Q: What is the first step I should take if I discover that my wallet or purse has been stolen?
A: Step 1

Q: How can I limit the disclosure of my personal information?
A: Step 2

Q: Should I do anything online?
A: Step 3

Q: Should I place a fraud alert on your credit report?
A: Step 4

Q: Can I receive a free copy of my credit report?
A: Step 5

Q: Will an FTC ID Theft Report and its attached Fraudulent Account Statement enable companies to investigate the fraud and to decide the claim outcome?
A: Step 6

Q: If I have had checks stolen or bank accounts set up fraudulently, should I report it to my bank or to a check verification company?
A: Step 7

Q: Do I have the right to obtain any documentation that relates to fraudulent transactions made on my accounts or on accounts opened in my name and that use my personal information?
A: Step 8

Q: Should I close my accounts?
A: Step 9

Q: Do need to close *all* of my accounts?
A: Step 10

Q: Should I report stolen ATM, debit, prepaid, gas station, phone, department store, or any other cards?
A: Step 11

Q: Even if my Social Security card hasn't been stolen, should I contact the Social Security Administration?
A: Step 12

Q: Should I notify the U.S. State Department about lost or stolen passports either here or abroad?
A: Step 13

Q: What happens when I share my identity theft complaint with the Federal Trade Commission?
A: Step 14

Q: Is it more important to call the credit bureaus first and gather as much evidence about the identity theft; then, call the local police only when you know without a doubt that your identity has been stolen AND used?
A: Step 15

Q: Before I pay a bill from here on out, should I examine it to make sure all charges are accurate and report unauthorized charges immediately to the company?
A; Step 16

Q: Should I question any callers who want my information?
A: Step 17

Q: Do I have the right to block certain information from credit file?
A: Step 18

Q: Can I stop businesses that may report information about me to a Credit Reporting Agency?
A: Step 19

Q: What happens if I have entered into a billing dispute?
A: Step 20

Q: How can I deal with false civil and criminal judgments?
A: Step 21

Q: Should I consult an attorney to determine whether I need to take legal action or to defend against false civil and criminal charges?
A: Step 22

Q: Why should I secure all of my personal information?
A: Step 23

Q: Where else can I check to see if I may have missed anything that might pertain specifically to my case?
A: Step 24

http://www.yourcreditadvisor.com/blog/2007/03/your_identity_h.html

24-Point Recovery Checklist

Step 1: Take a deep breath and act rather than react.

As soon as you discover that your wallet has been stolen, or if a collection agency calls about a debt that you don't owe, or you're contacted to verify a loan that you didn't authorize, take a deep breath, grab a piece of paper and a pencil, and begin to document all communication and actions. Try to remember where you were if your wallet or credit cards were stolen and backtrack to recover any information that will help you to determine the time and place where the theft took place. If you talk with a loan officer or debt collector, don't cut them off. Write down the name of the person who's calling, their direct phone number and address, and a brief synopsis of your conversation. Follow up the phone call with a certified letter, return receipt requested, that allows the contacting party to file your conversation in their records.
If you received one call from a debt collector on a debt that you didn't incur, chances are you will receive more calls from collection agencies. Be nice, gather information about the agency, write down information about your conversation, and check into the charges immediately. Do not give the caller any means to pay off that collection such as a credit card or bank number, because this could cause more problems for you if the call isn't legitimate (see #20).
From this point forward, document all communications and actions taken regarding your identity theft and keep this information organized in files. This documentation will help you to verify that your identity has been stolen, and it will also help you to keep this problem from recurring.

Step 2: Limit further disclosure of personal information.

You can begin to limit the disclosure of your personal information immediately when you contact all the agencies and businesses noted below. *Make a note now* to tell all banks, brokers, credit card and check bureaus, department stores and any other business that you contact that you want to opt out of any programs that share personal information.

Step 3: Change all passwords that you use online as you walk through the next 21 steps.

While you search for business contacts and download forms to fill out in this recovery process, begin to change all your online passwords (this is assuming your computer wasn't stolen!). Thieves may have acquired your information through an online password-protected account. Use new and different passwords for each account, and stop saving your passwords online or on your computer.

Step 4. Place a fraud alert on your credit reports.

When you place a fraud alert on your credit report, you can help to prevent an identity thief from opening any accounts under your name from that point forward for 90 days. Contact any one of the three national Credit Reporting Agency (CRA) numbers listed here to file a fraud alert. You only need to contact one company, as that company is required to contact the other two companies to replicate your request. All three companies will then send a confirmation to you that will confirm that you have placed a fraud alert on your files. If you don't receive confirmation from a specific company by mail within 15 days, call that company directly to file a fraud alert.
The companies will accept your calls 24/7 any day of the year. Although the initial alert is good for 90 days, you can extend that alert for seven years if necessary.

- **Equifax**: 1-800-685-1111; www.equifax.com
- **Experian**: 1-888-EXPERIAN (888-397-3742); www.experian.com
- **TransUnion**: 1-800-916-8800; www.transunion.com

Step 5. Obtain copies of your credit reports when you file the fraud alert.

You can receive one free copy of your credit report from each agency listed above when you file a fraud alert. The credit reports will outline any financial, residential, and even medical or criminal activity that has been filed under your name. Read over these reports carefully and pay special attention to "credit inquiries" that appear unusual to you. For instance, if you find an inquiry about your credit from an unfamiliar source, this is a strong indicator that someone else has filed an application for credit under your name. This information is important, as it could supply evidence that your identity has been compromised.

You are entitled to one free credit report every year. You can stagger your requests over 12 months by requesting one report from one CRA every four months. Learn more about your credit report at the FTC so that you'll be informed about your rights before your identity is ever stolen. Outside of the three CRAs listed above, only one Web site is authorized to fill orders for the free annual credit report you are entitled to under law — annualcreditreport.com. If you request your report online, you should be able to access it immediately. If you order your report via mail or by calling toll-free 1-877-322-8228, your report will be processed and mailed to you within 15 days.

Step 6: Create an ID Theft Report with attached Fraudulent Account Statement.

To relieve yourself from any debts incurred by an identity theft, you must prove to every company where fraudulent accounts were opened or where accounts in your name were used that you didn't create that debt. The information contained on the FTC ID Theft Report and its attached Fraudulent Account Statement will enable companies to investigate the fraud and to decide the claim outcome. Plus, when you complete this form you'll better understand where to focus your attention. The last page on this form, or the Fraudulent Account Statement, will prepare you for the phone calls you need to make.

So complete this affidavit [PDF] as soon as possible. Many creditors ask that you send it within two weeks after your phone call. Delays on your part could slow the investigation and possibly increase your liability.

When you mail this affidavit to each creditor, bank, or company that provided the thief with unauthorized credit, goods, or services, attach a copy of the Fraudulent Account Statement that only pertains to accounts with a specific company. In other words, don't send information contained in your Fraudulent Account Statement that's about Company A to Company B. You might also want to include any other pertinent information for that given account, such as photocopies of bills, your documentation about phone conversations, etc.

Step 7: Report stolen checks, and close unauthorized checking and savings accounts.

The longer you wait to contact any bank or credit card company, the more liability you may take on for fraudulent activity. If you have had checks stolen or bank accounts set up fraudulently, report it to your bank or to one of the check verification companies listed below. (If a store rejects your check, ask them for the name of their check verification company.)

When you contact the major check verification companies listed below, request that they notify retailers using their databases not to accept the lost or stolen checks. You can also ask your bank to notify its check verification service. Authorize stop payments on any outstanding checks that you haven't written.

You can also ask your bank to open new accounts or to change the numbers for your existing accounts. The bank may ask you for a password to use if you want to withdraw cash while you make a deposit. You can also request this service, but don't use your mother's maiden name or your birthdate. Use an obscure password instead, like the name of a pet or a scientific term.

- **Chexsystems**: 1-800-428-9623
- **CrossCheck**: 1-707-586-0551
- **Equifax Check Systems**: 1-800-437-5120
- **International Check Services**: 1-800-526-5380
- **National Check Fraud Service**: 1-843-571-2143
- **SCAN**: 1-800-262-7771
- **TeleCheck**: 1-800-710-9898 or 1-800-927-0188

Step 8: Begin to call companies for any information that can help you prove your identity theft.

You have the right to obtain any documentation that relates to fraudulent transactions made on your accounts or on accounts opened in your name and that use your personal information. (If your name is John Smith, you may need to prove that you are *the* correct John Smith.) You may need to ask for copies of credit or other business applications in writing. Some businesses may ask for the affidavit from #6 or a police report before they'll release the information.
In some cases, a company may refuse to offer you information or provide you with documents, but in most cases they will give you an idea about how long the abuse has been going on and how much has been charged to your name. This information can help you to determine approximately when and where the theft took place. Remember that a debt collector must provide you with at least the name of the creditor and the amount of the debt you believe was incurred falsely in your name, but you must ask about that information if it isn't offered.

Step 9: Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Once you have an idea about the companies where you have tampered accounts or where accounts have been opened in your name, the security or fraud department within those companies can close those accounts. Follow up each closing with a certified letter, return receipt requested.

Step 10: Contact all your other creditors to notify them about the theft.

If you have accounts that appear to be untouched, do not close those accounts. Once you begin this identity theft recovery process, you may find that new accounts will be difficult to open — even for you. But, do contact these companies to inform them about your dilemma and to change your Personal Identification Numbers (PIN) and your passwords. Some credit card companies may offer other security efforts that can take effect immediately. Accept those suggestions if you feel comfortable with them.

Step 11. Report stolen ATM, debit, prepaid, gas station, phone, department store, or any other cards.

While you're working on those stolen checks, remember to get a new ATM card, account number, and password. If you have debit cards with any other companies, contact those companies immediately to let them know about the theft. Long distance calling cards, department store credit cards, and other cards that you use for benefits or rewards all need to be canceled or changed. Check with all companies concerned to make sure that those cards have not been used and that your personal information, if any, is safe.

Step 12. Contact the Social Security Administration.

Even if your Social Security card hasn't been stolen, a thief could still discover your Social Security number (SSN) through phishing or from your mailbox. You cannot change your SSN except under extreme circumstances, so be prepared to monitor the use of your SSN for the rest of your life. As a side

note, if you place a fraud alert with a CRA, you won't be able to access some online services (like create a password or access certain information) at the Social Security Administration site, but neither will anyone else.

- The Social Security Administration has a toll-free number that operates from 7 a.m. to 7 p.m., Monday through Friday: 1-800-772-1213, so call them to let them know that your card was stolen, or if you feel that someone else is using it.
- Order a copy of your Social Security Statement to validate that your earnings are correct.
- Order a new card if the one that you had was stolen. You are limited to three replacement cards in a year and 10 during your lifetime. Legal name changes and changes in noncitizen status that require card updates may not count toward these limits.

Step 13: Notify the U.S. State Department about lost or stolen passports.

Report any lost or stolen passports to the U.S. State Department or request Form DS-64 in writing to the address below if you are in the U.S.:

U.S. Department of State
Passport Services
Consular Lost/Stolen Passport Section
1111 19th St NW Ste 500
Washington DC 20036

If your passport is lost or stolen abroad, you should report the loss immediately to the local police and to the nearest U.S. embassy or consulate. If you can provide the consular officer with the information contained in your passport, it will facilitate issuance of a new passport. Therefore, it is a good idea to make two photocopies of the data page of your passport. Keep one copy separately from your passport to take with you on your trip, and leave the other copy with a relative or friend in the United States.

Step 14: File a complaint with the Federal Trade Commission.

When you share your identity theft with the FTC, you provide important data that can help law enforcement officials in your area and across the nation track down identity thieves. According to the FTC, their organization also can refer victims' complaints to other government agencies and companies for further action "as well as investigate companies for violations of laws that the FTC enforces." Document this information when it's provided and ask about what else they can do for you. You're going to have your hands full for a while, and any help that the FTC can offer might provide welcome relief.
You can file a complaint with the FTC online. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave NW
Washington DC 20580

Step 15. File a report with your local police or the police in the community where the identity theft took place.

Many identity theft articles state that a call to your local police should be your first priority. However, from personal experience, I know that it's more important to call the credit bureaus first and gather as much

evidence about the identity theft. Then, call the local police only when you know without a doubt that your identity has been stolen AND used.
In some cases, the police may not want to get involved at all, so don't waste your time trying to convince them to file a report. Instead, take care of some of the upcoming steps so that you have more evidence to support your complaint and then try again. The FTC site suggests that you ask to file a "Miscellaneous Incidents" report or simply try to file in another jurisdiction, like with your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or go to www.naag.org for a list of state Attorneys General.
If law officials do become interested in your case, make sure you receive a copy of the police report or the number of the report. This report, along with the affidavit in #6, will help you receive the information you need from creditors.

Step 16: Find all your bills.

Over the next few days you should begin to look for and organize all old bills to make sure that a bill isn't missing. A missing bill may indicate that a thief has changed a billing address or that one was stolen to gather your personal information. As you find bills, examine them to make sure that they're accurate. Before you pay a bill from here on out, examine it to make sure all charges are accurate and report unauthorized charges immediately to the company.

Step 17: Question any callers who want your information.

From here on out, anytime someone calls to ask for your personal information, find out what that information will be used for and why it's required. This questioning is especially important if you didn't initiate the call. If a caller states that they're from your credit card company, tell them you'll call back, hang up, and use the number on the back of your card or the number on your bill to return the call.

Step 18: Begin to block information from your credit report.

At this point you're probably confident that your identity has been stolen, and you can begin to remedy some problems that have already occurred. Additionally, you now have accurate information about debts that may have been run up and not paid by the thief. This information will appear on your credit report, but you have the right to block this information from your file. The CRAs listed in #3 can block that information, but you'll need to identify the information and provide the CRA with proof of your identity and a copy of your identity theft report.
Once a debt has been blocked, a person or business with notice of the block may not sell, transfer, or place the debt for collection. This action will help you to prevent a file from being transferred and information altered or lost — like information about your identity theft.

Step 19: Stop businesses that may report information about you to a CRA.

You also may prevent a business from reporting information about you to consumer reporting agencies if you believe the information to be false. To do so, you must send your request to the address specified by the business that reports the information to the consumer reporting agency. The business will expect you to identify what information you do not want reported and to provide an identity theft report.

Step 20: Contest bills.

When you refuse to pay off debts, you have entered into a billing dispute. If this dispute begins with a call from a collection agency, simply state that you're willing to cooperate but unwilling to pay the debt. When disputing credit card bills, you must conduct this dispute in writing by following the dispute instruction provided by any given credit card company, such as Citi or Chase. As a victim of identity theft, legal action should not be taken against you and your credit rating should not be permanently affected. If creditors try to coerce you or threaten you, report this conduct immediately to the FTC Bureau of Consumer Protection:

Federal Trade Commission
Bureau of Consumer Protection
55 E Monroe St # 1437
Chicago IL 60603
312-353-4423

Step 21: Expect to deal with false civil and criminal judgments.

Thanks to criminal identity theft, victims are wrongfully accused of crimes committed by the thief. If judgments are entered in your name for actions taken or for debts incurred by the thief, contact the court where the judgment was entered and report your status as a victim. If you remain wrongfully prosecuted, contact the Department of Justice to obtain information on how to clear your name from criminal charges.

Step 22: Seek legal advice.

At this point you may want to consult an attorney to determine whether you need to take legal action or to defend against false civil and criminal charges. Focus on finding a lawyer who specializes in consumer law, the Fair Credit Reporting Act [PDF], and the Fair Credit Billing Act. You can call your local bar association or legal aid office for help in this direction.

Step 23: Secure all your personal information.

If you keep personal information in your home or office, secure that information. This action is especially important it strangers have access to either area. When you discard personal information, such as rewards credit card offers, canceled checks, or statements, use a shredder on those items before you throw them away.

Step 24: Don't leave a stone unturned.

Go to the FTC ID Theft site or other sites like the ID Theft Center to see if you've missed anything that might pertain specifically to your case. Be persistent with the steps above and follow through with requirements. If a company wants information from you, you need to call to make sure that they received it. If a collection agency or a creditor promises to remove an offending piece of data, get that promise in writing. If you don't receive confirmation within 10 days, call every day until you see results. You can also obtain new copies of your credit reports so that you can verify if the agency followed through. If not, then copy the report and send it to the agency along with all pertinent documentation, and demand that the change be made.