



# Defend: Recover From Identity Theft

## Take Steps to Respond to and Recover from Identity Theft as Soon as You Suspect It

### What Are the Steps I Should Take If I'm a Victim of Identity Theft?

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. The FTC has developed a template for recording the steps you've taken to report the fraudulent use of your identity, see the "Helpful Resources" section at the end of this guide for information on how to access this document.

#### 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. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

Name	Phone	URL	Address
<b>TransUnion</b>	800-680-7289	www.transunion.com	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790
<b>Equifax</b>	800-525-6285	www.equifax.com	P.O. Box 74024 Atlanta, GA 30374-0241
<b>Experian</b>	888-EXPERIAN (397-3742)	www.experian.com	P.O. Box 9532 Allen, TX 75013

Once you place the fraud alert in your file, you're entitled to order one free copy of your credit report from each of the three consumer reporting companies, and, if you ask, only the last four digits of your Social Security number 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 Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See the section on "Correcting Fraudulent Information in Credit Reports" in the guide *Resolving Specific Identity Theft Problems* to learn how. When you correct your credit report, use an Identity Theft Report (discussed later in this guide) with a cover letter explaining your request, to get the fastest and most complete results. A sample cover letter to block fraudulent information in credit reports has been developed by the FTC, see

the “Helpful Resources” section at the end of this guide for information on how to access this document.

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.

## 2. Close 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 Social Security number or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or has 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 a cover letter 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. A sample cover letter for disputing fraudulent charges in existing accounts has been developed by the FTC, see the “Helpful Resources” section at the end of this guide for information on how to access this document.

- ◆ For new unauthorized accounts, you can either file a dispute directly with the company or file a report with the police and provide a copy, called an “Identity Theft Report,” to the company.

- If you want to file a dispute directly with the company, and do not want to file a report with the police, ask if the company accepts the FTC’s ID Theft Affidavit. If it does not, ask the representative to send you the company’s fraud dispute forms. See the “Helpful Resources” section at the end of this guide for information on how to access the FTC’s ID Theft Affidavit.
- However, filing a report with the police and then providing the company with an Identity Theft Report will give you greater protection. For example, if the company has already reported these unauthorized accounts or debts on your credit report, an Identity Theft Report will require them to stop reporting that fraudulent information. Use sample cover letter to dispute new unauthorized accounts developed by the FTC, to explain to the company the rights you have by using the Identity Theft Report. See the “Helpful Resources” section at the end of this guide for information on how to access this document. More information about getting and using an Identity Theft Report can be found in the guide *Resolving Specific Identity Theft Problems*.

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.

### 3. File a Complaint with the Federal Trade Commission

You can file a complaint with the FTC three ways:

- ◆ **Complete the online complaint form:**  
[www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov)
- ◆ **Call the Identity Theft Hotline:** toll-free: 877-ID-THEFT (438-4338); TTY: 1-866-653-4261
- ◆ **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.

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.

Additionally, you can provide a printed copy of your online Complaint form to the police to incorporate into their police report. The printed FTC ID Theft Complaint, in conjunction with the police report, can constitute an Identity Theft Report and entitle you to certain protections. This Identity Theft Report can be used to:

1. permanently block fraudulent information from appearing on your credit report
2. ensure that debts do not reappear on your credit report
3. prevent a company from continuing to collect debts that result from identity theft; and
4. place an extended fraud alert on your credit report.

### 4. File a Report with Your Local Police or the Police in the Community Where the Identity Theft Took Place

Call your local police department and tell them that you want to file a report about your identity theft. Ask them if you can file the report in person. If you cannot, ask if you can file a report over the Internet or telephone. See below for information about Automated Reports.

If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" 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 visit [www.naag.org](http://www.naag.org) for a list of state Attorneys General.

When you go to your local police department to file your report, bring a printed copy of your FTC ID Theft Complaint form (see the section "Instructions for Completing the ID Theft Complaint Form" in the guide *Filing a Complaint With The FTC* for more information), your cover letter, and your supporting documentation. The "Law Enforcement Cover Letter" developed by the FTC explains why a police report and an ID Theft Complaint are so important to victims. See the "Helpful Resources" section at the end of this guide for information on how to access this document.

Ask the officer to attach or incorporate the ID Theft Complaint into their police report. Tell them that you need a copy of the Identity Theft Report (the police report with your ID Theft Complaint attached or incorporated) to dispute the fraudulent accounts and debts created by the identity thief. (In some jurisdictions the officer will not be able to give you a copy of the official police report, but should be able to sign your Complaint and write the police report number in the "Law Enforcement Report" section.)

## What Is a Fraud Alert?

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

- ◆ **An initial fraud 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. With an initial fraud alert, potential creditors must use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. However, the steps potential creditors take to verify your identity may not always alert them that the applicant is not you. When you place an initial fraud alert on your credit report, you're entitled to order one free credit report from each of the three nationwide consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports.
- ◆ **An extended fraud 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. An automated Identity Theft Report, such as the printed ID Theft Complaint available from the FTC at [www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf](http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf), should be sufficient to obtain an extended fraud alert. With an extended fraud alert, potential creditors must actually contact you, or meet with you in person, before they issue you credit. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve 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, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

As mentioned, depending on the type of fraud alert you place, potential creditors must either contact you or take reasonable steps to verify your identity. 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.

## What Does a Fraud Alert Not Do?

While a fraud alert can help keep an identity thief from opening new accounts in your name, it's not a solution to all types of identity theft. It will not protect you from an identity thief using your existing credit cards or other accounts. It also will not protect you from an identity thief opening new accounts in your name that do not require a credit check—such as a telephone, wireless, or bank account. And, if there's identity theft already going on when you place the fraud alert, the fraud alert alone won't stop it. A fraud alert, however, can be extremely useful in stopping identity theft that involves opening a new line of credit.

## What Is a Credit Freeze?

Many states have laws that let consumers "freeze" their credit—in other words, letting a consumer restrict access to his or her credit report. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless

you temporarily lift the freeze. This means that it's unlikely that an identity thief would be able to open a new account in your name. Placing a credit freeze does not affect your credit score—nor does it keep you from getting your free annual credit report, or from buying your credit report or score.

Credit freeze laws vary from state to state. In some states, anyone can freeze their credit file, while in other states, only identity theft victims can. The cost of placing, temporarily lifting, and removing a credit freeze also varies. Many states make credit freezes free for identity theft victims, while other consumers pay a fee—typically \$10. It's also important to know that these costs are for each of the credit reporting agencies. If you want to freeze your credit, it would mean placing the freeze with each of three credit reporting agencies, and paying the fee to each one.

You can find more information about credit freeze laws specific to your state, including information on how to place one, by visiting [www.consumersunion.org/campaigns/learn\\_more/003484indiv.html](http://www.consumersunion.org/campaigns/learn_more/003484indiv.html).

### Who Can Access My Credit Report If I Place a Credit Freeze?

If you place a credit freeze, you will continue to have access to your free annual credit report. You'll also be able to buy your credit report and credit score even after placing a credit freeze. Companies that you do business with will still have access to your credit report—for example, your mortgage, credit card, or cell phone company—as would collection agencies that are working for one of those companies. Companies will also still be able to offer you prescreened credit. Those are the credit offers you receive in the mail that you have not applied for. Additionally, in some states, potential employers, insurance companies, landlords, and other non-creditors can still get access to your credit report with a credit freeze in place.

### Can I Temporarily Lift My Credit Freeze If I Need to Let Someone Check My Credit Report?

If you want to apply for a loan or credit card, or otherwise need to give someone access to your credit report and that person is not covered by an exception to the credit freeze law, you would need to temporarily lift the credit freeze. You would do that by using a PIN that each credit reporting agency would send once you placed the credit freeze. In most states, you'd have to pay a fee to lift the credit freeze. Most states currently give the credit reporting agencies three days to lift the credit freeze. (For information about credit freeze laws, visit [www.consumersunion.org/campaigns/learn\\_more/003484indiv.html](http://www.consumersunion.org/campaigns/learn_more/003484indiv.html).) This might keep you from getting “instant” credit, which may be something to weigh when considering a credit freeze.

### What Does a Credit Freeze *Not* Do?

While a credit freeze can help keep an identity thief from opening most new accounts in your name, it's not a solution to all types of identity theft. It will not protect you, for example, from an identity thief who uses your existing credit cards or other accounts. There are also new accounts, such as telephone, wireless, and bank accounts, which an ID thief could open without a credit check. In addition, some creditors might open an account without first getting your credit report. And, if there's identity theft already going on when you place the credit freeze, the freeze itself won't be able to stop it. While a credit freeze may not protect you in these kinds of cases, it can protect you from the vast majority of identity theft that involves opening a new line of credit.

## What's the Difference between a Credit Freeze and a Fraud Alert?

A fraud alert is another tool for people who've had their ID stolen—or who suspect it may have been stolen. With a fraud alert in place, businesses may still check your credit report. Depending on whether you place an initial 90-day fraud alert or an extended fraud alert, potential creditors must either contact you or use what the law refers to as “reasonable policies and procedures” to verify your identity before issuing credit in your name. However, the steps potential creditors take to verify your identity may not always alert them that the applicant is not you.

A credit freeze, on the other hand, will prevent potential creditors and other third parties from accessing your credit report at all, unless you lift the freeze or already have a relationship with the company. Some consumers use credit freezes because they feel they give more protection. As with credit freezes, fraud alerts are mainly effective against new credit accounts being opened in your name, but will likely not stop thieves from using your existing accounts, or opening new accounts such as new telephone or wireless accounts, where credit is often not checked. Also, only people who've had their ID stolen—or who suspect it may have been stolen—may place fraud alerts. In some states, anyone can place a credit freeze. For information about credit freeze laws, visit [www.consumersunion.org/campaigns/learn\\_more/003484indiv.html](http://www.consumersunion.org/campaigns/learn_more/003484indiv.html).

## What Is an Identity Theft Report?

An Identity Theft Report is a police report with more than the usual amount of detail. The Identity Theft Report includes enough detail about the crime for the credit reporting companies and the businesses involved to verify that you are a victim—and to know which accounts and inaccurate information came from identity theft. Normal police reports often don't have many details about the accounts that were opened or misused by identity thieves.

The printed copy of your ID Theft Complaint Form can provide additional details for the police report. The police are not legally required to use the FTC's ID Theft Complaint Form as part of their report. Your police department may have another way to incorporate the details of your crime. In these cases, the police report by itself may serve as an Identity Theft Report.

When you file your Identity Theft Report, the credit reporting companies will permanently block fraudulent information from appearing on your credit report. Filing an Identity Theft Report with the credit reporting companies or with the companies where the thief used your information should ensure that these debts do not reappear on your credit report. (For more information, please see the guide *Resolving Specific Identity Theft Problems*.) An Identity Theft Report can prevent a company from continuing to try to collect debts that result from identity theft, or sell those debts to others for collection. It also allows you to place an extended fraud alert on your credit report. The credit reporting companies may decline your Identity Theft Report if it does not contain enough detail for them to verify that you are a victim of identity theft. In that case, the credit reporting companies have certain timeframes (see below) for responding to your Identity Theft Report with requests for additional information.

Creating and using an Identity Theft Report may require two steps:

**Step One** begins with filing your report with a local, state, or federal law enforcement agency. These agencies may include your local police department, your State Attorney General, the FBI, the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service. Some state laws require local police departments to take reports, but there is no law requiring federal agencies to take a report.

In your report, you should give 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. It may help you give the necessary level of detail if you file an online complaint with the FTC, and then ask your local police department to incorporate a copy of the printed ID Theft Complaint into its police report.

**Step Two** begins when you send the businesses involved and the credit reporting companies a copy of your Identity Theft Report, which you should do by certified mail, return receipt requested. The companies may ask you to give them more information or documentation to help them verify your identity theft. They have to make their request within 15 days of receiving your Identity Theft Report. The credit reporting company or business then has 15 more days to work with you to make sure your Identity Theft Report contains everything they need. They are also entitled to five days to review any information you give them. For example, if you give them information 11 days after they request it, they have until day 16 to make a final decision.

### [How Do I Get an Identity Theft Report?](#)

The officer taking your police report can attach or incorporate your ID Theft Complaint into their police report to add more detail. Ask the officer to give you a copy of the official police report that incorporates or attaches your ID Theft Complaint. In some places the officer will not be able to give you a copy of the official police report, but should be able to sign a copy of your ID Theft Complaint and write the police report number in the “Law Enforcement Report” section. Be sure to keep a copy of the police report number

The police are not legally required to use the FTC’s ID Theft Complaint Form as part of their report. Your police department may have another way to include all the details of your identity theft information in their police report. In these cases, the police report by itself may serve as an Identity Theft Report.

Because the detailed Identity Theft Report is required for you to get many important protections, you may wish to use the “Law Enforcement Cover Letter” developed by the FTC to explain to the police department how important it is for you to get a police report—as well as the legal protections that a detailed Identity Theft Report gives you. See the “Helpful Resources” section at the end of this guide for information on how to access this document.

### [How Do I Submit My Identity Theft Report to the Credit Reporting Companies, or to Businesses Where the Thief Used My Information?](#)

When you send a copy of your Identity Theft Report to the fraud departments of the three major credit reporting companies, include a cover letter, along with copies of your supporting documentation. See the “Helpful Resources” section at the end of this guide for information on how to access a sample cover letter to block fraudulent information in credit reports. Send your information by certified mail with return receipt requested. The mailing addresses for sending Identity Theft Reports to the three major credit reporting companies are on the cover letter.

When writing to the fraud departments of each of the companies where the identity thief has committed fraud using your personal information, include copies of the Identity Theft Report, your supporting documentation, and the appropriate cover letter for fraud on your existing accounts, or for fraud on new accounts. See the “Helpful Resources” section at the end of this guide for information on how to access these documents. Always send this information by certified mail, with a return receipt requested.

The credit reporting companies have certain timeframes for responding to your Identity Theft Report with requests for additional information. See the section “What is an Identity Theft Report?” above for more information on timeframes.

### **What Do I Do If the Police Only Take Reports About Identity Theft over the Internet or Telephone?**

The FTC ID Theft Complaint has a special section for police reports that are not filed face-to-face, to help you use it to supplement an automated police report. If you file a police report online or over the phone, complete the “Automated Report Information” block of the ID Theft Complaint. Attach a copy of any filing confirmation received from the police.

If you have a choice, however, you should file your police report in person and not use an automated report. It is more difficult for the consumer reporting company and information provider to verify the information in an automated report, and they will likely require additional information and/or documentation.

### **What Do I Do If the Local Police Won't Take a Report?**

There are efforts at the federal, state and local levels to ensure that local law enforcement agencies understand identity theft, its impact on victims, and the importance of taking a police report. However, the FTC still hears that some departments are not taking reports. The following tips may help you to get a report if you're having difficulties:

- ◆ Provide the officer with a copy of the “Law Enforcement Cover Letter” developed by the FTC that explains why the police report and the Identity Theft Report are so important to both victims and industry. See the “Helpful Resources” section at the end of this guide for information on how to access this document.
- ◆ Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, a copy of your printed ID Theft Complaint, and other evidence of fraudulent activity can help demonstrate the legitimacy of your case. Provide the police a copy of “Remedying the Effects of Identity Theft,” which shows that police reports are necessary to secure your rights. See the “Helpful Resources” section at the end of this guide for information on how to access this document.
- ◆ Be persistent if local authorities tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Remind them that consumer reporting companies 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. In addition, a police report may be needed to obtain the fraudulent application and other records the company has.
- ◆ If you're told that identity theft is not a crime under your state law, ask to file a “Miscellaneous Incident Report” instead.
- ◆ 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.
- ◆ Some states require the police to take reports for identity theft. Check with the office of your State Attorney General, which can be found at [www.naag.org](http://www.naag.org), to find out if your state has this law.

## **How Do I Prove That I'm an Identity Theft 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, accompanied by a police report.

## **Getting Information from Businesses That Dealt with the Identity Thief**

You can request documents, at no cost to you, about the applications and fraudulent transactions made by the thief. You can request these documents from the businesses the thief dealt with. These documents can help you show that you did not apply for the account or make the transactions, and can help the police catch the thief. Among other documents that may be useful to you and the police are documents that show the thief's signature, or show which address the thief gave.

You must make your request to the business in writing, and you must demonstrate to the business that you are who you say you are (see below for more information). You must also demonstrate that you are an identity theft victim. You do that by providing the company with a copy of the police report, so be sure to get that from your police contact. Also, in your letter, you can request that the business provide the documents to you or to your law enforcement contact. The business must provide you with the records within 30 days after they receive your written request.

Before writing your letter, you should first call the company and ask two things: (1) to what address you should send your written request; and (2) what identification and other information does the company require.

Then, complete the "Request for Information on a Fraudulent Transaction" form letter developed by the FTC (see the "Helpful Resources" section at the end of this guide for information on how to access this document), make a copy for yourself, and mail it. We suggest mailing it by certified mail, return receipt requested.

As you complete the letter, please note the following: You'll need to insert your own information where it's requested. Also, be sure to give as complete a description as possible of the fraudulent transaction/account at the top of the form. And, if the business requires you to provide information different from that listed in A-C in the letter, simply substitute the type of information required by the company for the information listed.

## **Should I Apply for a New Social Security Number?**

Under certain circumstances, the Social Security Administration may issue you a new Social Security number—at your request—if, after trying to resolve the problems brought on by identity theft, you continue to experience problems. Consider this option carefully. A new Social Security number may not resolve your identity theft problems, and may actually create new problems. For example, a new Social Security number does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old Social Security number with those from your new Social Security number. Even when the old credit information is not associated with your new Social Security number, the absence of any credit history under your new Social Security number may make it more difficult for you to get credit. And finally, there's no guarantee that a new Social Security number wouldn't also be misused by an identity thief.

## Helpful Resources

### Federal Trade Commission

Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
877-IDTHEFT (877-438-4338)  
[www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft)  
[www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov) (Online complaint form)

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit [ftc.gov](http://ftc.gov) or call toll-free. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

The following sample documents can be downloaded from the FTC:

- ◆ **Sample Cover Letter to Dispute New Unauthorized Accounts:**  
[www.ftc.gov/bcp/edu/microsites/idtheft/downloads/dispute-letter-for-new-accounts.doc](http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/dispute-letter-for-new-accounts.doc)
- ◆ **“Law Enforcement Cover Letter”:**  
[www.ftc.gov/bcp/edu/microsites/idtheft/downloads/memorandum.pdf](http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/memorandum.pdf)
- ◆ **“Remedying the Effects of Identity Theft”:**  
[www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt09.pdf](http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt09.pdf)
- ◆ **Request for Information on a Fraudulent Transaction Form Letter:**  
[www.ftc.gov/bcp/edu/microsites/idtheft/downloads/Request-for-Fraudulent-Transaction.doc](http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/Request-for-Fraudulent-Transaction.doc)
- ◆ **Template for Recording Steps to Report Fraudulent Use of Your Identity**  
[www.ftc.gov/bcp/edu/resources/forms/chart-course-action.pdf](http://www.ftc.gov/bcp/edu/resources/forms/chart-course-action.pdf).
- ◆ **Sample Cover Letter to Block Fraudulent Information in Credit Reports:**  
[www.ftc.gov/bcp/edu/microsites/idtheft/downloads/blocking-letter-consumer-reporting-company.doc](http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/blocking-letter-consumer-reporting-company.doc)
- ◆ **Sample Cover Letter to Dispute Fraudulent Charges in Existing Accounts:**  
[www.ftc.gov/bcp/edu/microsites/idtheft/downloads/dispute-letter-for-existing-accounts.doc](http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/dispute-letter-for-existing-accounts.doc)
- ◆ **Identity Theft Affidavit:**  
[www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf](http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf)



Source: U.S. Federal Trade Commission

*This publication is for general informational purposes only and is not intended to provide any reader with specific authority, advice or recommendations.*

Copyright © 2009 LifeCare®, Inc. All rights reserved. LifeCare®, Inc. is the worldwide provider of Life Event Management® Services | [www.lifecare.com](http://www.lifecare.com)

#1156\_DefendRecoverfromIdentityTheft\_0309

