

## Identity Theft Crime Victim Assistance Kit

### INTRODUCTION

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

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

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

### HOW IDENTITY THEFT OCCURS

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

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

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

How identity thieves get your personal information:

They get information from businesses or other institutions by:

- stealing records or information while they're on the job
- bribing an employee who has access to these records
- hacking these records
- conning information out of employees

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

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

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

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

They may steal your wallet or purse.

They may complete a “change of address form” to divert your mail to another location.

They may steal personal information they find in your home.

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

How identity thieves use your personal information:

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

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

They may establish phone or wireless service in your name.

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

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

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

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

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

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

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

## If Your Personal Information Has Been Lost or Stolen

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

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

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

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

Once you've taken these precautions, watch for signs that your information is being misused.

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

## IDENTITY THEFT VICTIMS: IMMEDIATE STEPS

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

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

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact

one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241

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

TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your SSN will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your SSN, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

## Fraud Alerts

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

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

An extended alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "identity theft report." 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 SSN, name, address and other personal information requested by the consumer reporting company.

When a business sees the alert on your credit report, they must verify your identity before

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

## **2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.**

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

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

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

For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. Write to the company at the address given for "billing inquiries," NOT the address for sending your payments.

For new unauthorized accounts, ask the representative to send you the company's fraud dispute forms. If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information.

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

## **Proving You're a Victim**

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

may give permission to any law enforcement agency to get these records, or ask in your written request that a copy of these records be sent to a particular law enforcement officer.

The company can ask you for:

Proof of your identity: This may be a photocopy of a government-issued ID card, (the same type of information the identity thief used to open or access the account, or the type of information the company usually requests from applicants or customers) a police report and a completed affidavit.

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

Then, get a copy of the police report or at the very least, the number of the report. It can help you deal with creditors who need proof of the crime.

### **4. File a complaint with the Federal Trade Commission.**

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

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

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

## **The Identity Theft Report**

An identity theft report may have two parts:

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

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

Part Two of an identity theft report depends on the policies of the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company). That is, they may ask you to provide information or documentation in addition to that included in the law enforcement report which is reasonably intended to verify your identity theft.

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

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

## Tips For Organizing

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** to help you.

Follow up in writing with all contacts you’ve made on the phone or in person. Use certified mail, return receipt requested, so you can document what the company or organization received and when.

Keep copies of all correspondence or forms you send.

Keep the originals of supporting documents, like police reports and letters to and from creditors; send copies only.

Set up a filing system for easy access to your paperwork.

Keep old files even if you believe your case is closed. Once resolved, most cases stay resolved, but problems can crop up.

Chart Your Course of Action [PDF version of form]

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 Agency	Phone Number	Date Contracted	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 & Phone Number	Date Contacted	Contact Person	Comments

**Law Enforcement Authorities – Report Identity Theft**

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