TAKE CHARGE:

Fighting Back Against Identity Theft

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

TABLE OF CONTENTS

INTRODUCTION

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, change service providers for your cell phone, or apply for a credit card. Chances are you don't give these everyday transactions a second thought. But an identity thief does.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years – and thousands of dollars – cleaning up the mess the thieves have made of a good name and credit record. In the meantime, victims of identity theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they didn't commit. Humiliation, anger, and frustration are among the feelings victims experience as they navigate the process of rescuing their identity.

Working with other government agencies and organizations, the Federal Trade Commission (FTC) has produced this booklet to help you remedy the effects of an identity theft. It describes what steps to take, your legal rights, how to handle specific problems you may encounter on the way to clearing your name, and what to watch for in the future.

HOW IDENTITY THEFT OCCURS

I first was notified that someone had used my Social Security number for their taxes in February 2004. I also found out that this person opened a checking account, cable and utility accounts, and a cell phone account in my name. I'm still trying to clear up everything and just received my income tax refund after waiting four to five months. Trying to work and get all this cleared up is very stressful.

From a consumer's complaint to the FTC, July 9, 2004

Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves may use a variety of methods to gain access to your data.

HOW IDENTITY THIEVES GET YOUR PERSONAL INFORMATION:

- They get information from businesses or other institutions by:
  - stealing records or information while they're on the job
  - bribing an employee who has access to these records
  - hacking these records
  - conning information out of employees

- They may steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.

- They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."

- They may get your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.

- They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.

- They may steal your wallet or purse.

- They may steal personal information they find in your home.

- They may steal personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, or "pretexting" by phone.

HOW IDENTITY THIEVES USE YOUR PERSONAL INFORMATION:

- They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.

- They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.

- They may establish phone or wireless service in your name.

- They may open a bank account in your name and write bad checks on that account.

- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account.

- They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.

- They may buy a car by taking out an auto loan in your name.

- They may get identification such as a driver's license issued with their picture, in your name.

- They may get a job or file fraudulent tax returns in your name.

- They may give your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

IF YOUR PERSONAL INFORMATION HAS BEEN LOST OR STOLEN

If you've lost personal information or identification, or if it has been stolen from you, taking certain steps quickly can minimize the potential for identity theft.

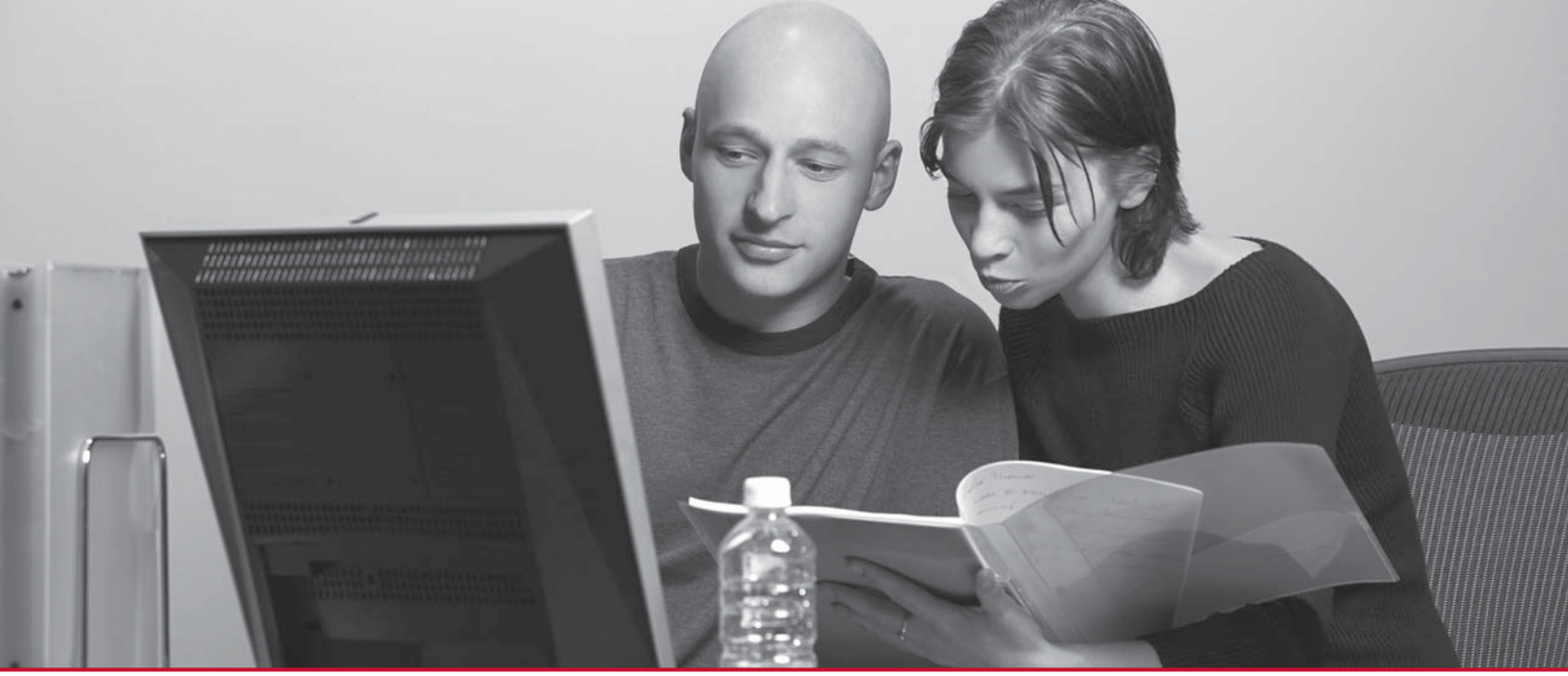
- **Financial accounts:**Close accounts, like credit cards and bank accounts, immediately. When you open new accounts, place passwords on them. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

- **Social Security number:**Call the toll-free fraud number of any of the three nationwide consumer reporting companies and place an **initial fraud alert** on your credit reports. An alert can help stop someone from opening new credit accounts in your name. For consumer reporting company contact information, see page 5. For more information about fraud alerts, see page 6.

- **Driver's license/other government-issued identification:** Contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and to get a replacement. Ask the agency to flag your file so that no one else can get a license or any other identification document from them in your name.

Once you've taken these precautions, watch for signs that your information is being misused. See **Staying Alert**, page 27.

If your information has been misused, file a report about the theft with the police, and file a complaint with the Federal Trade Commission, as well. If another crime was committed – for example, if your purse or wallet was stolen or your house or car was broken into – report it to the police immediately.



IDENTITY THEFT VICTIMS: IMMEDIATE STEPS

If you are a victim of identity theft, take the following four steps as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

1. PLACE A FRAUD ALERT ON YOUR CREDIT REPORTS, AND REVIEW YOUR CREDIT REPORTS.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

- **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

- **Experian:** 1-888-EXPERIAN (1-888-397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your SSN will appear on your credit reports.

Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information like your SSN, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See **Correcting Credit Reports**, page 17 to learn how. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

FRAUD ALERTS

There are two types of fraud alerts: an initial alert, and an extended alert.

- An initial alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer reporting companies.

- An extended alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "identity theft report" (see page 9). When you place an extended alert on your credit report, you're entitled to two free credit reports within 12 months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years – unless you ask them to put your name back on the list before then.

To place either of these alerts on your credit report, you will be required to provide appropriate proof of your identity, which may include your SSN, name, address and other personal information requested by the consumer reporting company. To remove the fraud alert, you will need a copy of an identity theft report and proof of your identity.

When a business sees the alert on your credit report, they must verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

2. CLOSE THE ACCOUNTS THAT YOU KNOW, OR BELIEVE, HAVE BEEN TAMPERED WITH OR OPENED FRAUDULENTLY.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. *It's important to notify credit card companies and banks in writing*. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the sample letter on page 20 to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.

- For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit (see page 37). If not, ask the representative to send you the company's fraud dispute forms.

If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information. See **Correcting Credit Reports**, page 17 to learn how.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

PROVING YOU'RE A VICTIM

Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing. Be sure to ask the company representative where you should mail your request. Companies must provide these records at no charge to you within 30 days of receipt of your request and your supporting documents. You also may give permission to any law enforcement agency to get these records, or ask in your written request that a copy of these records be sent to a particular law enforcement officer.

The company can ask you for:

- proof of your identity. This may be a photocopy of a government-issued ID card, the same type of information the identity thief used to open or access the account, or the type of information the company usually requests from applicants or customers, and

- a police report and a completed affidavit, which may be the Identity Theft Affidavit (see page 37) or the company's own affidavit.

3. FILE A REPORT WITH YOUR LOCAL POLICE OR THE POLICE IN THE COMMUNITY WHERE THE IDENTITY THEFT TOOK PLACE.

Then, get a copy of the police report or at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like 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 check www.naag.org for a list of state Attorneys General.

4. FILE A COMPLAINT WITH THE FEDERAL TRADE COMMISSION.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

You can file a complaint online at www.consumer.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (1-877-438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Be sure to call the Hotline to update your complaint if you have any additional information or problems.

THE IDENTITY THEFT REPORT

An identity theft report may have two parts:

Part One is a copy of a report filed with a local, state, or federal law enforcement agency, like your local police department, your State Attorney General, the FBI, the U.S. Secret Service, the FTC, and the U.S. Postal Inspection Service. There is no federal law requiring a federal agency to take a report about identity theft; however, some state laws require local police departments to take reports. When you file a report, provide as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened, and the alleged identity thief.

Note: Knowingly submitting false information could subject you to criminal prosecution for perjury.

Part Two of an identity theft report depends on the policies of the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company). That is, they may ask you to provide information or documentation in addition to that included in the law enforcement report which is reasonably intended to verify your identity theft. They must make their request within 15 days of receiving your law enforcement report, or, if you already obtained an extended fraud alert on your credit report, the date you submit your request to the credit reporting company for information blocking. The consumer reporting company and information provider then have 15 more days to work with you to make sure your identity theft report contains everything they need. They are entitled to take five days to review any information you give them. For example, if you give them information 11 days after they request it, they do not have to make a final decision until 16 days after they asked you for that information. If you give them any information after the 15-day deadline, they can reject your identity theft report as incomplete; you will have to resubmit your identity theft report with the correct information.

You may find that most federal and state agencies, and some local police departments, offer only "automated" reports – a report that does not require a face-to-face meeting with a law enforcement officer. Automated reports may be submitted online, or by telephone or mail. If you have a choice, do not use an automated report. The reason? It's more difficult for the consumer reporting company or information provider to verify the information. Unless you are asking a consumer reporting company to place an extended fraud alert on your credit report, you probably will have to provide additional information or documentation when you use an automated report.

TIPS FOR ORGANIZING YOUR CASE

Accurate and complete records will help you to resolve your identity theft case more quickly.

- Have a plan when you contact a company. Don't assume that the person you talk to will give you all the information or help you need. Prepare a list of questions to ask the representative, as well as information about your identity theft. Don't end the call until you're sure you understand everything you've been told. If you need more help, ask to speak to a supervisor.
- Write down the name of everyone you talk to, what he or she tells you, and the date the conversation occurred. Use *Chart Your Course of Action* on page 11 to help you.
- Follow up in writing with all contacts you've made on the phone or in person. Use certified mail, return receipt requested, so you can document what the company or organization received and when.
- Keep copies of all correspondence or forms you send.
- Keep the originals of supporting documents, like police reports and letters to and from creditors; send copies only.
- Set up a filing system for easy access to your paperwork.
- Keep old files even if you believe your case is closed. Once resolved, most cases stay resolved, but problems can crop up.

CHART YOUR COURSE OF ACTION

Use this form to record the steps you've taken to report the fraudulent use of your identity. Keep this list in a safe place for reference.

NATIONWIDE CONSUMER REPORTING COMPANIES – REPORT FRAUD

Consumer Reporting Company	Phone Number	Date Contacted	Contact Person	Comments
Equifax	1.800.525.6285			
Experian	1.888.EXPERIAN (397.3742)			
TransUnion	1.800.680.7289			

BANKS, CREDIT CARD ISSUERS AND OTHER CREDITORS (Contact each creditor promptly to protect your legal rights.)

Creditor	Address and Phone Number	Date Contacted	Contact Person	Comments

LAW ENFORCEMENT AUTHORITIES – REPORT IDENTITY THEFT

Agency/ Department	Phone Number	Date Contacted	Contact Person	Report Number	Comments

RESOLVING SPECIFIC PROBLEMS

I received a copy of my credit report and saw about a half a dozen items that I didn't know anything about. It's affected my credit rating so badly that I couldn't get a student loan. I didn't realize there was a problem until my student loan application was denied.

From a consumer's complaint to the FTC, May 25, 2004

While dealing with problems resulting from identity theft can be time-consuming and frustrating, most victims can resolve their cases by being assertive, organized, and knowledgeable about their legal rights. Some laws require you to notify companies within specific time periods. Don't delay in contacting any companies to deal with these problems, and ask for supervisors if you need more help than you're getting.

BANK ACCOUNTS AND FRAUDULENT WITHDRAWALS

Different laws determine your legal remedies based on the type of bank fraud you have suffered. For example, state laws protect you against fraud committed by a thief using paper documents, like stolen or counterfeit checks. But if the thief used an electronic fund transfer, federal law applies. Many transactions may seem to be processed electronically but are still considered "paper" transactions. If you're not sure what type of transaction the thief used to commit the fraud, ask the financial institution that processed the transaction.

Fraudulent Electronic Withdrawals

The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card, or another electronic way to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

You have 60 days from the date your bank account statement is sent to you to report in writing any money withdrawn from your account without your permission. This includes instances when your ATM or debit card is "skimmed" – that is, when a thief captures your account number and PIN without your card having been lost or stolen.

If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how **quickly** you report the loss.

- If you report the loss or theft within two business days of discovery, your losses are limited to $50.

- If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500 of what the thief withdraws.

- If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days.

Note: Most card issuers voluntarily have agreed to limit or waive consumers' liability for unauthorized use of their debit cards, no matter how much time has elapsed since the discovery of the loss or theft of the card. Contact your card issuer for more information.

The best way to protect yourself in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing – by certified letter, return receipt requested – so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After receiving your notification about an error on your statement, the institution generally has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that it occurred. If the institution needs more time, it may take up to 45 days to complete the investigation – but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation. For more information, see *Electronic Banking* and *Credit, ATM and Debit Cards: What To Do If They're Lost or Stolen* at www.consumer.gov/idtheft.

Fraudulent Checks and Other "Paper" Transactions

In general, if an identity thief steals your checks or counterfeits checks from your existing bank account, stop payment, close the account, and ask your bank to notify Chex Systems, Inc., (contact information on page 15) or the check verification service with which it does business. That way, retailers can be notified not to accept these checks. While no federal law limits your losses if someone uses your checks with a forged signature, or uses another type of "paper" transaction such as a demand draft, state laws may protect you. Most states hold the bank responsible for losses from such transactions. At the same time, most states require you to take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely manner that a check was lost or stolen. Contact your state banking or consumer protection agency for more information.

You can contact major check verification companies directly for the following services:

- To request that they notify retailers who use their databases not to accept your checks, call:
  - TeleCheck at 1-800-710-9898 or 1-800-927-0188
  - Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120

- To find out if the identity thief has been passing bad checks in your name, call:
  - SCAN: 1-800-262-7771

If your checks are rejected by a merchant, it may be because an identity thief is using the Magnetic Information Character Recognition (MICR) code (the numbers at the bottom of checks), your driver's license number, or another identification number. The merchant who rejects your check should give you its check verification company contact information so you can find out what information the thief is using. If you find that the thief is using your MICR code, ask your bank to close your checking account, and open a new one. If you discover that the thief is using your driver's license number or some other identification number, work with your DMV or other identification issuing agency to get new identification with new numbers. Once you have taken the appropriate steps, your checks should be accepted.

Note:

- The check verification company may or may not remove the information about the MICR code or the driver's license/identification number from its database because this information may help prevent the thief from continuing to commit fraud.

- If the checks are being passed on a new account, contact the bank to close the account. Also contact Chex Systems, Inc., to review your consumer report to make sure that no other bank accounts have been opened in your name.

- Dispute any bad checks passed in your name with merchants so they don't start any collections actions against you.

Fraudulent New Accounts

If you have trouble opening a new checking account, it may be because an identity thief has been opening accounts in your name. Chex Systems, Inc., produces consumer reports specifically about checking accounts, and as a consumer reporting company, is subject to the Fair Credit Reporting Act. You can request a free copy of your consumer report by contacting Chex Systems, Inc. If you find inaccurate information on your consumer report, follow the procedures under **Correcting Credit Reports** (see page 17) to dispute it. Contact each of the banks where account inquiries were made, too. This will help ensure that any fraudulently opened accounts are closed.

Chex Systems, Inc.: 1-800-428-9623; www.chexhelp.com
Fax: 602-659-2197
Chex Systems, Inc.
Attn: Consumer Relations
7805 Hudson Road, Suite 100
Woodbury, MN 55125

WHERE TO FIND HELP

If you have trouble getting a financial institution to help you resolve your banking-related identity theft problems, including problems with bank-issued credit cards, contact the agency that oversees your bank (see list below). If you're not sure which of these agencies is the right one, call your bank or visit the National Information Center of the Federal Reserve System at www.ffiec.gov/nic/ and click on "Institution Search."

Federal Deposit Insurance Corporation (FDIC) – www.fdic.gov

The FDIC supervises state-chartered banks that are not members of the Federal Reserve System, and insures deposits at banks and savings and loans.

Call the FDIC Consumer Call Center toll-free: 1-800-934-3342; or write: Federal Deposit Insurance Corporation, Division of Compliance and Consumer Affairs, 550 17th Street, NW, Washington, DC 20429.

FDIC publications:

- *Classic Cons... And How to Counter Them*
  www.fdic.gov/consumers/consumer/news/cnsprg98/cons.html

- *A Crook Has Drained Your Account. Who Pays?*
  www.fdic.gov/consumers/consumer/news/cnsprg98/crook.html

- *Your Wallet: A Loser's Manual*
  www.fdic.gov/consumers/consumer/news/cnfall97/wallet.html

Federal Reserve System (Fed) – www.federalreserve.gov
The Fed supervises state-chartered banks that are members of the Federal Reserve System.

Call: 202-452-3693; or write: Division of Consumer and Community Affairs, Mail Stop 801, Federal Reserve Board, Washington, DC 20551; or contact the Federal Reserve Bank in your area. The Reserve Banks are located in Boston, New York, Philadelphia, Cleveland, Richmond, Atlanta, Chicago, St. Louis, Minneapolis, Kansas City, Dallas, and San Francisco.

National Credit Union Administration (NCUA) – www.ncua.gov
The NCUA charters and supervises federal credit unions and insures deposits at federal credit unions and many state credit unions.

Call: 703-518-6360; or write: Compliance Officer, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314.

Office of the Comptroller of the Currency (OCC) – www.occ.treas.gov
The OCC charters and supervises national banks. If the word "national" appears in the name of a bank, or the initials "N.A." follow its name, the OCC oversees its operations.

Call toll-free: 1-800-613-6743 (business days 9:00 a.m. to 4:00 p.m. CST); fax: 713-336-4301; or write: Customer Assistance Group, 1301 McKinney Street, Suite 3710, Houston, TX 77010.

OCC publications:
- *Check Fraud: A Guide to Avoiding Losses*
  www.occ.treas.gov/chckfrd/chckfrd.pdf

- *How to Avoid Becoming a Victim of Identity Theft*
  www.occ.treas.gov/idtheft.pdf

- *Identity Theft and Pretext Calling Advisory Letter 2001-4*
  www.occ.treas.gov/ftp/advisory/2001-4.doc

Office of Thrift Supervision (OTS) – www.ots.treas.gov
The OTS is the primary regulator of all federal, and many state-chartered, thrift institutions, including savings banks and savings and loan institutions.

Call: 202-906-6000; or write: Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552.

BANKRUPTCY FRAUD

U. S. Trustee (UST) – www.usdoj.gov/ust

If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A list of the U.S. Trustee Programs' Regional Offices is available on the UST website, or check the Blue Pages of your phone book under U.S. Government Bankruptcy Administration.

In your letter, describe the situation and provide proof of your identity. The U.S. Trustee will make a criminal referral to law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed. The U.S. Trustee does not provide legal representation, legal advice, or referrals to lawyers. That means you may need to hire an attorney to help convince the bankruptcy court that the filing is fraudulent. When you or your attorney ask the bankruptcy court to dismiss the fraudulently filed bankruptcy case, you also should request that the bankruptcy court include in its order of dismissal facts that will help you repair your credit, including a statement that you did not file this bankruptcy case and that the case was filed by an imposter as the result of identity theft. Ask the bankruptcy court to send a copy of the dismissal order to each consumer reporting company; if the court will not do so, you should send the order to the consumer reporting companies yourself. Some courts will even provide you with several official copies of the order at no charge so that you can send them to creditors or use them in case of future problems. The U.S. Trustee does not provide consumers with copies of court documents. You can get them from the bankruptcy clerk's office for a fee.

CORRECTING FRAUDULENT INFORMATION IN CREDIT REPORTS

The Fair Credit Reporting Act (FCRA) establishes procedures for correcting fraudulent information on your credit report and requires that your report be made available only for certain legitimate business needs.

Under the FCRA, both the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company), such as a bank or credit card company, are responsible for correcting fraudulent information in your report. To protect your rights under the law, contact both the consumer reporting company and the information provider.

Consumer Reporting Company Obligations

Consumer reporting companies will block fraudulent information from appearing on your credit report if you take the following steps: Send them a copy of an identity theft report (see page 9) and a letter telling them what information is fraudulent. The letter also should state that the information does not relate to any transaction that you made or authorized. In addition, provide proof of your identity that may include your SSN, name, address, and other personal information requested by the consumer reporting company.

The consumer reporting company has four business days to block the fraudulent information after accepting your identity theft report. It also must tell the information provider that it has blocked the information. The consumer reporting company may refuse to block the information or remove the block if, for example, you have not told the truth about your identity theft. If the consumer reporting company removes the block or refuses to place the block, it must let you know.

The blocking process is only one way for identity theft victims to deal with fraudulent information. There's also the "reinvestigation process," which was designed to help all consumers dispute errors or inaccuracies on their credit reports. For more information on this process, see *How to Dispute Credit Report Errors* and *Your Access to Free Credit Reports*, two publications from the FTC at www.consumer.gov/idtheft.

SAMPLE BLOCKING LETTER – CONSUMER REPORTING COMPANY

Date
Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Name of Consumer Reporting Company
Address
City, State, Zip Code

Dear Sir or Madam:

I am a victim of identity theft. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. The items also are circled on the attached copy of the report I received. (Identify item(s) to be blocked by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

Enclosed is a copy of the law enforcement report regarding my identity theft. Please let me know if you need any other information from me to block this information on my credit report.

Sincerely,
Your name

Enclosures: (List what you are enclosing.)

Information Provider Obligations

Information providers stop reporting fraudulent information to the consumer reporting companies once you send them an identity theft report and a letter explaining that the information they're reporting resulted from identity theft. But you must send your identity theft report and letter to the address specified by the information provider. Note that the information provider may continue to report the information if it later learns that the information does not result from identity theft.

If a consumer reporting company tells an information provider that it has blocked fraudulent information in your credit report, the information provider may not continue to report that information to the consumer reporting company. The information provider also may not hire someone to collect the debt that relates to the fraudulent account, or sell that debt to anyone else who would try to collect it.

CREDIT CARDS

The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts, including fraudulent charges on your accounts. The law also limits your liability for unauthorized credit card charges to $50 per card. To take advantage of the law's consumer protections, you **must**:

- write to the creditor at the address given for "billing inquiries," NOT the address for sending your payments. Include your name, address, account number, and a description of the billing error, including the amount and date of the error. A sample letter is on page 20.

- send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. If an identity thief changed the address on your account and you didn't receive the bill, your dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill. This is one reason it's essential to keep track of your billing statements, and follow up quickly if your bills don't arrive on time.

You should send your letter by certified mail, and request a return receipt. It becomes your proof of the date the creditor received the letter. Include copies (NOT originals) of your police report or other documents that support your position. Keep a copy of your dispute letter.

The creditor must acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

For more information, see *Fair Credit Billing* and *Avoiding Credit and Charge Card Fraud,* two publications from the FTC at www.consumer.gov/idtheft.

SAMPLE DISPUTE LETTER – FOR EXISTING ACCOUNTS

Date
Your Name
Your Address
Your City, State, Zip Code
Your Account Number

Name of Creditor
Billing Inquiries
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) on my account in the amount of $_____. I am a victim of identity theft, and I did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,
Your name

Enclosures: (List what you are enclosing.)

CRIMINAL VIOLATIONS

Procedures to correct your record within criminal justice databases can vary from state to state, and even from county to county. Some states have enacted laws with special procedures for identity theft victims to follow to clear their names. You should check with the office of your state Attorney General, but you can use the following information as a general guide.

If wrongful criminal violations are attributed to your name, contact the police or sheriff's department that originally arrested the person using your identity, or the court agency that issued the warrant for the arrest. File an impersonation report with the police/sheriff's department or the court, and confirm your identity: Ask the police department to take a full set of your fingerprints,

photograph you, and make a copies of your photo identification documents, like your driver's license, passport, or travel visa. To establish your innocence, ask the police to compare the prints and photographs with those of the imposter.

If the arrest warrant is from a state or county other than where you live, ask your local police department to send the impersonation report to the police department in the jurisdiction where the arrest warrant, traffic citation, or criminal conviction originated.

The law enforcement agency should then recall any warrants and issue a "clearance letter" or "certificate of release" (if you were arrested/booked). You'll need to keep this document with you at all times in case you're wrongly arrested again. Ask the law enforcement agency to file the record of the follow-up investigation establishing your innocence with the district attorney's (D.A.) office and/or court where the crime took place. This will result in an amended complaint. Once your name is recorded in a criminal database, it's unlikely that it will be completely removed from the official record. Ask that the "key name" or "primary name" be changed from your name to the imposter's name (or to "John Doe" if the imposter's true identity is not known), with your name noted as an alias.

You'll also want to clear your name in the court records. To do so, you'll need to determine which state law(s) will help you with this and how. If your state has no formal procedure for clearing your record, contact the D.A.'s office in the county where the case was originally prosecuted. Ask the D.A.'s office for the appropriate court records needed to clear your name. You may need to hire a criminal defense attorney to help you clear your name. Contact Legal Services in your state or your local bar association for help in finding an attorney.

Finally, contact your state Department of Motor Vehicles (DMV) to find out if your driver's license is being used by the identity thief. Ask that your files be flagged for possible fraud.

DEBT COLLECTORS

The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection, even if those bills don't result from identity theft.

You can stop a debt collector from contacting you in two ways:

- Write a letter to the collection agency telling them to stop. Once the debt collector receives your letter, the company may not contact you again – with two exceptions: They can tell you there will be no further contact, and they can tell you that the debt collector or the creditor intends to take some specific action.

- Send a letter to the collection agency, within 30 days after you received written notice of the debt, telling them that you do not owe the money. Include copies of documents that support your position. Including a copy (NOT original) of your police report may be useful. In this case, a collector can renew collection activities only if it sends you proof of the debt.

If you don't have documentation to support your position, be as specific as possible about why the debt collector is mistaken. The debt collector is responsible for sending you proof that you're wrong. For example, if the debt you're disputing originates from a credit card you never applied for, ask for a copy of the application with the applicant's signature. Then, you can prove that it's not your signature.

If you tell the debt collector that you are a victim of identity theft and it is collecting the debt for another company, the debt collector must tell that company that you may be a victim of identity theft.

While you can stop a debt collector from contacting you, that won't get rid of the debt itself. To dispute the debt, it's important to contact the company that originally opened the account, otherwise that company may send it to a different debt collector, report it on your credit report, or initiate a lawsuit to collect on the debt.

For more information, see *Fair Debt Collection*, a publication from the FTC at www.consumer.gov/idtheft.

DRIVER'S LICENSE

If you think your name or SSN is being used by an identity thief to get a driver's license or a non-driver's ID card, contact your state DMV. If your state uses your SSN as your driver's license number, ask to substitute another number.

INVESTMENT FRAUD

U.S. Securities and Exchange Commission (SEC) – www.sec.gov

The SEC's Office of Investor Education and Assistance serves investors who complain to the SEC about investment fraud or the mishandling of their investments by securities professionals. If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the SEC. You can file a complaint with the SEC's Complaint Center at www.sec.gov/complaint.shtml. Include as much detail as possible. If you don't have Internet access, write to the SEC at: SEC Office of Investor Education and Assistance, 100 F Street, NE, Washington, DC 20549. For answers to general questions, call 202-551-6551.

MAIL THEFT

U.S. Postal Inspection Service (USPIS) – www.usps.gov/websites/depart/inspect

The USPIS is the law enforcement arm of the U.S. Postal Service, and investigates cases of identity theft. The USPIS has primary jurisdiction in all matters infringing on the integrity of the U.S. mail. If an identity thief has stolen your mail to get new credit cards, bank or credit card statements, pre-screened credit offers, or tax information, or has falsified change-of-address forms or obtained your personal information through a fraud conducted by mail, report it to your local postal inspector.

You can locate the USPIS district office nearest you by calling your local post office, checking the Blue Pages of your telephone directory, or visiting www.usps.gov/websites/depart/inspect.

PASSPORT FRAUD

United States Department of State (USDS) – www.travel.state.gov/passport/passport_1738.html

If you've lost your passport, or believe it was stolen or is being used fraudulently, contact the USDS through their website, or call a local USDS field office. Local field offices are listed in the Blue Pages of your telephone directory.

PHONE FRAUD

If an identity thief has established phone service in your name, is making unauthorized calls that seem to come from – and are billed to – your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs. If you're having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the appropriate agency below.

- For local service, contact your state Public Utility Commission.

- For cellular phones and long distance, contact the Federal Communications Commission (FCC) at www.fcc.gov. The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable. Call: 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554. You can file complaints online at www.fcc.gov, or e-mail your questions to fccinfo@fcc.gov.

SOCIAL SECURITY NUMBER MISUSE

Social Security Administration (SSA) – www.ssa.gov

If you have specific information of SSN misuse that involves the buying or selling of Social Security cards, may be related to terrorist activity, or is designed to obtain Social Security benefits, contact the SSA Office of the Inspector General. You may file a complaint online at www.socialsecurity.gov/oig, call toll-free: 1-800-269-0271, fax: 410-597-0118, or write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235.

You also may call SSA toll-free at 1-800-772-1213 to verify the accuracy of the earnings reported on your SSN, request a copy of your Social Security Statement, or get a replacement SSN card if yours is lost or stolen. Follow up in writing.

SSA publications:

- *SSA Fraud Hotline for Reporting Fraud*
  www.ssa.gov/oig/guidelin.htm

- *Social Security: Your Number and Card (SSA Pub. No. 05-10002)*
  www.ssa.gov/pubs/10002.html

- *Identity Theft And Your Social Security Number (SSA Pub. No. 05-10064)*
  www.ssa.gov/pubs/10064.html

STUDENT LOANS

Contact the school or program that opened the student loan to close the loan. At the same time, report the fraudulent loan to the U.S. Department of Education. Call the Inspector General's Hotline toll-free at 1-800-MIS-USED; visit www.ed.gov/about/offices/list/oig/hotline.html?src=rt; or write: Office of Inspector General, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202-1510.

TAX FRAUD

Internal Revenue Service (IRS) – www.treas.gov/irs/ci

The IRS is responsible for administering and enforcing tax laws. Identity fraud may occur as it relates directly to your tax records. Visit www.irs.gov and type in the IRS key word "Identity Theft" for more information.

If you have an unresolved issue related to identity theft, or you have suffered or are about to suffer a significant hardship as a result of the administration of the tax laws, visit the IRS Taxpayer Advocate Service website www.irs.gov/advocate/ or call toll-free: 1-877-777-4778.

If you suspect or know of an individual or company that is not complying with the tax law, report it to the Internal Revenue Service Criminal Investigation Informant Hotline by calling toll-free: 1-800-829-0433 or visit www.irs.gov and type in the IRS key word "Tax Fraud."

FOR MORE INFORMATION

Federal Trade Commission (FTC) – ftc.gov

The FTC wants consumers and businesses to know about the importance of personal information privacy. To request free copies of brochures, visit www.consumer.gov/idtheft or call 1-877-FTC-HELP (1-877-382-4357).

FTC publications:

- *ID Theft: What It's All About*
  ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm

- *Avoiding Credit and Charge Card Fraud*
  ftc.gov/bcp/conline/pubs/credit/cards.htm

- *Credit, ATM and Debit Cards: What to Do If They're Lost or Stolen*
  ftc.gov/bcp/conline/pubs/credit/atmcard.htm

- *Credit Card Loss Protection Offers: They're The Real Steal*
  ftc.gov/bcp/conline/pubs/alerts/lossalrt.htm

- *Electronic Banking*
  ftc.gov/bcp/conline/pubs/credit/elbank.htm

- *Fair Credit Billing*
  ftc.gov/bcp/conline/pubs/credit/fcb.htm

- *Fair Debt Collection*
  ftc.gov/bcp/conline/pubs/credit/fdc.htm

- *Getting Purse-onal: What To Do If Your Wallet or Purse Is Stolen*
  ftc.gov/bcp/conline/pubs/alerts/getpurse.htm

- *How to Dispute Credit Report Errors*
  ftc.gov/bcp/conline/pubs/credit/crdtdis.htm

- *Identity Crisis... What to Do If Your Identity Is Stolen*
  ftc.gov/bcp/conline/pubs/alerts/idenalrt.htm

- *Identity Thieves Can Ruin Your Good Name: Tips for Avoiding Identity Theft*
  ftc.gov/bcp/conline/pubs/credit/idthieves.htm

- *Your Access to Free Credit Reports*
  ftc.gov/bcp/conline/pubs/credit/freereports.htm

Department of Justice (DOJ) – www.usdoj.gov
The DOJ and its U.S. Attorneys prosecute federal identity theft cases. Information on identity theft is available at www.usdoj.gov/criminal/fraud/idtheft.html.

Federal Bureau of Investigation (FBI) – www.fbi.gov
The FBI, a criminal law enforcement agency, investigates cases of identity theft. The FBI recognizes that identity theft is a component of many crimes, including bank fraud, mail fraud, wire fraud, bankruptcy fraud, insurance fraud, fraud against the government, and terrorism. Local field offices are listed in the Blue Pages of your telephone directory.

U.S. Secret Service (USSS) – www.treas.gov/usss
The U.S. Secret Service investigates financial crimes, which may include identity theft. Although the Secret Service generally investigates cases where the dollar loss is substantial, your information may provide evidence of a larger pattern of fraud requiring their involvement.

Local field offices are listed in the Blue Pages of your telephone directory.

Financial Crimes Division – www.treas.gov/usss/financial_crimes.shtml

STAYING ALERT

Once resolved, most cases of identity theft stay resolved. But occasionally, some victims have recurring problems. To help stay on top of the situation, continue to monitor your credit reports and read your financial account statements promptly and carefully. You may want to review your credit reports once every three months in the first year of the theft, and once a year thereafter. And stay alert for other signs of identity theft, like:

- failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.

- receiving credit cards that you didn't apply for.

- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason.

- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

GETTING YOUR CREDIT REPORT

Free Annual Credit Reports

The Fair Credit Reporting Act requires each of the nationwide consumer reporting companies – Equifax, Experian, and TransUnion – to provide you with a free copy of your credit report, at your request, once every 12 months.

To order your free annual report from one or all the national consumer reporting companies, visit www.annualcreditreport.com, call toll-free 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The form is at the back of this booklet, or you can print it from ftc.gov/credit. Do not contact the three nationwide consumer reporting companies individually. They provide free annual credit reports only through www.annualcreditreport.com, 1-877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

The FTC advises consumers who order their free annual credit reports online to be sure to correctly spell www.annualcreditreport.com, or link to it from the FTC's website to avoid being misdirected to other websites that offer supposedly free reports, but only with the purchase of other products. While consumers may be offered additional products or services while on the authorized website, they are not required to make a purchase to receive their free annual credit reports.

For more information,
see *Your Access to Free Credit Reports*,
a publication from the FTC,
at ftc.gov/credit.

Other Consumer Rights to Free Reports

Under federal law, you're entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; you're on welfare; or your report is inaccurate because of fraud. Otherwise, a consumer reporting company may charge you up to $9.50 for another copy of your report within a 12-month period.

To buy a copy of your report, contact:

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

Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont already have free access to their credit reports.

MINIMIZING RECURRENCES

Last week I noticed that I was getting products in the mail that I hadn't ordered. Then I noticed charges on my credit card statement that I hadn't made. I spent a whole day calling the vendors' numbers listed on my statement to let them know someone was using my credit card to make purchases without my permission. I don't know what else this person may be doing with my accounts and/or my name, and I'm worried about that.

From a consumer's complaint to the FTC, January 7, 2004

When it comes to identity theft, you can't control whether you will become a victim. But there are certain steps you can take to minimize recurrences.

WHAT TO DO TODAY

- Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask if you can use a password instead.

- Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done in your home.

- Ask about information security procedures in your workplace or at businesses, doctor's offices, or other institutions that collect your personally identifying

information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

ACTIVE DUTY ALERTS FOR MILITARY PERSONNEL

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report.

When you place an active duty alert, you'll be removed from the credit reporting companies' marketing list for pre-screened credit card offers for two years unless you ask to go back on the list before then.

For contact information for the consumer reporting companies, see page 5. The process for getting and removing an alert, and a business's response to your alert, are the same as that for an initial alert (see page 6). You may use a personal representative to place or remove an alert.

MAINTAINING VIGILANCE

- Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their SSN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book. For more information, see *How Not to Get Hooked by a 'Phishing' Scam*, a publication from the FTC at www.consumer.gov/idtheft.

- Treat your mail and trash carefully.
  - Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.

- To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail. To opt out of receiving offers of credit in the mail, call: 1-888-5-OPTOUT (1-888-567-8688). The three nationwide consumer reporting companies use the same toll-free number to let consumers choose not to receive credit offers based on their lists. **Note:** You will be asked to provide your SSN which the consumer reporting companies need to match you with your file.

- Don't carry your SSN card; leave it in a secure place.

- Give your SSN only when absolutely necessary, and ask to use other types of identifiers. If your state uses your SSN as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your SSN as your policy number.

- Carry only the identification information and the credit and debit cards that you'll actually need when you go out.

- Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.

- Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

- When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.

A SPECIAL WORD ABOUT SOCIAL SECURITY NUMBERS

Your employer and financial institutions will need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your SSN for general record keeping. If someone asks for your SSN, ask:

- Why do you need my SSN?
- How will my SSN be used?
- How do you protect my SSN from being stolen?
- What will happen if I don't give you my SSN?

If you don't provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to these questions will help you decide whether you want to share your SSN with the business. The decision to share is yours.

THE DOORS AND WINDOWS ARE LOCKED, BUT . . .

You may be careful about locking your doors and windows, and keeping your personal papers in a secure place. Depending on what you use your personal computer for, an identity thief may not need to set foot in your house to steal your personal information. You may store your SSN, financial records, tax returns, birth date, and bank account numbers on your computer. These tips can help you keep your computer – and the personal information it stores – safe.

- Virus protection software should be updated regularly, and patches for your operating system and other software programs should be installed to protect against intrusions and infections that can lead to the compromise of your computer files or passwords. Ideally, virus protection software should be set to automatically update each week. The Windows XP operating system also can be set to automatically check for patches and download them to your computer.

- Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard. For more information, see *File Sharing: A Fair Share? Maybe Not* and *Spyware*, publications from the FTC at www.consumer.gov/idtheft.

- Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.

- Use a secure browser – software that encrypts or scrambles information you send over the Internet – to guard your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You also can download some browsers for free over the Internet. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password – a combination of letters (upper and lower case), numbers, and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become 1LFHA6c. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it's harder for a thief to access your personal information.

- Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.

- Look for website privacy policies. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy – or if you can't understand it – consider doing business elsewhere.

For more information, see *Site-Seeing on the Internet: A Traveler's Guide to Cyberspace*, a publication from the FTC at ftc.gov.

APPENDIX

IT'S THE LAW

Federal Law

The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028) makes identity theft a federal crime.

Under federal criminal law, identity theft takes place when someone "knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Under this definition, a name or Social Security number is considered a "means of identification." So is a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

Violations of the federal crime are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the Social Security Administration's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

For the purposes of the law, the FCRA defines identity theft to apply to consumers and businesses.

State Laws

Many states have passed laws making identity theft a crime or providing help in recovery from identity theft; others are considering such legislation. Where specific criminal identity theft laws do not exist, the practices may be prohibited under other laws. Contact your state Attorney General (for a list of state offices, visit www.naag.org) or local consumer protection agency for laws related to identity theft, or visit www.consumer.gov/idtheft.

INSTRUCTIONS FOR COMPLETING THE ID THEFT AFFIDAVIT

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened or used in your name that you didn't create the debt.

A group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) developed an ID Theft Affidavit to make it easier for fraud victims to report information. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it.

It will be necessary to provide the information in this affidavit anywhere a **new** account was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. If someone made unauthorized charges to an **existing** account, call the company for instructions.

This affidavit has two parts:

- **Part One**— the ID Theft Affidavit — is where you report general information about yourself and the theft.
- **Part Two** — the Fraudulent Account Statement — is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

   - Equifax: 1-800-525-6285; www.equifax.com
   - Experian: 1-888-EXPERIAN (1-888-397-3742); www.experian.com
   - TransUnion: 1-800-680-7289; www.transunion.com

   In addition to placing the fraud alert, the three consumer reporting companies will send you free copies of your credit reports, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

3. Your local police or the police in the community where the identity theft took place to file a report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like 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 check www.naag.org for a list of state Attorneys General.

4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC 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.

You can file a complaint online at www.consumer.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (1-877-438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

ID Theft Affidavit

Victim Information

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My Social Security number is_____

(5) My driver's license or identification card state and number are_____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was

_____ _____

City _____ State _____ Zip Code _____

(9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is (_____)_____

My evening telephone number is (_____)_____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11) ❑ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12) ❑ I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13) ❑ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were ❑ stolen ❑ lost on or about _____.
(day/month/year)

(14) ❑ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____ Name (if known)	_____ Name (if known)
_____ Address (if known)	_____ Address (if known)
_____ Phone number(s) (if known)	_____ Phone number(s) (if known)
_____ Additional information (if known)	_____ Additional information (if known)

(15) ❑ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) ❑ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

_____

_____

_____

_____

_____

(Attach additional pages as necessary.)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Victim's Law Enforcement Actions

(17) (check one) I ❑ am ❑ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I ❑ am ❑ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I ❑ have ❑ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ❑ did ❑ did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

_____	_____
(Agency #1)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(email address, if any)
_____	_____
(Agency #2)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) ❑ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) ❑ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

(22) ❑ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. §1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

_____ _____
(signature) (date signed)

_____
(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____
(signature) (printed name)

_____ _____
(date) (telephone number)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company**. Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below**.
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

❑ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address (the company that opened the account or provided the goods or services)	Account Number	Type of unauthorized credit/goods/services provided by creditor (if known)	Date issued or opened (if known)	Amount/Value provided (the amount charged or the cost of the goods/services)
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	auto loan	01/05/2002	$25,500.00

❑ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address_____

Account number _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

EQUIFAX® experian® TransUnion®

Annual Credit Report Request Form

You have the right to get a free copy of your credit file disclosure, commonly called a credit report, once every 12 months, from each of the nationwide consumer credit reporting companies - Equifax, Experian and TransUnion.

For instant access to your free credit report, visit www.annualcreditreport.com.

For more information on obtaining your free credit report, visit www.annualcreditreport.com or call 877-322-8228.

Use this form if you prefer to write to request your credit report from any, or all, of the nationwide consumer credit reporting companies. The following information is required to process your request. **Omission of any information may delay your request.**

Once complete, fold (do not staple or tape), place into a #10 envelope, affix required postage and mail to:
Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281.

Please use a Black or Blue Pen and write your responses in PRINTED CAPITAL LETTERS without touching the sides of the boxes like the examples listed below:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

Social Security Number: ___ - ___ - ____

Date of Birth: ___ / ___ / ____
Month / Day / Year

Fold Here — Fold Here

First Name _____ **M.I.** _____

Last Name _____ **JR, SR, III, etc.** _____

Current Mailing Address:

House Number _____ **Street Name** _____

Apartment Number / Private Mailbox _____ **For Puerto Rico Only: Print Urbanization Name** _____

City _____ **State** _____ **ZipCode** _____

Previous Mailing Address (complete only if at current mailing address for less than two years):

House Number _____ **Street Name** _____

Fold Here — Fold Here

Apartment Number / Private Mailbox _____ **For Puerto Rico Only: Print Urbanization Name** _____

City _____ **State** _____ **ZipCode** _____

Shade Circle Like This → ●

Not Like This → ⊗ ✓

I want a credit report from (shade each that you would like to receive):

- ◯ **Equifax**
- ◯ **Experian**
- ◯ **TransUnion**

◯ **Shade here if, for security reasons, you want your credit report to include no more than the last four digits of your Social Security Number.**

If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

31238

THE FTC'S PRIVACY POLICY

When you contact the FTC with complaints or requests for information, you can do it online at www.consumer.gov/idtheft; by telephone, toll-free at 1-877-ID-THEFT (1-877-438-4338); or by mail: Federal Trade Commission, Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Before you contact us, there are a few things you should know.

We enter the information you send into the Identity Theft Clearinghouse, an electronic database. The Clearinghouse is a system of records covered under the Privacy Act of 1974. In general, the Privacy Act prohibits unauthorized disclosures of the records it protects. It also gives individuals the right to review records about themselves. Learn more about your Privacy Act rights and the FTC's Privacy Act procedures by contacting the FTC's Freedom of Information Act Office: 202-326-2430; ftc.gov/foia/privacy_act.htm.

The information you submit is shared with FTC attorneys and investigators. It also may be shared with employees of various federal, state, or local law enforcement or regulatory authorities. The FTC also may share your information with some private entities, such as consumer reporting companies and any companies you may have complained about, where it believes that doing so might help resolve identity theft-related problems. You may be contacted by the FTC or any of the agencies or private entities to whom your complaint has been referred. In some limited circumstances, including requests from Congress, the FTC may be required by law to disclose information you submit.

You have the option to submit your information anonymously. However, if you do not provide your name and contact information, law enforcement agencies and other organizations will not be able to contact you for more information to help in identity theft investigations and prosecutions.

February 2006

1-877-ID-THEFT (1-877-438-4338)

ftc.gov/idtheft