

# A Manual and Tutorial for Dealing with ID Theft

(Adapted from FTC Recommendations 2004)

## Introduction

*My purse was stolen in December 1990. In February 1991, I started getting notices of bounced checks. About a year later, I received information that someone using my identity had defaulted on a number of lease agreements and bought a car. In 1997, I learned that someone had been working under my Social Security number for a number of years. A man had been arrested and used my SSN on his arrest sheet. There's a hit in the FBI computers for my SSN with a different name and gender. I can't get credit because of this situation. I was denied a mortgage loan, employment, credit cards, and medical care for my children. I've even had auto insurance denied, medical insurance and tuition assistance denied.*

From a consumer complaint to the FTC, January 2, 2001

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, call home on your cell phone, order new checks or apply for a credit card. Chances are you don't give these everyday transactions a second thought. But someone else may.

The 1990's spawned a new variety of crooks called identity thieves. Their stock in trade is your everyday transaction. Each transaction requires you to share personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); or your name, address and phone numbers. An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name.

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 their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans for education, housing, cars, or even be arrested for crimes they didn't commit. Humiliation, anger and frustration are common feelings victims experience as they navigate the arduous process of reclaiming their identity.

Perhaps you've received your first call from a collections agent demanding payment on a loan you never took out — for a car you never bought. Maybe you've already spent a significant amount of time and money calling financial institutions, canceling accounts, struggling to regain your good name and credit. Or maybe your wallet's been stolen, or you've just heard about identity theft for the first time on the nightly news, and you'd like to know more about protecting yourself from this devastating crime. This booklet is for you.

The Federal Trade Commission (FTC), working with other government agencies and organizations, has produced this booklet to help you guard against and recover from identity theft. Can you completely prevent identity theft from occurring? Probably not, especially if someone is determined to commit the crime. But you can minimize your risk by managing your personal information wisely and cautiously.

## WHAT TO DO WHEN YOU ARE A VICTIM

If you've been a victim of identity theft, call the FTC's Identity Theft Hotline toll-free at **1-877-IDTHEFT (438-4338)**. Counselors will take your complaint and advise you on how to deal with the credit-related problems that could result. In addition, the FTC, in conjunction with banks, credit grantors and consumer advocates, has developed the ID Theft Affidavit to help victims of ID theft restore their good names. The ID Theft Affidavit, a form that can be used to report information to many organizations, simplifies the process of disputing charges with companies where a new account was opened in your name. For a copy of the ID Theft Affidavit, scroll down to the [Appendix](#) or visit the ID Theft Web site at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

The Hotline and Web site give you one place to report the theft to the federal government and receive helpful information. The FTC puts your information into a secure consumer fraud database where it can be used to help other law enforcement agencies and private entities in their investigations and victim assistance.

### How Identity Theft Occurs

*My wallet was stolen in December 1998. There's been no end to the problems I've faced since then. The thieves used my identity to write checks, use a debit card, open a bank account with a line of credit, open credit accounts with several stores, obtain cell phones and run up huge bills, print fraudulent checks on a personal computer bearing my name, and more. I've spent the last two years trying to repair my credit report (a very frustrating process) and have suffered the ill effects of having a marred credit history. I've recently been denied a student loan because of inaccurate information on my credit report.*

From a consumer complaint to the FTC, February 22, 2001

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 — low- and hi-tech — to gain access to your data. Here are some of the ways imposters can get your personal information and take over your identity.

How identity thieves **get** your personal information:

- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, pre-approved credit offers, new checks, and tax information.
- They complete a "change of address form" to divert your mail to another location.
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving."
- They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for, and legal right to, the information.
- They find personal information in your home.
- They use personal information you share on the Internet.
- They scam you, often through email, by posing as legitimate companies or government agencies you do business with.
- They get your information from the workplace in a practice known as "business record theft" by: stealing files out of offices where you're a customer, employee, patient or

student; bribing an employee who has access to your files; or “hacking” into electronic files.

How identity thieves **use** your personal information:

- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there’s a problem.
- They open a new credit card account, using your name, date of birth and SSN. When they use the credit card and don’t pay the bills, the delinquent account is reported on your credit report.
- They establish phone or wireless service in your name.
- They open a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they’ve incurred under your name, or to avoid eviction.
- They counterfeit checks or debit cards, and drain your bank account.
- They buy cars by taking out auto loans in your name.
- They give your name to the police during an arrest. If they’re released from police custody, but don’t show up for their court date, an arrest warrant is issued in your name.

### **Minimize Your Risk**

*I’m tired of the hours I’ve spent on the phone and all the faxing I’ve had to do. When will it be over?*

**From a consumer complaint to the FTC, March 13, 2001**

*Tomorrow is Sunday so we won’t get any notices, but I’m not looking forward to Monday’s mail.*

**From a consumer complaint to the FTC, November 13, 2001**

While you probably can’t prevent identity theft entirely, you can minimize your risk. By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft.

What You Can Do Today

- **Order a copy of your credit report from each of the three major credit bureaus.** Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you’ve been sued, arrested or filed for bankruptcy. Make sure it’s accurate and includes only those activities you’ve authorized. By law, credit bureaus can charge you no more than \$9 for a copy of your credit report. See “Credit Reports,” below, for details about removing fraudulent and inaccurate information from your credit report.
- **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. Use a password instead.

- **Secure personal information in your home**, especially if you have roommates, employ outside help or are having service work done in your home.
- **Ask about information security procedures in your workplace.** Find out who has access to your personal information and verify that records are kept in a secure location. Ask about the disposal procedures for those records as well.

### CREDIT BUREAUS

**Equifax** — [www.equifax.com](http://www.equifax.com)

To order your report, call: 800-685-1111  
 To report fraud, call: 800-525-6285/  
 TDD 800-255-0056 and write:  
 P.O. Box 740241, Atlanta, GA 30374-0241

**Experian** — [www.experian.com](http://www.experian.com)

To order your report, call: 888-EXPERIAN (397-3742)  
 To report fraud, call: 888-EXPERIAN (397-3742)/  
 TDD 800-972-0322 and write:  
 P.O. Box 9532, Allen TX 75013

**TransUnion** — [www.transunion.com](http://www.transunion.com)

To order your report, call: 800-888-4213  
 To report fraud, call: 800-680-7289/  
 TDD 877-553-7803; fax: 714-447-6034; email:  
[fvad@transunion.com](mailto:fvad@transunion.com) or write: Fraud Victim Assistance  
 Department, P.O. Box 6790, Fullerton, CA 92834-6790

#### Maintaining Vigilance

- Order a copy of your credit report from each of the three major credit bureaus once a year. By checking your report on a regular basis you can catch mistakes and fraud before they wreak havoc on your personal finances. Don't underestimate the importance of this step. One of the most common ways that consumers find out that they're victims of identity theft is when they try to make a major purchase, like a house or a car. The deal can be lost or delayed while the credit report mess is straightened out. Knowing what's in your credit report allows you to fix problems before they jeopardize a major financial transaction.
- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your 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. You can check the organization's Web site as many companies post scam alerts when their name is used improperly, or you can call customer service using the number listed on your account statement or in the telephone book.
- Guard your mail and trash from theft.

Deposit 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.

- Before revealing any personally identifying information (for example, on an application), find out how it will be used and secured, and whether it will be shared with others. Ask if you have a choice about the use of your information. Can you choose to have it kept confidential?
- Don't carry your SSN card; leave it in a secure place.
- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible. If your state uses your SSN as your driver's license number, ask to substitute another number.
- Carry only the identification information and the number of credit and debit cards that you'll actually need.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work.

#### A SPECIAL WORD ABOUT SOCIAL SECURITY NUMBERS

Your employer and financial institution will likely need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check, like when you apply for a loan, rent an apartment, or sign up for utilities. Sometimes, however, they simply want your SSN for general record keeping. You don't have to give a business your SSN just because they ask for it. If someone asks for your SSN, ask the following questions:

- Why do you need my SSN?
- How will my SSN be used?
- What law requires me to give you my SSN?

- What will happen if I don't give you my SSN?

Sometimes a business may not provide you with the service or benefit you're seeking if you don't provide your SSN. Getting answers to these questions will help you decide whether you want to share your SSN with the business. Remember — the decision 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. But, 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. SSNs, financial records, tax returns, birth dates, and bank account numbers may be stored in your computer — a goldmine to an identity thief. The following tips can help you keep your computer and your personal information safe.

- Update your virus protection software regularly, or when a new virus alert is announced. Computer viruses can have a variety of damaging effects, including introducing program code that causes your computer to send out files or other stored information. Be on the alert for security repairs and patches that you can download from your operating system's Web site.
- Do not download files sent to you by strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.
- Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1, which leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited guests from accessing your computer. Without it, hackers can take over your computer and access your 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 the security of 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. Don't use an automatic log-in feature which saves your user name and password so you don't have to enter them each time you log-in or enter a site. And always log off when you're finished. That way, if your laptop gets stolen, it's harder for the thief to access your personal information.
- Before you dispose of a computer, delete personal information. Deleting files using the keyboard or mouse commands may not be enough because the files may stay on the computer's hard drive, where they may be easily retrieved. Use a "wipe" utility program to overwrite the entire hard drive. It makes the files unrecoverable. For more information, see *Clearing Information From Your Computer's Hard Drive*

([www.hq.nasa.gov/office/oig/hq/harddrive.pdf](http://www.hq.nasa.gov/office/oig/hq/harddrive.pdf)) from the National Aeronautics and Space Administration (NASA).

- Look for Web site privacy policies. They answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, as well as how information will be used, and whether it will be provided to third parties. If you don't see a privacy policy, consider surfing elsewhere.

For more information, see *Site-Seeing on the Internet: A Traveler's Guide to Cyberspace* from the FTC at [www.ftc.gov](http://www.ftc.gov).

#### Choosing to Share Your Personal Information — or Not

*In November 2000, I found out that someone used my information to obtain a cell phone. Since then, I've been living a nightmare. My credit report is a mess. It's a full-time job to investigate and correct the information.*

From a consumer complaint to the FTC, April 3, 2001

Our economy generates an enormous amount of data. Most users of that information are from honest businesses — getting and giving legitimate information. Despite the benefits of the information age, some consumers may want to limit the amount of personal information they share. And they can: More organizations are offering people choices about how their personal information is used. For example, many feature an “opt-out” choice that limits the information shared with others or used for promotional purposes. When you “opt-out,” you may cut down on the number of unsolicited telemarketing calls, promotional mail and spam emails that you receive. Learn more about the options you have for protecting your personal information by contacting the following organizations.

#### Credit Bureaus

##### Pre-Screened Credit Offers

If you receive pre-screened credit card offers in the mail (namely, those based upon your credit data), but don't tear them up after you decide you don't want to accept the offer, identity thieves could retrieve the offers for their own use without your knowledge.

To opt out of receiving pre-screened credit card offers, call: 1-888-5-OPTOUT (1-888-567- 8688). The three major credit bureaus use the same toll-free number to let consumers choose to not receive pre-screened credit offers.

#### Marketing Lists

In addition, you can notify the three major credit bureaus that you do not want personal information about you shared for promotional purposes. To ask the three major credit bureaus not to share your personal information, write to:

Equifax, Inc.  
Options  
PO Box 740123  
Atlanta, GA 30374-0123

Experian  
Consumer Opt-Out  
701 Experian Parkway  
Allen, TX 75013

TransUnion  
Marketing List Opt Out  
PO Box 97328  
Jackson, MS 39288-7328

Department of Motor Vehicles

The Drivers Privacy Protection Act forbids states from distributing personal information to direct marketers. It does allow for the sharing of personal information with law enforcement officials, courts, government agencies, private investigators, insurance underwriters and similar businesses. Check with your state DMV to learn more, or visit [www.ftc.gov/privacy/protect.htm#Motor](http://www.ftc.gov/privacy/protect.htm#Motor).

## Stopping Direct Marketers

Telemarketing

The federal government has created the National Do Not Call Registry — the free, easy way to reduce the telemarketing calls you get at home. To register, or to get information, visit [www.donotcall.gov](http://www.donotcall.gov), or call 1-888-382-1222 from the phone you want to register. You will receive fewer telemarketing calls within three months of registering your number. It will stay in the registry for five years or until it is disconnected or you take it off the registry. After five years, you will be able to renew your registration.

Mail

The Direct Marketing Association's (DMA) Mail Preference Service lets you "opt-out" of receiving direct mail marketing from many national companies for five years. When you register with this service, your name will be put on a "delete" file and made available to direct-mail marketers. However, your registration will not stop mailings from organizations that are not registered with the DMA's Mail Preference Service. To register with DMA, send your letter to:

Direct Marketing Association  
Mail Preference Service  
PO Box 643  
Carmel, NY 10512

Or register online at [www.the-dma.org/consumers/offmailinglist.html](http://www.the-dma.org/consumers/offmailinglist.html).

Email

The DMA also has an EMail Preference Service to help you reduce unsolicited commercial emails. To "opt-out" of receiving unsolicited commercial email, use DMA's online form at [www.dmaconsumers.org/offemaillist.html](http://www.dmaconsumers.org/offemaillist.html). Your online request will be effective for one year.

If You're a Victim

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information to yourself. If you suspect that your personal information has been hijacked and misappropriated to commit fraud or theft, take action immediately, and keep a record of your conversations and correspondence. You may want to use the form, "[Chart Your Course of Action](#)," below. Exactly which steps you should take to protect yourself depends on your circumstances and how your identity has been misused. However, four basic actions are appropriate in almost every case.

## Your First Four Steps

### 1. Place a fraud alert on your credit reports and review your credit reports.

Call the toll-free fraud number of any one of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

- **Equifax** — To report fraud, call: 1-800-525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian** — To report fraud, call: 1-888-EXPERIAN (397-3742), and write: P.O. Box 9532, Allen, TX 75013
- **TransUnion** — To report fraud, call: 1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you receive your reports, review them carefully. Look for inquiries you didn't initiate, accounts you didn't open, and unexplained debts on your true accounts. Where "inquiries" appear from the company(ies) that opened the fraudulent account(s), request that these "inquiries" be removed from your report. (See "Credit Reports" for more information.) You also should check that information such as your SSN, address(es), name or initial, and employers are correct. Inaccuracies in this information also may be due to typographical errors. Nevertheless, whether the inaccuracies are due to fraud or error, you should notify the credit bureau as soon as possible by telephone and in writing. You should continue to check your reports periodically, especially in the first year after you've discovered the theft, to make sure no new fraudulent activity has occurred. The automated "one-call" fraud alert process only works for the initial placement of your fraud alert. Orders for additional credit reports or renewals of your fraud alerts must be made separately at each of the three major credit bureaus.

### 2. Close any accounts that have been tampered with or opened fraudulently.

#### ***Credit Accounts***

Credit accounts include all accounts with banks, credit card companies and other lenders, and phone companies, utilities, ISPs, and other service providers.

If you're closing existing accounts and opening new ones, use new Personal Identification Numbers (PINs) and passwords.

If there are fraudulent charges or debits, ask the company about the following forms for disputing those transactions:

- For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit (available at [www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf](http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf) or in the [Appendix](#) below). If they don't, ask the representative to send you the company's fraud dispute forms.
- For your existing accounts, ask the representative to send you the company's fraud dispute forms.
- If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can. Get a new card with a new PIN.

### **Checks**

If your checks have been stolen or misused, close the account and ask your bank to notify the appropriate check verification service. While no federal law limits your losses if someone steals your checks and forges your signature, state laws may protect you. Most states hold the bank responsible for losses from a forged check, but they also 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 way that a check was lost or stolen. Contact your state banking or consumer protection agency for more information.

You also should contact these major check verification companies. Ask that retailers who use their databases not accept your checks.

**TeleCheck** — 1-800-710-9898 or 927-0188

**Certegy, Inc.** — 1-800-437-5120

**International Check Services** — 1-800-631-9656

Call SCAN (1-800-262-7771) to find out if the identity thief has been passing bad checks in your name.

### **3. File a report with your local police or the police in the community where the identity theft took place.**

Keep a copy of the report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number.

### **4. File a complaint with the FTC.**

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them. The FTC also can refer victim complaints to other appropriate government agencies and companies for further action. The FTC enters the information you provide into our secure database.

To file a complaint or to learn more about the FTC's Privacy Policy, visit [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). If you don't have access to the Internet, you can call the FTC's Identity Theft Hotline: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Tips on Filing a Police Report

- **Provide documentation.** Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, your notarized ID Theft Affidavit, and other evidence of fraudulent activity can help the police file a complete report.
- **Be persistent.** Local authorities may tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Also remind them that under their voluntary "Police Report Initiative," credit bureaus will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but **only if** you can give them a copy of the police report. If you can't get the local police to take a report, try your county police. If that doesn't work, try your state police.

If you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead. See the list of state laws below.

- **Be a motivating force.** Ask your police department to search the FTC's Consumer Sentinel database for other complaints in your community. You may not be the first or only victim of this identity thief. If there is a pattern of cases, local authorities may give your case more consideration.

That's why it's also important to file a complaint with the FTC. Law enforcement agencies use complaints filed with the FTC to aggregate cases, spot patterns, and track growth in identity theft. This information can then be used to improve investigations and victim assistance.

### Tips on Organizing Your Case

Accurate and complete records will greatly improve your chances of resolving your identity theft case.

- Follow up in writing with all contacts you've made on the phone or in person. Use certified mail, return receipt requested.

- Keep copies of all correspondence or forms you send.
- Write down the name of anyone you talk to, what he or she told you, and the date the conversation occurred. Use [Chart Your Course of Action](#), below, to help you.
- Keep the originals of supporting documentation, 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. One of the most difficult and annoying aspects of identity theft is that errors can reappear on your credit reports or your information can be re-circulated. Should this happen, you'll be glad you kept your files.

#### 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.

#### Credit Bureaus — Report Fraud

| Bureau      | Phone Number   | Date Contacted | Contact Person | Comments |
|-------------|----------------|----------------|----------------|----------|
| Equifax     | 1-800-525-6285 |                |                |          |
| Experian    | 1-888-397-3742 |                |                |          |
| Trans Union | 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 |
|--------------------------|---------------|----------------|----------------|---------------|----------|
| Federal Trade Commission | 1-877-IDTHEFT |                |                |               |          |
| Local Police Department  |               |                |                |               |          |
|                          |               |                |                |               |          |

Resolving Credit Problems

*I applied for a loan in November 2000 and was told I had bad credit. I requested a credit report in November 2000 and found all sorts of crazy information on it. I'm single but was listed as married. When I renewed my driver's license by mail, I was surprised to find someone else's face on my license. This is a nightmare and requires a large amount of my time.*

While resolving credit problems resulting from identity theft can be time-consuming and frustrating, the good news is that there are procedures under federal laws for correcting credit report and billing errors, and stopping debt collectors from contacting you about debts you don't owe. Here is a brief summary of your rights, and what to do to clear up credit problems that result from identity theft.

## Credit Reports

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

Under the FCRA, both the credit bureau and the organization that provided the information to the credit bureau (the "information provider"), such as a bank or credit card company, are responsible for correcting inaccurate or incomplete information in your report. To protect your rights under the law, contact both the credit bureau and the information provider. It's very important to follow the procedures outlined below. Otherwise you won't have any legal recourse if you have a future dispute with the credit bureau or an information provider about inaccurate information that should be blocked from your report.

First, call the credit bureau and follow up in writing. Tell them what information you believe is inaccurate. Include copies (NOT originals) of documents that support your position. If you don't have any paperwork from the creditor, send a copy of the police report and the ID Theft Affidavit (in the [Appendix](#) below) In addition to providing your complete name and address, your letter should clearly identify each item in your report that you dispute, give the facts and explain why you dispute the information, and request deletion or correction. You may want to enclose a copy of your report with circles around the items in question. Your letter may look something like the [sample](#) below. Send your letter by certified mail, return receipt requested, so you can document what the credit bureau received and when. Keep copies of your dispute letter and enclosures.

The credit bureau's investigation must be completed within 30 days (45 days if you provide additional documents). If the credit bureau considers your dispute frivolous (which may mean it believes you didn't provide enough documentation to support your claim), it must tell you so within five business days. Otherwise, it must forward all relevant documents you provide about the dispute to the information provider. The information provider then must investigate, review all relevant information provided by the credit bureau, and report the results to the credit bureau. If the information provider finds the disputed information to be inaccurate, it must notify any nationwide credit bureau to which it reports, so that the credit bureau can correct this information in your file. Note that:

- Disputed information that cannot be verified must be deleted from your file.
- If your report contains erroneous information, the credit bureau must correct it.
- If an item is incomplete, the credit bureau must complete it. For example, if your file shows that you have been late making payments, but fails to show that you are no longer delinquent, the credit bureau must show that you're current.
- If your file shows an account that belongs to someone else, the credit bureau must delete it.

When the investigation is complete, the credit bureau must give you the written results and, if the dispute results in a change, a free copy of your report. If an item is changed or removed, the credit bureau cannot put the disputed information back in your file unless the information provider

verifies its accuracy and completeness, and the credit bureau gives you a written notice that includes the name, address and phone number of the information provider.

If you ask, the credit bureau must send notices of corrections to anyone who received your report in the past six months. Job applicants can have a corrected copy of their report sent to anyone who received a copy during the past two years for employment purposes. If an investigation does not resolve your dispute, ask the credit bureau to include a 100-word statement of the dispute in your file and in future reports.

Second, in addition to writing to the credit bureau, write to the creditor or other information provider to tell them that you dispute an item. Again, include copies (NOT originals) of documents that support your position, like your police report and the ID Theft Affidavit. Many information providers specify an address for disputes. If the information provider then reports the disputed item(s) to a credit bureau, it must include a notice of your dispute. If you're correct that the disputed information is not inaccurate, the information provider may not use it again.

For more information, see *How to Dispute Credit Report Errors and Fair Credit Reporting*, from the FTC at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

### Credit Cards

In most cases, the Truth in Lending Act limits your liability for unauthorized credit card charges to \$50 per card. The Fair Credit Billing Act (FCBA) establishes procedures for resolving billing errors on your credit card accounts. This includes fraudulent charges on your accounts.

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 fraudulent charge, including the amount and date of the error. Your letter may look something like the [sample](#) below.
- send your letter so that it reaches the creditor within 60 days from when the first bill containing the fraudulent charge was mailed to you. If the address on your account was changed by an identity thief and you never received the bill, your dispute letter still must reach the creditor within 60 days of when the bill would have been mailed to you. This is why it's so important to keep track of your billing statements and immediately follow up when your bills don't arrive on time.

Send your letter by certified mail, return receipt requested. This will be your proof of the date the creditor received the letter. Include copies (NOT originals) of sales slips 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*, from the FTC at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

### 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.

You can stop a debt collector from contacting you by writing 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.

A collector also may not contact you if, within 30 days after you receive the written notice, you send the collection agency a letter stating you do not owe the money.

Although your letter should stop the debt collector's calls and dunning notices, it will not necessarily get rid of the debt itself, which may still turn up on your credit report.

A collector can renew collection activities if you're sent proof of the debt. So, along with your letter stating you don't owe the money, include copies of documents that support your position.

If you're a victim of identity theft, include a copy (NOT the original) of the police report. 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 in dispute originates from a credit card you never applied for, ask for the actual application containing the applicant's signature. You can then prove that it's not your signature on the application. In many cases, the debt collector will not send you any proof, but will instead return the debt to the creditor.

For more information, see Fair Debt Collection from the FTC at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

#### ATM Cards, Debit Cards and Electronic Fund Transfers

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

It's important to report lost or stolen ATM and debit cards immediately because the amount you can be held responsible for depends on **how quickly** you report the loss.

- If you report your ATM card lost or stolen within two business days of discovering the loss or theft, your losses are limited to \$50.
- If you report your ATM card lost or stolen after the two business days, but within 60 days after a statement showing an unauthorized electronic fund transfer, you can be liable for up to \$500 of what a thief withdraws.
- If you wait more than 60 days, you could lose **all** the money that was taken from your account from the end of the 60 days to the time you reported your card missing.

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 notification about an error on your statement, the financial 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 the error has 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.

**Note:** VISA and MasterCard voluntarily have agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to \$50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.

For more information, see *Electronic Banking and Credit, ATM and Debit Cards: What to Do If They're Lost or Stolen*, two consumer publications from the FTC at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

### **Proving You're a Victim, Not a Deadbeat**

Unlike victims of other crimes, who generally are treated with respect and sympathy, identity theft victims often find themselves having to prove that they're victims, too — not deadbeats trying to get out of paying bad debts. So how do you go about proving something you didn't do? Getting the right documents and getting them to the right people is key.

**The Police Report:** If you have a police report, send a copy to Experian, Equifax and TransUnion. They will block the information you're disputing from your credit reports. This may take up to 30 days. The credit bureaus have the right to remove the block, if they believe it was wrongly placed. Because this initiative is voluntary in the vast majority of states, it's important to also follow the dispute procedures outlined in "[Credit Reports](#)," above. Contact the credit bureaus to find out more about how the "Police Report Initiative" works. If you're having trouble getting a police report, see "[Tips on Filing a Police Report](#)," above.

**The ID Theft Affidavit:** Since you didn't open the accounts in dispute or run up the related debts, of course you don't have any paperwork showing you didn't do these things. That's where the ID Theft Affidavit can be very helpful. The FTC, in conjunction with banks, credit grantors and consumer advocates, developed the ID Theft Affidavit (see [Appendix](#) below) to help you close unauthorized accounts and get rid of debts wrongfully attributed to your name. If you don't have a police report or any paperwork from creditors, send the completed ID Theft Affidavit to the three major credit bureaus. They will use it to start the dispute investigation process. Not all companies accept the ID Theft Affidavit. They may require you to use their forms instead. Check first.

**Creditor Documentation:** Getting documentation from a

creditor may be difficult. Creditors' policies on confidentiality and record keeping vary and may prevent you from getting the paperwork you need to prove you didn't make the transaction. On the upside, most victims can get accounts closed and debts dismissed by completing the creditor's fraud paperwork or the ID Theft Affidavit and including a copy of your police report. Insist on a letter from the creditor stating that they have closed the disputed accounts and have discharged you of the fraudulent debts. This letter is your best defense if errors reappear or your personal information gets re-circulated. (See ["Tips on Organizing Your Case."](#) above). This letter is also the best document to give credit bureaus and debt collectors if your police report and ID Theft Affidavit aren't enough to resolve your problems with them.

#### SAMPLE DISPUTE LETTER — CREDIT BUREAU

Date

Your Name

Your Address

Your City, State, Zip Code

Complaint Department

Name of Credit Bureau

Address

City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute also are circled on the attached copy of the report I received. (Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

I am a victim of identity theft, and did not make the charge(s). I am requesting that the item be blocked to correct my credit report.

Enclosed are copies of (use this sentence if applicable and describe any enclosed documentation) supporting my position. Please investigate this (these) matter(s) and block the disputed item(s) as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

SAMPLE DISPUTE LETTER — FOR EXISTING CREDIT 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) attributed to 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 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.)

FILING A COMPLAINT WITH THE FTC IS IMPORTANT

If you've been a victim of identity theft, file a complaint with the FTC by contacting the FTC's Identity Theft Hotline by telephone: toll-free **1-877-IDTHEFT (438-4338)**; TDD: 202-326-2502; by mail: Identity Theft Clearinghouse,

Federal Trade Commission,  
600 Pennsylvania Avenue, NW, Washington, DC 20580; or online: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

Although the FTC does not have the authority to bring criminal cases, the Commission can help victims of identity theft by providing information to assist them in resolving the financial and other problems that can result from this crime.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them. The FTC also refers victim complaints to other appropriate government agencies and private organizations for further action.

## Specific Problems

Numerous federal and state agencies have jurisdiction over specific aspects of identity theft. If your theft relates to any of the following categories, contact the agencies directly for help and information or to initiate an investigation.

### Bank Fraud

If you're having trouble getting your financial institution to help you resolve your banking-related identity theft problems, including problems with bank-issued credit cards, contact the agency with the appropriate jurisdiction. If you're not sure which of the agencies listed below has jurisdiction over your institution, call your bank or visit [www.ffiec.gov/enforcement.htm](http://www.ffiec.gov/enforcement.htm).

#### **Federal Deposit Insurance Corporation (FDIC)** — [www.fdic.gov](http://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 at 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](http://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](http://www.fdic.gov/consumers/consumer/news/cnsprg98/crook.html)
- *Your Wallet: A Loser's Manual* — [www.fdic.gov/consumers/consumer/news/cnfall97/wallet.html](http://www.fdic.gov/consumers/consumer/news/cnfall97/wallet.html)

#### **Federal Reserve System (Fed)** — [www.federalreserve.gov](http://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 12 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](http://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](http://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: 1-800-613-6743 (business days 9:00 a.m. to 4:00 p.m. CST); fax: 713-336-4301; 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](http://www.occ.treas.gov/chckfrd/chckfrd.pdf)
- *How to Avoid Becoming a Victim of Identity Theft* — [www.occ.treas.gov/idtheft.pdf](http://www.occ.treas.gov/idtheft.pdf)
- *Identity Theft and Pretext Calling Advisory Letter 2001-4* — [www.occ.treas.gov/ftp/advisory/2001-4.doc](http://www.occ.treas.gov/ftp/advisory/2001-4.doc)

**Office of Thrift Supervision (OTS)** — [www.ots.treas.gov](http://www.ots.treas.gov)

The OTS is the primary regulator of all federal, and many state-chartered, thrift institutions, which include 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](http://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’s Regional Offices is available on the UST Web site, or check the Blue Pages of your phone book under U.S. Government Bankruptcy Administration.

Your letter should describe the situation and provide proof of your identity. The U.S. Trustee, if appropriate, 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. The U.S. Trustee does not provide consumers with copies of court documents. Those documents are available from the bankruptcy clerk’s office for a fee.

### Criminal Violations

Although procedures to correct your record within the criminal justice databases vary from state to state, and even from county to county, the following information can be used as a general guide.

If wrongful criminal violations are attributed to your name, contact the arresting or citing law enforcement agency — that is, 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. And have your identity confirmed: The police department takes a full set of your fingerprints and your photograph, and copies any photo identification documents like your

driver's license, passport or visa. Ask the law enforcement agency to compare the prints and photographs with those of the imposter to establish your innocence. 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. Also, ask the law enforcement agency to file, with the district attorney's (D.A.) office and/or court where the crime took place, the record of the follow-up investigation establishing your innocence. This will result in an amended complaint being issued. 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 only as an alias.

You'll also want to clear your name in the court records. You'll need to determine which state law(s) will help you do 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.

Finally, contact your state 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.

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.

#### Fake 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 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](http://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 using the online Complaint Center at [www.sec.gov/complaint.shtml](http://www.sec.gov/complaint.shtml). Be sure to include as much detail as possible. If you don't have access to the Internet, you can write to the SEC at: SEC Office of Investor Education and Assistance, 450 Fifth Street, NW, Washington DC, 20549-0213. For general questions, call 202-942-7040.

#### Mail Theft

##### **U.S. Postal Inspection Service (USPIS)** — [www.usps.gov/websites/depart/inspect](http://www.usps.gov/websites/depart/inspect)

USPIS is the law enforcement arm of the U.S. Postal Service responsible for investigating cases of identity theft. 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, 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 USPIIS district office nearest you by calling your local post office or checking the list at the Web site above.

#### Passport Fraud

**United States Department of State (USDS)** — [www.travel.state.gov/passport\\_services.html](http://www.travel.state.gov/passport_services.html)

If you've lost your passport or believe it was stolen or is being used fraudulently, contact the USDS through their Web site 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 from the list below.

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

**For cellular phones and long distance**, contact the Federal Communications Commission (FCC) — [www.fcc.gov](http://www.fcc.gov). The FCC regulates interstate and international communications by radio, television, wire, satellite and cable. You can contact the FCC's Consumer Information Bureau to find out about information, forms, applications and current issues before the FCC. 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 via the online complaint form at [www.fcc.gov](http://www.fcc.gov), or e-mail questions to [fccinfo@fcc.gov](mailto:fccinfo@fcc.gov).

#### Social Security Number (SSN) Theft and Misuse

**Social Security Administration (SSA)** — [www.socialsecurity.gov](http://www.socialsecurity.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](http://www.socialsecurity.gov/oig). You may also call: 1-800-269-0271; fax: 410-597-0118; or write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235.

Also call SSA at 1-800-772-1213 to verify the accuracy of the earnings reported on your SSN, and to request a copy of your Social Security Statement. Follow up in writing.

SSA publications:

- *SSA Fraud Hotline for Reporting Fraud* — [www.ssa.gov/oig/guidelin.htm](http://www.ssa.gov/oig/guidelin.htm)
- *Social Security: Your Number and Card* (SSA Pub. No. 05-10002) — [www.ssa.gov/pubs/10002.html](http://www.ssa.gov/pubs/10002.html)
- *When Someone Misuses Your Number* (SSA Pub. No. 05-10064) — [www.ssa.gov/pubs/10064.html](http://www.ssa.gov/pubs/10064.html)

#### Tax Fraud

**Internal Revenue Service (IRS)** — [www.treas.gov/irs/ci](http://www.treas.gov/irs/ci)

The IRS is responsible for administering and enforcing tax laws. If you believe someone has

assumed your identity to file federal Income Tax Returns, or to commit other tax fraud, call toll-free: 1-800-829-0433. Victims of identity theft who are having trouble filing their returns should call the IRS Taxpayer Advocates Office, toll-free: 1-877-777-4778.

#### FOR MORE INFORMATION

**Department of Justice (DOJ)** — [www.usdoj.gov](http://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](http://www.usdoj.gov/criminal/fraud/idtheft.html).

**Federal Bureau of Investigation (FBI)** — [www.fbi.gov](http://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/uss](http://www.treas.gov/uss)

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/uss/financial\\_crimes.shtml](http://www.treas.gov/uss/financial_crimes.shtml)

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) is the federal law making identity theft a crime.

Identity Theft and Assumption Deterrence Act of 1998

The Identity Theft and Assumption Deterrence Act makes it a federal crime when someone “knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.”

Under the Act, a name or SSN 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 Act are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and SSA's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

In most instances, a conviction for identity theft carries a maximum penalty of 15 years imprisonment, a fine and forfeiture of any personal property used or intended to be used to commit the crime. Pursuant to the Act, the U.S. Sentencing Commission has developed federal sentencing guidelines to provide appropriate penalties for those persons convicted of identity theft.

Schemes to commit identity theft or fraud also may involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties — in some cases, as high as 30 years in prison as well as fines and criminal forfeiture.

## State Laws

Many states have passed laws related to identity theft; others are considering such legislation. Where specific identity theft laws do not exist, the practices may be prohibited under other laws. Contact your State Attorney General's office (for a list of state offices, visit [www.naag.org](http://www.naag.org)) or local consumer protection agency for laws related to identity theft, or visit [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). State laws enacted at the time of this booklet's publication are listed below.

### Alabama

Alabama Code § 13A-8-190 through 201

### Alaska

Alaska Stat. § 11.46.565

### Arizona

Ariz. Rev. Stat. § 13-2008

### Arkansas

Ark. Code Ann. § 5-37-227

### California

Cal. Penal Code § 530.5-530.8

### Colorado

No ID theft law

### Connecticut

Conn. Stat. § 53a-129a (criminal);

Conn. Stat. § 52-571h (civil)

### Delaware

11 Del Code, § 854

### Florida

Fla. Stat. Ann. § 817.568

### Georgia

Ga. Code Ann. § 16-9-120 through 128

### Hawaii

No ID theft law

### Idaho

Idaho Code § 18-3126 (criminal); Idaho Code § 28-51-102 (civil)

### Illinois

720 Ill. Comp. Stat. 5/16G

Indiana  
Ind. Code § 35-43-5-3.5

Iowa  
Iowa Code § 715A.8 (criminal); Iowa Code § 714.16.B (civil)

Kansas  
Kan. Stat. Ann. § 21-4018

Kentucky  
Ky. Rev. Stat. Ann. § 514.160

Louisiana  
La. Rev. Stat. Ann. § 14:67.16

Maine  
No ID theft law

Maryland  
Md. Code Ann. art. 27, § 231

Massachusetts  
Mass. Gen. Laws ch. 266, § 37E

Michigan  
Mich. Comp. Laws § 750.219e

Minnesota  
Minn. Stat. § 609.527

Mississippi  
Miss. Code Ann. § 97-19-85

Missouri  
Mo. Rev. Stat. § 570.223

Montana  
Mon. Code Ann. § 45-6-332

Nebraska  
No ID theft law

Nevada  
Nev. Rev. State. § 205.463-465

New Hampshire  
N.H. Rev. Stat. Ann. § 638:26

New Jersey  
N.J. Stat. Ann. § 2C:21-17

New Mexico  
N.M. Stat. Ann. § 30-16-24.1

New York  
No ID theft law

North Carolina  
N.C. Gen. Stat. § 14-113.20-23

North Dakota  
N.D.Cent. Codes § 12.1-23-11

Ohio  
Ohio Rev. Code Ann. § 2913.49

Oklahoma  
Okla. Stat. tit. 21, § 1533.1

Oregon  
Or. Rev. Stat. § 165.800

Pennsylvania  
18 Pa. Cons. Stat. § 4120

Rhode Island  
R.I. Gen. Laws Sect. 11-49-1.1

South Carolina  
S.C. Code Ann. § 16-13-510

South Dakota  
S.D. Codified Laws § 22-30A-3.1.

Tennessee  
TCA § 39-14-150 (criminal); TCA § 47-18-2101 (civil)

Texas  
Tex. Penal Code § 32.51

Utah  
Utah Code Ann. § 76-6-1101-1104

Virginia  
Va. Code Ann. § 18.2-186.3

Vermont  
No ID theft law

Washington  
Wash. Rev. Code § 9.35.020

West Virginia  
W. Va. Code § 61-3-54

Wisconsin  
Wis. Stat. § 943.201

Wyoming  
Wyo. Stat. Ann. § 6-3-901

## U.S. TERRITORIES

Guam  
9 Guam Code Ann. § 46.80

U.S. Virgin Islands  
No ID theft law

## Appendix

### Instructions for Completing the ID Theft Affidavit

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

A working group composed of credit grantors, consumer advocates and the Federal Trade Commission (FTC) developed this ID Theft Affidavit to help you report information to many companies using just one standard form. Use of this affidavit is optional for companies. 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.

You can use this affidavit where 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 to find out what to do.)

This affidavit has two parts:

- ID Theft Affidavit is where you report general information about yourself and the theft.
- 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, police report) you have. 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 of receiving it. Delaying 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. Please 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 to each affidavit a copy of the Fraudulent Account Statement with information only on accounts

opened at the institution receiving 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 for your records.

If you cannot 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. Each of the three **national consumer reporting agencies**. Ask each agency to place a "fraud alert" on your credit report, and send you a copy of your credit file. When you have completed your affidavit packet,