

# 2009 Identity Theft Guide



**GovAmerica**

FREE Federal, Military & Family Guides

[www.GovAmerica.org](http://www.GovAmerica.org)

# 2009 Identity Theft Guide

Published by GovAmerica.org

Publisher's Note: This FREE Guide is sponsored by WAEPA, a non-profit association governed by FEDERAL EMPLOYEES. Since 1943, over 100,000 federal employees – and their families – have been covered by WAEPA. WAEPA currently protects over 40,000 federal employees, and their families, with over \$9.1 billion of life insurance coverage.

For more details, just take a look at the WAEPA application in the back of this Guide or go to their website at <http://www.waepa.org>.

**WAEPA. Better Insurance. Better Prices. Better Value.**

FREE Federal, Military & Family Guides

[www.GovAmerica.org](http://www.GovAmerica.org)

Copyright © 2008-2009. GovAmerica.org, 8311 Wisconsin Avenue, Suite A-3, Bethesda, MD 20814. Telephone: 301-915-0901, Fax: 301-915-0902.

All rights reserved. No part of this book may be reproduced in any form or by any means without prior written permission from the Publisher. Printed in U.S.A.

“This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal, accounting or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.” – From a Declaration of Principles jointly adopted by a committee of the American Bar Association and a committee of publishers and associations.

# Contents

Safeguarding Your Social Security: An Overview.....	3
What to Do If You Are The Victim of Identity Theft .....	8
Steps to Respond and Recover .....	8
Charting Your Course of Action .....	12
Identity Theft Report.....	13
Fraud Alerts and Credit Freezes .....	15
Other Frequently Asked Questions .....	17
Resolving Specific Problems .....	20
Bank Accounts and Fraudulent Withdrawals .....	20
Correcting Fraudulent Information in Credit Reports .....	23
Credit Cards .....	25
Criminal Violations .....	26
Debt Collectors.....	27
Driver's License.....	28
Investment Fraud .....	28
Mail Theft .....	28
Passport Fraud.....	28
Phone Fraud .....	28
Social Security Number Misuse .....	29
Student Loans .....	29
Tax Fraud.....	29
Appendix .....	30
ID Theft Affidavit.....	31
Fraudulent Account Statement.....	35
Request for Fruadulent Transaction/Account Information.....	36

# 1

## Safeguarding Your Social Security Number

Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and do not pay the bills. You may not find out that someone is using your number until you are turned down for credit or you begin to get calls from unknown creditors demanding payment for items you never bought.

Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

### **Your Social Security Number is Confidential**

The Social Security Administration protects your Social Security number and keeps your records confidential. We do not give your number to anyone, except when authorized by law. You should be careful about sharing your number, even when you are asked for it. You should ask why your number is needed, how it will be used and what will happen if you refuse. The answers to these questions can help you decide if you want to give out your Social Security number.

### **How might someone steal your number?**

Identity thieves get your personal information by:

- Stealing wallets, purses and your mail (bank and credit card statements, pre-approved credit offers, new checks and tax information);
- Stealing personal information you provide to an unsecured site on the Internet, from business or personnel records at work and personal information in your home;
- Rummaging through your trash, the trash of businesses and public trash dumps for personal data;
- Posing by phone or E-mail as someone who legitimately needs information about you, such as employers or landlords; or

- Buying personal information from “inside” sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services or credit.

### **Be careful with your Social Security card and number**

Show your card to your employer when you start a job so your records are correct. Provide your Social Security number to your financial institution(s) for tax reporting purposes. Keep your card and any other document that shows your Social Security number on it in a safe place. **DO NOT** routinely carry your card or other documents that display your number.

### **What if you think someone is using your number?**

Sometimes more than one person uses the same Social Security number, either on purpose or by accident. If you suspect that someone else is using your number for work purposes, you should contact us to report the problem. We will review your earnings with you to ensure that our records are correct.

You also may review earnings posted to your record on your *Social Security Statement* (Form SSA-7005). The Statement is mailed automatically each year to workers age 25 and older. You also can get a Statement at any time by requesting one online or by calling our 800 number.

### **What is identity theft?**

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

The FTC estimates that as many as 9 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft. The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make – or until you're contacted by a debt collector.

Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

### **How do thieves steal an identity?**

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.

Skilled identity thieves may use a variety of methods to get hold of your information, including:

- **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.

- **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
- **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
- **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
- **Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
- **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

### **What do thieves do with a stolen identity?**

Once they have your personal information, identity thieves use it in a variety of ways. See later sections of this guide with specifics on what to do in each event.

#### Credit card fraud:

- They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

#### Phone or utilities fraud:

- They may open a new phone or wireless account in your name, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

#### Bank/finance fraud:

- They may create counterfeit checks using your name or account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic withdrawals your name, draining your accounts.
- They may take out a loan in your name.

#### Government documents fraud:

- They may get a driver's license or official ID card issued in your name but with their picture.

- They may use your name and Social Security number to get government benefits.
- They may file a fraudulent tax return using your information.

Other fraud:

- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

**How can you find out if your identity was stolen?**

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft.

Unfortunately, many consumers learn that their identity has been stolen after some damage has been done.

- You may find out when bill collection agencies contact you for overdue debts you never incurred.
- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.
- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

**What should you do if your identity is stolen?**

Filing a police report, checking your credit reports, notifying creditors, and disputing any unauthorized transactions are some of the steps you must take immediately to restore your good name.

**Should you file a police report if your identity is stolen?**

A police report that provides specific details of the identity theft is considered an Identity Theft Report, which entitles you to certain legal rights when it is provided to the three major credit reporting agencies or to companies where the thief misused your information. An Identity Theft Report can be used to permanently block fraudulent information that results from identity theft, such as accounts or addresses, from appearing on your credit report. It will also make sure these debts do not reappear on your credit reports. Identity Theft Reports can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to place an extended fraud alert on your credit report.

You may not need an Identity Theft Report if the thief made charges on an existing account and you have been able to work with the company to resolve the dispute. Where an identity thief

has opened new accounts in your name, or where fraudulent charges have been reported to the consumer reporting agencies, you should obtain an Identity Theft Report so that you can take advantage of the protections you are entitled to.

In order for a police report to entitle you to the legal rights mentioned above, it must contain specific details about the identity theft. You should file an ID Theft Complaint with the FTC and bring your printed ID Theft Complaint with you to the police station when you file your police report. The printed ID Theft Complaint can be used to support your local police report to ensure that it includes the detail required.

A police report is also needed to get copies of the thief's application, as well as transaction information from companies that dealt with the thief. To get this information, you must submit a request in writing, accompanied by the police report, to the address specified by the company for this purpose. You can find more information and a model letter here.

### **How long can the effects of identity theft last?**

It's difficult to predict how long the effects of identity theft may linger. That's because it depends on many factors including the type of theft, whether the thief sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit report.

Victims of identity theft should monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft.

Don't delay in correcting your records and contacting all companies that opened fraudulent accounts. Make the initial contact by phone, even though you will normally need to follow up in writing. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem.

### **What can you do to help fight identity theft?**

A great deal.

Awareness is an effective weapon against many forms identity theft. Be aware of how information is stolen and what you can do to protect yours, monitor your personal information to uncover any problems quickly, and know what to do when you suspect your identity has been stolen.

Armed with the knowledge of how to protect yourself and take action, you can make identity thieves' jobs much more difficult. You can also help fight identity theft by educating your friends, family, and members of your community. The FTC has prepared a collection of easy-to-use materials to enable anyone regardless of existing knowledge about identity theft to inform others about this serious crime.

# 2

## What to Do If You Are The Victim of Identity Theft

### Steps to Respond and Recover

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

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

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

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

Once you place the fraud alert in your file, you're entitled to order 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. When you correct your credit report, use an Identity Theft Report with a cover letter explaining your request, to get the fastest and most complete results.

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 the accounts that you know, or believe, have been tampered with or opened fraudulently

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

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your 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 the sample 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.
- 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 ID Theft Affidavit. If it does not, ask the representative to send you the company's fraud dispute forms.

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 the cover letter to explain to the company the rights you have by using the Identity Theft Report.

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 using the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Be sure to call the Hotline to update your complaint if you have any additional information or problems.

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:

- Permanently block fraudulent information from appearing on your credit report;
- Ensure that debts do not reappear on your credit report;
- Prevent a company from continuing to collect debts that result from identity theft;
- 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 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, your cover letter, and your supporting documentation. The cover letter explains why a police report and an ID Theft Complaint are so important to victims. 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.

### **Tips For Organizing Your Case**

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

- Have a plan when you contact a company. Don't assume that the person you talk to will give you all the information or help you need. Prepare a list of questions to ask the representative, as well as information about your identity theft. Don't end the call until you're sure you understand everything you've been told. If you need more help, ask to speak to a supervisor.
- Write down the name of everyone you talk to, what he or she tells you, and the date the conversation occurred. Use "Chart Your Course of Action" in the following pages to help keep you organized.
- Follow up in writing with all contacts you've made on the phone or in person. Use certified mail, return receipt requested, so you can document what the company or organization received and when.

- Keep copies of all correspondence or forms you send.
- Keep the originals of supporting documents, like police reports and letters to and from creditors; send copies only.
- Set up a filing system for easy access to your paperwork.
- Keep old files even if you believe your case is closed. Once resolved, most cases stay resolved, but problems can crop up.

## CHART YOUR COURSE OF ACTION

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

### NATIONWIDE CONSUMER REPORTING COMPANIES – REPORT FRAUD

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

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

Creditor	Address and Phone Number	Date Contacted	Contact Person	Comments

### LAW ENFORCEMENT AUTHORITIES – REPORT IDENTITY THEFT

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

## Identity Theft Report

*Note: Please see the Appendix of this guide for sample forms, affidavits, etc.*

- 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. 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 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 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.

- 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 copy of the credit reporting company cover letter, along with copies of your supporting documentation. 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. 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.

- 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 level to ensure that local law enforcement agencies understand identity theft, its impact on victims, and the importance of taking a police

report. However, we still hear that some departments are not taking reports. The following tips may help you to get a report if you're having difficulties:

1. Provide the officer with a copy of the Law Enforcement Cover Letter that explains why the police report and the Identity Theft Report are so important to both victims and industry.
2. 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.
3. 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.

### **Fraud Alerts and Credit Freezes**

- What is a fraud alert?

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

1. 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.
2. 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 this Web site, 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.

- 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. 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.

### **Other Frequently Asked Questions**

- 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. Use the model letter in the Appendix of this guide to request this information.

- 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.

- If your information has been compromised, but not yet misused

Having your information lost or stolen can be a frightening experience, because you may worry about how the information may be misused if it falls into the wrong hands. You might be in this situation if, for example, your wallet was stolen; you responded to a phishing email; or you were notified that a company experienced a data breach and lost some of your data. Fortunately, if your data may have been accessed without authorization, there are steps you can take to detect misuse that has already occurred and to help prevent potential future misuse.

If a company informs you that it experienced a breach and that some of your personal information has been compromised, the company may offer free credit monitoring. You should consider accepting this offer, as credit monitoring from a reputable company can help you quickly detect any misuse of your information.

Companies or institutions that keep personal information about you have an obligation to safeguard it. Still, from time to time, the personal information they hold may be accidentally disclosed or deliberately stolen. If your information falls into the wrong hands, it may be misused to commit fraud against you. If you get a notice that your personal information may have been compromised, taking certain steps quickly can minimize the potential for the theft of your identity.

If the stolen information includes your financial accounts, close compromised credit card accounts immediately. Consult with your financial institution about whether to close bank or brokerage accounts immediately or first change your passwords and have the institution monitor for possible fraud. Place passwords on any new accounts that you open. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers. If the stolen information includes your Social Security number, call the toll-free fraud number of any one of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. This alert can help stop someone from opening new credit accounts in your name. Please see the contact information for Equifax, Experian, and TransUnion earlier in this guide.

An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report with one nationwide consumer reporting company, you'll get information about ordering one free credit report from each of the companies. It's prudent to wait about a month after your information was stolen before you order your report. That's because suspicious

activity may not show up right away. Once you get your reports, review them for suspicious activity, like inquiries from companies you didn't contact, accounts you didn't open, and debts on your accounts that you can't explain. Check that information – like your SSN, address(es), name or initials, and employers – is correct.

If the stolen information includes your driver's license or other government-issued identification, contact the agencies that issued the documents and follow their procedures to cancel a document and get a replacement. Ask the agency to "flag" your file to keep anyone else from getting a license or another identification document in your name.

Once you've taken these precautions, watch for signs that your information is being misused. For example, you may not get certain bills or other mail on time. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks. Other signs include:

- Receiving credit cards that you didn't apply for;
- Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason; and
- Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

Continue to read your financial account statements promptly and carefully, and to monitor your credit reports every few months in the first year of the theft, and once a year thereafter. If your information has been misused, follow the instructions earlier in this guide regarding Identity Theft.

# 3

## Resolving Specific Problems

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

### **Bank Accounts and Fraudulent Withdrawals**

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

### **Fraudulent Electronic Withdrawals**

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

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

- If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how quickly you report the loss.
- If you report the loss or theft within two business days of discovery, your losses are limited to \$50.
- If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to \$500 of what the thief withdraws.
- If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days.

Note: 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.

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

After receiving your notification about an error on your statement, the institution generally has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that it occurred. If the institution needs more time, it may take up to 45 days to complete the investigation but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

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

You can contact major check verification companies directly to request that they notify retailers who use their databases not to accept your checks:

- TeleCheck at 1-800-710-9898 or 1-800-927-0188
- Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120
- To find out if the identity thief has been passing bad checks in your name, call SCAN: 1-800-262-7771

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

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

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

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

### **Fraudulent New Accounts**

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

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

### **Where to Find Help**

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

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

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

### 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, including savings banks and savings and loan institutions.

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

### Bankruptcy Fraud U.S. Trustee (UST)

[www.usdoj.gov/ust](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' Regional Offices is available on the UST website, or check the Blue Pages of your phone book under U.S. Government Bankruptcy Administration.

In your letter, describe the situation and provide proof of your identity. The U.S. Trustee will make a criminal referral to law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed. The U.S. Trustee does not provide legal representation, legal advice, or referrals to lawyers. That means you may need to hire an attorney to help convince the bankruptcy court that the filing is fraudulent. The U.S. Trustee does not provide consumers with copies of court documents. You can get them from the bankruptcy clerk's office for a fee.

### **Correcting Fraudulent Information in Credit Reports**

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

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

your rights under the law, contact both the consumer reporting company and the information provider.

### Consumer Reporting Company Obligations

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

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

The blocking process is only one way for identity theft victims to deal with fraudulent information. There's also the "reinvestigation process," which was designed to help all consumers dispute errors or inaccuracies on their credit reports

### Information Provider Obligations

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

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

**Sample Blocking Letter Consumer Reporting Company**

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

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

Dear Sir or Madam:

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

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

Sincerely,  
Your name

Enclosures: (List what you are enclosing.)

### **Credit Cards**

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

- Write to the creditor at the address given for "billing inquiries," NOT the address for sending your payments. Include your name, address, account number, and a description of the billing error, including the amount and date of the error. See Sample Letter.
- Send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. If an identity thief changed the address on your account and you didn't receive the bill, your dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill. This is one reason it's essential to keep track of your billing statements, and follow up quickly if your bills don't arrive on time.

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

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

### Sample Dispute Letter For Existing Accounts

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

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

Dear Sir or Madam:

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

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

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

### Criminal Violations

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

If wrongful criminal violations are attributed to your name, contact the police or sheriff's department that originally arrested the person using your identity, or the court agency that issued the warrant for the arrest. File an impersonation report with the police/sheriff's department or the court, and confirm your identity: Ask the police department to take a full set of your fingerprints, photograph you, and make a copies of your photo identification documents, like your driver's license, passport, or travel visa. To establish your innocence, ask the police to compare the prints and photographs with those of the imposter.

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

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

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

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

### **Debt Collectors**

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

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

1. Write a letter to the collection agency telling them to stop. Once the debt collector receives your letter, the company may not contact you again with two exceptions: They can tell you there will be no further contact, and they can tell you that the debt collector or the creditor intends to take some specific action.
2. Send a letter to the collection agency, within 30 days after you received written notice of the debt, telling them that you do not owe the money. Include copies of documents that support your position. Including a copy (NOT original) of your police report may be useful. In this case, a collector can renew collection activities only if it sends you proof of the debt.

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

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

While you can stop a debt collector from contacting you, that won't get rid of the debt itself. It's important to contact the company that originally opened the account to dispute the debt,

otherwise that company may send it to a different debt collector, report it on your credit report, or initiate a lawsuit to collect on the debt.

### **Driver's License**

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

### **Investment Fraud**

#### U.S. Securities and Exchange Commission (SEC)

[www.sec.gov](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's Complaint Center at [www.sec.gov/complaint.shtml](http://www.sec.gov/complaint.shtml). Include as much detail as possible. If you don't have Internet access, write to the SEC at: SEC Office of Investor Education and Assistance, 450 Fifth Street, NW, Washington DC, 20549-0213. For answers to 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)

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

You can locate the USPIS district office nearest you by calling your local post office, checking the Blue Pages of your telephone directory.

### **Passport Fraud**

#### United States Department of State (USDS)

[www.travel.state.gov/passport/passport\\_1738.html](http://www.travel.state.gov/passport/passport_1738.html)

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

### **Phone Fraud**

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

removed from your account or getting an unauthorized account closed, contact the appropriate agency below.

- For local service, contact your state Public Utility Commission.
- For cellular phones and long distance, contact the Federal Communications Commission (FCC) at [www.fcc.gov](http://www.fcc.gov). The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable. Call: 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554.

### **Social Security Number Misuse**

Social Security Administration (SSA)

[www.ssa.gov](http://www.ssa.gov)

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

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

### **Student Loans**

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

### **Tax Fraud**

Internal Revenue Service (IRS)

[www.treas.gov/irs/ci](http://www.treas.gov/irs/ci)

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

If you have an unresolved issue related to identity theft, or you have suffered or are about to suffer a significant hardship as a result of the administration of the tax laws, visit the IRS Taxpayer Advocate Service website [www.irs.gov/advocate/](http://www.irs.gov/advocate/) or call toll-free: 1-877-777-4778. If you suspect or know of an individual or company that is not complying with the tax law, report it to the Internal Revenue Service Criminal Investigation Informant Hotline by calling toll-free: 1-800-829-0433 or visit [www.irs.gov](http://www.irs.gov) and type in the IRS key word "Tax Fraud."

# 4

## Appendix:

- ID Theft Affidavit
- Fraudulent Account Statement
- Request for Fraudulent Transaction/Account Information)

Name \_\_\_\_\_ Phone number \_\_\_\_\_ Page 1

## ID Theft Affidavit

### Victim Information

- (1) My full legal name is \_\_\_\_\_  
(First) (Middle) (Last) (Jr., Sr., III)
- (2) (If different from above) When the events described in this affidavit took place, I was known as \_\_\_\_\_  
(First) (Middle) (Last) (Jr., Sr., III)
- (3) My date of birth is \_\_\_\_\_  
(day/month/year)
- (4) My Social Security number is \_\_\_\_\_
- (5) My driver's license or identification card state and number are \_\_\_\_\_
- (6) My current address is \_\_\_\_\_  
City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_
- (7) I have lived at this address since \_\_\_\_\_  
(month/year)
- (8) (If different from above) When the events described in this affidavit took place, my address was \_\_\_\_\_  
City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_
- (9) I lived at the address in Item 8 from \_\_\_\_\_ until \_\_\_\_\_  
(month/year) (month/year)
- (10) My daytime telephone number is (\_\_\_\_\_) \_\_\_\_\_  
My evening telephone number is (\_\_\_\_\_) \_\_\_\_\_

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

Name \_\_\_\_\_ Phone number \_\_\_\_\_ Page 2

**How the Fraud Occurred**

**Check all that apply for items 11 - 17:**

- (11)  I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.
- (12)  I did not receive any benefit, money, goods or services as a result of the events described in this report.
- (13)  My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were  stolen  lost on or about \_\_\_\_\_  
(day/month/year)
- (14)  To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

\_\_\_\_\_  
Name (if known)

\_\_\_\_\_  
Name (if known)

\_\_\_\_\_  
Address (if known)

\_\_\_\_\_  
Address (if known)

\_\_\_\_\_  
Phone number(s) (if known)

\_\_\_\_\_  
Phone number(s) (if known)

\_\_\_\_\_  
Additional information (if known)

\_\_\_\_\_  
Additional information (if known)

- (15)  I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.
- (16)  Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

(Attach additional pages as necessary.)

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

**Victim's Law Enforcement Actions**

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

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

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

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

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

**Documentation Checklist**

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

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

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

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

Name \_\_\_\_\_ Phone number \_\_\_\_\_ Page 4

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

**Signature**

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

\_\_\_\_\_  
(signature)

\_\_\_\_\_  
(date signed)

\_\_\_\_\_  
(Notary)

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

**Witness:**

\_\_\_\_\_  
(signature)

\_\_\_\_\_  
(printed name)

\_\_\_\_\_  
(date)

\_\_\_\_\_  
(telephone number)

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

Name \_\_\_\_\_ Phone number \_\_\_\_\_ Page 5

## Fraudulent Account Statement

### Completing this Statement

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

**I declare (check all that apply):**

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

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

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

Billing name \_\_\_\_\_

Billing address \_\_\_\_\_

Account number \_\_\_\_\_

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

**Request for Fraudulent Transaction/Account Information  
Made pursuant to Section 609(e) of the Fair Credit Reporting Act  
(15 U.S.C. § 1681(g))**

To:  
Account Number:  
Description of fraudulent transaction/account:

From:           [Name]  
                  [Address]  
                  [Telephone Number]

As we discussed on the phone, I am a victim of identity theft. The thief made a fraudulent transaction or opened a fraudulent account with your company. Pursuant to federal law, I am requesting that you provide me, at no charge, copies of application and business records in your control relating to the fraudulent transaction. A copy of the relevant federal law is enclosed.

Pursuant to the law, I am providing you with the following documentation, so that you can verify my identity:

- (A) A copy of my driver's license or other government-issued identification card; and
- (B) A copy of the police report about the identity theft; and
- (C) A copy of the identity theft affidavit, on the form made available by the Federal Trade Commission.

Please provide all information relating to the fraudulent transaction, including:

- Application records or screen prints of Internet/phone applications
- Statements
- Payment/charge slips
- Investigator's summary
- Delivery addresses
- All records of phone numbers used to activate the account or used to access the account
- Any other documents associated with the account.

Please send the information to me at the above address. In addition, I am designating a law enforcement officer to receive the information from you. This officer is investigating my case. The law enforcement officer's name, address and telephone number is: [insert]. Please also send all documents and information to this officer.

Enclosure: Section 609(e) of the Fair Credit Reporting Act (15 U.S.C. § 1681(g))

**ENCLOSURE:**  
**FCRA 609(e) (15 U.S.C. § 1681g(e)) Disclosures to Consumers –**  
**Information Available to Victims**

(e) Information available to victims

(1) In general

For the purpose of documenting fraudulent transactions resulting from identity theft, not later than 30 days after the date of receipt of a request from a victim in accordance with paragraph (3), and subject to verification of the identity of the victim and the claim of identity theft in accordance with paragraph (2), a business entity that has provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, shall provide a copy of application and business transaction records in the control of the business entity, whether maintained by the business entity or by another person on behalf of the business entity, evidencing any transaction alleged to be a result of identity theft to--

**(A)** the victim;

**(B)** any Federal, State, or local government law enforcement agency or officer specified by the victim in such a request; or

**(C)** any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of records provided under this subsection.

(2) Verification of identity and claim

Before a business entity provides any information under paragraph (1), unless the business entity, at its discretion, otherwise has a high degree of confidence that it knows the identity of the victim making a request under paragraph (1), the victim shall provide to the business entity--

**(A)** as proof of positive identification of the victim, at the election of the business entity--

**(i)** the presentation of a government-issued identification card;

**(ii)** personally identifying information of the same type as was provided to the business entity by the unauthorized person; or

**(iii)** personally identifying information that the business entity typically requests from new applicants or for new transactions, at the time of the victim's request for information, including any documentation described in clauses (i) and (ii); and

**(B)** as proof of a claim of identity theft, at the election of the business entity--

**(i)** a copy of a police report evidencing the claim of the victim of identity theft; and

**(ii)** a properly completed--

**(I)** copy of a standardized affidavit of identity theft developed and made available by the Commission; or

**(II)** an affidavit of fact that is acceptable to the business entity for that purpose.

(3) Procedures

The request of a victim under paragraph (1) shall--

**(A)** be in writing;

**(B)** be mailed to an address specified by the business entity, if any; and

**(C)** if asked by the business entity, include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including--

**(i)** if known by the victim (or if readily obtainable by the victim), the date of the application or transaction; and

**(ii)** if known by the victim (or if readily obtainable by the victim), any other identifying information such as an account or transaction number.

(4) No charge to victim

Information required to be provided under paragraph (1) shall be so provided without charge.

(5) Authority to decline to provide information

A business entity may decline to provide information under paragraph (1) if, in the exercise of good faith, the business entity determines that--

**(A)** this subsection does not require disclosure of the information;

**(B)** after reviewing the information provided pursuant to paragraph (2), the business entity does not have a high degree of confidence in knowing the true identity of the individual requesting the information;

**(C)** the request for the information is based on a misrepresentation of fact by the individual requesting the information relevant to the request for information; or

**(D)** the information requested is Internet navigational data or similar information about a person's visit to a website or online service.

(6) Limitation on liability

Except as provided in section 1681s of this title, sections 1681n and 1681o of this title do not apply to any violation of this subsection.

(7) Limitation on civil liability

No business entity may be held civilly liable under any provision of Federal, State, or other law

for disclosure, made in good faith pursuant to this subsection.

(8) No new recordkeeping obligation

Nothing in this subsection creates an obligation on the part of a business entity to obtain, retain, or maintain information or records that are not otherwise required to be obtained, retained, or maintained in the ordinary course of its business or under other applicable law.

(9) Rule of construction

(A) In general

No provision of subtitle A of title V of Public Law 106-102, prohibiting the disclosure of financial information by a business entity to third parties shall be used to deny disclosure of information to the victim under this subsection.

(B) Limitation

Except as provided in subparagraph (A), nothing in this subsection permits a business entity to disclose information, including information to law enforcement under subparagraphs (B) and (C) of paragraph (1), that the business entity is otherwise prohibited from disclosing under any other applicable provision of Federal or State law.

(10) Affirmative defense

In any civil action brought to enforce this subsection, it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) for a business entity to file an affidavit or answer stating that--

**(A)** the business entity has made a reasonably diligent search of its available business records; and

**(B)** the records requested under this subsection do not exist or are not reasonably available.

(11) Definition of victim

For purposes of this subsection, the term "victim" means a consumer whose means of identification or financial information has been used or transferred (or has been alleged to have been used or transferred) without the authority of that consumer, with the intent to commit, or to aid or abet, an identity theft or a similar crime.

(12) Effective date

This subsection shall become effective 180 days after December 4, 2003.

(13) Effectiveness study

Not later than 18 months after December 4, 2003, the Comptroller General of the United States shall submit a report to Congress assessing the effectiveness of this provision.

# WAEPA Life Insurance

For Civilian Federal Employees and Their Families

## Better Insurance

WAEPA	FEGLI
<b>Member Coverage</b> \$25,000 up to \$750,000 (in \$25,000 increments)	<b>Member Coverage</b> Your Basic coverage is determined by your annual pay.
<b>Dependent Coverage</b> <b>Spouse/Domestic Partner</b> \$10,000 up to \$250,000 (in \$10,000 increments)	<b>Dependent Coverage</b> <b>Spouse</b> Option C is \$5,000 up to \$25,000 (in \$5,000 increments)
<b>Children</b> \$1,000 up to \$25,000	<b>Children</b> \$2,500 up to \$12,500 (in \$2,500 increments)

## Better Prices

Prices based on bi-weekly premiums per \$1,000 of coverage.

Member's Age	WAEPA	FEGLI Basic	Basic Coverage Savings
25	2.3¢	15.0¢	85%
30	2.6¢	15.0¢	85%
35	3.1¢	15.0¢	79%
40	4.3¢	15.0¢	71%
45	6.2¢	15.0¢	59%
50	9.4¢	15.0¢	37%
55	14.3¢	15.0¢	5%
60	24.2¢	15.0¢	-

## Better Value

- Premium Refunds: over \$39 million since 1996. In September 2008 alone WAEPA members received \$5.7 million in refunds.
- WAEPA College Scholarship Program: for children of WAEPA Life Insurance policyholders

## WAEPA Eligibility Requirements

You're eligible if you're currently a non-military government or Postal Service employee, you are less than 65 years old, and you are a U.S. citizen.

You're also eligible if you are a former non-military federal employee, under age 65, currently receiving a government retirement annuity.

## Act Today!

Complete the enclosed application to protect your family and start saving with WAEPA.

**For a Complete Listing of Benefits and Rates, please visit**

[www.waepa.org](http://www.waepa.org)

or call 1-800-368-3484



**Underwritten by the following CIGNA companies:**

Life Insurance Company of North America (LINA)  
 Connecticut General Life Insurance Company (CG)  
 CIGNA Companies (herein called the Insurance Company)

PLEASE COMPLETE PAGES 2, 3 & 4 OF THIS APPLICATION AND SIGN.

APPLICANT INFORMATION					
LIST BELOW ONLY INDIVIDUALS APPLYING FOR COVERAGE	RELATIONSHIP (TO APPLICANT)	BIRTH DATE (MM/DD/YY)	AGE	HEIGHT (FT. IN.)	WEIGHT (LBS.)
APPLICANT (Full Name)					
ELIGIBLE DEPENDENTS (Full Names)					

**HEALTH QUESTIONS SECTION A**

**Within the last five years, have you or your eligible dependents been:**

- diagnosed with any of the conditions shown in items A through J below,
  - told by a medical professional he/she has, or may have, any of the conditions shown in items A through J below,
  - or been treated by a medical professional for any of the conditions shown in items A through J below?
- A. High blood pressure, heart attack, chest pain or Angina, a heart murmur, poor circulation, or any other condition affecting the heart or circulatory system? .....  Yes **or**  No
- B. Diabetes, glandular condition, Hepatitis, or any condition affecting the esophagus, stomach, intestines, liver, or pancreas? .....  Yes **or**  No
- C. Asthma, Chronic Bronchitis, Emphysema, or any other condition affecting the lungs or respiratory tract? .....  Yes **or**  No
- D. Any condition affecting the kidneys, urinary tract, prostate gland, or reproductive system? .....  Yes **or**  No
- E. HIV infection, AIDS, or any other condition affecting the immune system or lymph nodes? .....  Yes **or**  No
- F. Stroke, Transient Ischemic Attack (TIA), Alzheimer's disease, paralysis, epilepsy, fainting, seizures, headaches, or other condition affecting the nervous system? .....  Yes **or**  No
- G. Anemia or any other condition affecting the blood, Lupus, Arthritis, deformity, or loss of limb? .....  Yes **or**  No
- H. Anxiety, Depression, Bipolar Disorder, or any other mental disorder or condition? .....  Yes **or**  No
- I. Cancer, Tumor, Leukemia, Hodgkin's Disease, Polyps, or Moles? .....  Yes **or**  No
- J. Alcohol or drug abuse or dependency? .....  Yes **or**  No

**HEALTH QUESTIONS SECTION B**

**Within the last five years, have you or your eligible dependents:**

- A. Used any controlled or illegal drug or other substance? .....  Yes **or**  No
- B. Been seen for, or been advised to have sought treatment for, observation and/or consultation for surgery, medical examination, and/or tests, such as blood, urine, X-rays, electrocardiograms, scans, biopsies, or any medical tests/exams not listed here or above, other than normal routine physical exams? .....  Yes **or**  No
- C. Used any medication prescribed by a physician or other medical practitioner, or used any form of alternative and complementary medical treatment or remedy, including herbs or acupuncture? .....  Yes **or**  No
- D. Been seen, sought treatment for, consulted, advised they had and/or received any medical advice from a health care practitioner for any disease, disorder and/or medical impairment not listed above? .....  Yes **or**  No

PHYSICIAN SECTION			
	Name	Contact Information	Street Address (City, State, & Zip)
<b>Applicant Physician</b>		Tel# Fax#	
<b>Spouse/Domestic Partner Physician</b>		Tel# Fax#	
<b>Child(ren) Physician</b>		Tel# Fax#	

**Caution:** Any person who knowingly and with intent to defraud any insurance company or other person: (1) files an application for insurance or statement of claim containing any materially false information; or (2) conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act.

USE THE SPACE BELOW TO EXPLAIN "YES" ANSWERS. IF MORE SPACE IS NEEDED, USE A NEW PAGE, SIGN AND DATE IT AND ATTACH TO THIS FORM.

Name of Person	Condition	Date Occurred	Duration/Treatment Received	Current Status

**AGREEMENTS AND AUTHORIZATION**

To the best of my knowledge and belief, all written, telephonic, and electronic information I gave is true and complete. I also understand that coverage for each of my dependents will not go into effect if a dependent is confined in a hospital or institution. The conditions for the requested insurance to be effective are described in the policy and certificate. The approval of this request by the Insurance Company is one of those conditions. I understand and agree that:

- (1) This request will be a part of the policy that provides the insurance.
- (2) I may need to provide more medical information.
- (3) I may need to take medical tests and report the results to the Insurance Company.
- (4) My dependent(s) may need to take medical tests. The results of those tests must be reported to the Insurance Company.
- (5) I must report any change in my health, or of a dependent for whom coverage is requested, that happens before the insurance is effective.
- (6) Requested insurance will not be effective for a person if the person does not meet the underwriting requirements on the date insurance is to be effective.

**AUTHORIZATION**

I permit any hospital, clinic, health care practitioner, pharmacy, benefit manager, employer, insurance company, or any other person or organization having information about the health, medical history, physical or mental condition, diagnosis or treatment, employment or income, or motor vehicle driving record, of me or my children to disclose to the Insurance Company or its authorized agent, any such information, for the purpose of underwriting this application for insurance or administering any claim under any insurance which is approved. This authorization is valid for 30 months from the date below. I accept that a copy of this Authorization is as valid as the original.

I understand that I and/or my authorized agent have the right to receive a copy of this authorization upon request.

I understand that the information will be used to assess my request for insurance.

I may revoke this authorization at any time in writing. Any such revocation will not: (1) change any action taken in reliance on the Authorization; and (2) change the Insurance Company's right to use the Authorization for contest of a claim or policy in accordance with the applicable law.

I understand that the information provided pursuant to this authorization may be disclosed by the recipient and is no longer subject to the protections of the Health Insurance Portability and Accountability Act (HIPAA). (The Insurance Companies are subject to the Gramm-Leach-Bliley act and state privacy laws. They do not disclose protected information except as permitted by those laws.)

X \_\_\_\_\_  
 Applicant's Signature Date

X \_\_\_\_\_  
 Signature of Spouse/Domestic Partner (if applying) Date

Notice: Personal information may be collected from persons other than those proposed for coverage. Information may be disclosed to third parties without your authorization as permitted by law. You have the right to access and correct all personal information collected. Additional information about the insurance company's privacy practices is available upon request.