



Please feel free to forward this e-book to friends or associates, or to include it in your website, as long as you do not change its content or links in any way.

To save this to your hard drive, click the disk icon on the Acrobat toolbar. (No downloading required.)

Identity Theft Self-Protection Kit

- ✓ Home
- ✓ Site Directory
- ✓ How To Locate People
- ✓ About Washington Research Associates
- ✓ Contact Us

CONTENTS:

- I. What Identity Theft Is
- II. Types of Identity Thieves
- III. What to Do if It Happens to You
- IV. Self-Protection Measures
- V. Sample Forms and Letters

Please note: Some links in this e-book are to web documents and require you to be connected to the internet.

I. WHAT IDENTITY THEFT IS

Identity theft, in simplest terms, is the use of your identity without your knowledge in order to secure credit. That is, to borrow money or purchase goods and services.

Today, identity theft is America's major white-collar crime, and it's growing fast, thanks in part to the ready availability of personal information on all of us via the Internet.

You're very wise to take a few moments to study the subject here and learn how to protect yourself against its happening to you.

If it does happen to you, it can turn your life upside down overnight.

II. TYPES OF IDENTITY THIEVES

There are two main types of identity thieves, namely, identity theft rings and individual identity thieves.

Identity theft rings operate using a hit-and-run strategy. They appear suddenly in an area, set up their operation, identify potential victims, burn out their victims' credit, then shut down and disappear.

How do these rings identify potential victims? Often, they target high-income individuals, such as people who own expensive homes or cars or are members of high-income professions, such as doctors or lawyers. Or they may target a group of individuals whose personal information is relatively easy to gather, such as college professors, government employees, or real estate brokers.

Once the ring has identified its group of targets, it then hires an information broker to obtain their social security numbers -- which is a simple matter of running their names through credit bureau files using what's called a "[national identifier search](#)."

As a rule, people whose social security numbers are found to be less than readily obtainable are dropped from the list of targets. After all, why bother, when there are so many millions of easy victims?

Armed with social security numbers, the ring will then apply for credit cards, loans, lines of credit, and checking accounts in the names of the targets. It will have the credit applications, credit cards, and checking account applications mailed to a phony address, perhaps a small apartment rented in advance.

Once the credit cards and blank checks start pouring in, the members of the ring go to work buying expensive merchandise (stereo and computer equipment and jewelry are favorites) and obtaining cash via bank credit lines or by cashing bad checks. Merchandise accumulated will be fenced or sold to pawn shops.

Very soon -- before the credit card bills start arriving and the checks start bouncing -- the ring will collapse its operation and move on to a new area and a new list of targets.

The other type of identity thief is the individual who, working alone, impersonates someone else in order to obtain credit.

This type of identity thief can be just as devastating to you and your good credit standing as the organized crime ring described previously.

An individual may get into this racket on either a short- or long-term basis. The short-term identity thief is looking for a boost in his or her standard of living and finds it by running up bills or obtaining cash using somebody else's credit. The long-term identity thief takes the scam a step further -- he or she essentially starts a whole new life somewhere far away using the credit history and/or employment history of the victim; in this case, oddly enough, there may be no financial loss to the target, for the identity thief is looking for a new start in life and will usually pay the bills he runs up on the credit lines he's been able to establish in the victim's name. Nonetheless, should he ever default on his obligations, he can destroy the credit of the person whose identity he is using.

Furthermore, whether the thief is in it for a quick killing (the short-term thief) or for a whole new start in life (the long-term thief), the victim is at serious personal risk. For example, suppose an identity thief commits a crime -- or even a serious traffic violation -- while impersonating a victim, possibly by means of a fake driver's license or other forged document. It's quite possible, and has frequently happened, that the victim will then be arrested and charged with the crime or other offense perpetrated by the identity thief!

III. WHAT TO DO IF IT HAPPENS TO YOU

Your first indication that you've been a victim of identity theft will probably be the arrival in your mail of a bill for merchandise you don't remember ordering or a call from a merchant complaining about a bad check or an invoice that never got paid. If this happens to you, immediately gather as much information from the caller as you can, such as when the purchase or loan took place, type of credit used (credit line or credit card), account number, monetary amount, where bills were sent. If a credit application was filled out, ask to obtain a copy of it. Explain to the merchant exactly what's happened, i.e., that you did not make the purchase or authorize the account, and ask to be removed from his list of delinquent debtors and that he not report it to the credit bureau in your name. Be sure to use the phrase "identity theft" -- it's such a widespread crime nowadays that it will leave no doubt in his mind as to what you're talking about.

You should then follow up this conversation with a letter; a [sample letter](#) for this purpose is provided in Section V.

At this point, having discovered that you've been victimized, it's important to act quickly to minimize the damage to your credit standing.

Start by immediately contacting all three major credit bureaus. Their numbers are:

Equifax (404) 885-8000 [main number]; (800) 525-6285 [fraud hotline]
Experian (888) 397-3742 [main number and fraud hotline]
Trans Union (800) 916-8800 [main number and fraud hotline]

Have a list of all your credit accounts and account numbers at hand when you call. You'll need to go through your credit report with the credit bureau representatives to identify accounts which are fraudulent. Instruct the representatives that each of those identified as fraudulent should be immediately deleted from your file. (Obtain the name, phone number and complete office address of each credit bureau rep you talk to and write it all down; you'll need it later.)

Ask the reps for names, addresses, and phone numbers corresponding to all fraudulent accounts. You will need to contact each of these businesses and inform them that you've been a victim of identity theft. You should contact each one both by phone and confirm your conversations with follow-up letters (See Section V for a [sample letter](#)).

Also, have the credit bureau representatives mail you a copy of your credit report, with the fraudulent accounts indicated. And as soon as you're off the phone to the reps, write follow-up letters to each of them, documenting your conversations (See Section V for a [sample letter](#)).

Thus follow-up letters should be sent both to the credit bureaus and to the individual merchants and bankers you talk to.

Within a week you should have your credit reports in the mail with the fraudulent accounts indicated, as you asked. These reports provide evidence that you've been defrauded. Take these documents to your local police station and file a formal police report. Keep the report with you; as pointed out above, it's quite possible you'll be charged with a crime -- such as passing bad checks -- perpetrated by the identity thief. The police report will go a long way in convincing the police that your "identity theft" story is true!

Having done all of the above, you still have several important tasks ahead of you to prevent this incident from turning into a real nightmare:

1. Recognizing that the identity thief may well have opened checking accounts in your name, you need to contact the major check-guarantee agencies (listed below). First, you have to inform them that you've been the victim of identity theft so they'll refuse to guarantee bad checks in your name (i.e., checks on accounts you did not open) in the future. Second, you need to have them purge any adverse information they may have on file about you due to bounced checks. Follow up these conversations with [formal letters](#) and a copy of the police report (see Section V). Send all correspondence via certified mail.

The telephone numbers of the major check-guarantee (also called check-clearing) companies are:

Chexsystems: (800) 428-9623
Telecheck: (800) 710-9898
Scan: (800) 262-7771
National Processing Company (800) 526-5380
Equifax: (800) 909-7304

Note: Be sure to keep copies of all letters you send to agencies, credit bureaus and credit grantors, courts, etc. regarding your case.

2. If via the check-guarantee services or by other means you discover that bad checks have been written, contact the bank on which they were written, speak to the manager and explain that you have been an identity theft victim, and ask that they refrain from reporting the checks to the credit bureau and check-guarantee agencies. Follow up with a [formal letter](#) and a copy of the police report, sent via certified mail (see Section V).
3. Visit your local Department of Motor Vehicles and inform them that you have been victimized by an identity thief. Ask to obtain a new drivers license with a new drivers license number; verify that your old drivers license has been voided in DMV records.
4. Visit your local Social Security Office. As at DMV, inform them that you've been victimized; ask to have a new SSN issued in your name. (You may need to show them a copy of your police report.) It will probably take several weeks for you to receive your new SSN.
5. Once you have your new SSN, it's time to start rebuilding your credit. Begin by applying for one or more new credit cards, using your new SSN. Do not have your old credit card accounts and other credit accounts transferred to your new SSN; this will inevitably result in some of the bad debts run up by the identity thief creeping back into your new credit bureau file. Instead, start an entirely new file with the new SSN.
6. Use BackgroundCheckGateway.com to find out if there are any currently-pending civil or criminal actions pending against you. Go to the [Step 3](#) section of the website (from homepage) and click on the relevant questions regarding civil suits and criminal history. You'll be taken to the State & County Public Records section of the website. Scroll down to the states and/or counties where you believe the identity thief has been operating (based on the addresses of the fraudulent bills you've received); then call the relevant county courthouse offices, explain your situation, and ask them to search their court records under your name. (Alternatively, you can hire an information professional to run this check for you.)

If you find court judgments against you, write a letter to the court explaining that you have been a victim of identity theft (enclosing copies of your credit bureau documents and police report) and ask that the judgment be vacated. Send the letter and police report via certified mail (See Section V, below.)

7. Write a letter to the U.S. State Department, informing them that you have been a victim of identity theft (including a copy of your police report) and requesting that they confirm that a passport has not been recently issued in your name. If one has, request that it be canceled immediately. The address to write to is:

U.S. State Department
Attn: Passport Services
1111 19th Street, NW, Ste. 500
Washington DC 20522

Once you've taken this action, if the identity thief did obtain a false passport in your name, he will very likely be apprehended when he tries to re-enter the U.S.

8. After a few months, and periodically thereafter, order a copy of your credit bureau report. As often happens in these cases, you'll find that despite all your efforts, some fraudulent charges have crept back onto your new credit record. This will happen because some merchants will continue reporting the bad debts to the credit bureau, despite your

requests that they refrain from doing so. If you find this is happening, you should write a strongly- worded letter to the relevant credit bureau, demanding that these fraudulent accounts be removed at once. (See Section V, below.) If your request is not honored you may have to have an attorney write a letter to the credit bureau threatening legal action and/or a formal complaint to the Federal Trade Commission, the federal agency responsible for regulating credit bureaus. (Of course, you can write to the FTC yourself; see Section V, below, for a [sample letter](#).)

9. You should be aware that the federal agency with official jurisdiction over identity theft is the [U.S. Secret Service](#). The main focus of the USSS is on the investigation of identity theft rings where the financial losses are quite large, and you probably won't be able to convince them to investigate your case; however, you may be able to persuade them to take an official report and provide you with a copy of it for your records.
10. Keep your police report (and USSS report, if any) with you continually. Check your credit bureau record periodically. And finally, take the positive steps outlined below to protect yourself from this disaster happening to you again.

IV. SELF-PROTECTION MEASURES

There are a few simple steps you can take to make yourself an unattractive target for identity thieves.

As outlined in Section II, above, the key piece of information sought by these criminals is the social security number. Once they have your SSN, it's a simple matter for them to start opening checking accounts and applying for credit cards in your name. What then can you do to make your social security number harder for them to obtain?

Remember that identity thieves commonly get their targets' social security numbers through information brokers (which have proliferated on the Internet). But how do these unethical information brokers get your SSN? The answer is the so-called "[National Identifier Search](#)," a computerized scan of the files of the big national credit bureaus which permits retrieval of social security numbers and other "header information" (i.e., the information at the top of your credit report); all the information broker needs is your name and address to run this search.

Now, there's not much you can do to keep an identity thief from getting your name, but you can make it difficult for him to get your home address.

The way you can do this is by using a post office box number on all credit applications and other types of forms which will become public information, such as voter registration records, instead of your home address.

Many experts recommend you obtain a private post office box number, such as those available through Mail Boxes, Etc. or Pac Mail. The advantage of using a private post office box, as opposed to those offered by the U.S. Post Office, is that you can use the street address of the Mail Boxes, Etc. or Pac Mail shop as your own, and then indicate "# [your box number]." In this way, you have the use of an actual street address for those situations in which this is a requirement.

Use your post office box address in all legal paperwork, on all credit applications, job applications, mail orders or Internet orders, warranty cards, etc.

A second very important step in identity-theft protection is to get your telephone number out of general circulation. Today, it is quite simple to obtain someone's home address via their telephone number, using an online criss-cross directory. Remember, once the identity thief has

your address, it's easy to get your social security number. So you want to make your phone number (hence your address) as difficult for strangers to obtain as possible.

You want, in other words, to have your number taken out of the phone directory, and thereby also out of CD-ROMs and other databases now commonly available which provide nationwide listings of numbers. To accomplish this, contact your phone company and request that your number be non-published (don't use the word "unlisted," as unlisted numbers still show up in many phone-number databases).

Just those two simple steps -- using a post office box for all public correspondence and getting your telephone number changed to "non-published" will help greatly in protecting you from identity thieves. But why stop there? There are a number of other important steps you can take to further protect yourself:

- Use personal checks only for by-mail bill paying, never for routine, day-to-day purchases. Every check that you write contains identifying information about your bank account, as well as your personal signature. What's more the "check-guarantee services" which are now used by most merchants compile databases of personal data and sell them to information brokers and others. Thus it's important to minimize the use of checks. For routine purchases such as groceries or gas use a credit card or debit card instead.
- Resist giving out your social security number. If it appears on your drivers license, contact your local DMV and ask if you can have it removed. Do not put your SSN on warranty cards, voters registration forms, or provide it to any private businesses (they have no legal right to request it). Never carry your social security card in your wallet or purse. Change your address on your drivers license and vehicle registration to your post office box address.
- Contact the major credit bureaus and inform them that you do not want to be included in "pre-screening," which is a marketing service they offer to anyone who wants to buy it. In pre-screening, the credit bureaus compile mailing lists of individuals from their records who meet any of various criteria selected by their customers, such as income level, credit worthiness, etc. Pre-screening lists are commonly used by identity theft rings to target well-to-do individuals. To be removed from pre-screening programs of all three major credit bureaus, call 800-353-0809 and inform the clerk that you wish to be removed from all pre-screening programs.

[Click to go to Sample Letters](#)

[Recommend this to a friend](#)

Need a background check conducted? [Click here](#) to learn about Washington Research's investigative services.

Privacy Policy

*As information professionals, we take your privacy very seriously.
We will never reveal or sell your personal information.*

© Washington Research Associates, 2001. All rights reserved

Design By [Mirage-Net](#) ~ The COOL Spot In The Desert