

## Chapter 1

---

# Who's Stealing What... and What You Can Do About It

---

### *In This Chapter*

- ▶ Understanding the scope of the identity theft problem
  - ▶ Knowing what information you need to guard
  - ▶ Using technology to help protect your information
  - ▶ Finding help against identity theft
  - ▶ Fighting back if your identity is stolen
- 

**I**n this chapter, I explain who identity theft affects, how it happens, and what personal information it involves. Although the fact of identity theft is pretty unnerving, a greater understanding of identity theft can be empowering. After you find out what identity theft is all about and how it occurs, you can protect your personal information from falling into the wrong hands — and you'll know the best way to take action if it does.

## *Taking a Look at the Fastest Growing Crime*

Identity theft happens when someone (the identity thief) uses another person's personal information (such as name, Social Security number, and date of birth) to fraudulently obtain credit cards or loans, open a checking account, or otherwise gain access to money or goods in the other person's name.

Identity theft takes two primary forms: financial and criminal. Financial identity theft includes activities such as credit card fraud, tax and mail fraud, passing bad checks, and so on. Of course, the identity thief's objective is to not pay back any of the *borrowed* money but, instead, to enjoy spending it. Criminal identity theft expands on the crime by using financial identity theft to support criminal activities up to and including terrorism.

In 1998, the U.S. Congress recognized the growth of identity theft and passed the Identity Theft and Assumption Deterrence Act, making identity theft a crime. In September 2003, the Federal Trade Commission (FTC) released the results of an impact survey that outlined the scope of the crime. The survey statistics show the following:

- ✔ 27.3 million Americans have been the victims of identity theft in the last five years.
- ✔ The total cost of this crime to financial institutions in the United States is \$33 billion, and the direct cost to consumers is \$5 billion.
- ✔ Identity theft is the fastest growing crime in the U.S. today. The crime of identity theft was noted by the FTC as the fastest growing crime in a survey conducted by the agency and published in a report on September 3, 2003.
- ✔ In 2003, the incidence of identity theft was up to 42 percent of all the complaints that consumers filed to the FTC.
- ✔ According to CBSnews.com, "Every 79 seconds, a thief steals someone's identity, opens accounts in the victim's name, and goes on a buying spree."

Some other interesting stats from the FTC study that people find surprising are:

- ✔ In more than 25 percent of all cases, the victim knows the thief.
- ✔ In 35 percent of those cases, the thief is a family member or relative.
- ✔ Almost 50 percent of victims don't know how their information was stolen.
- ✔ The average out-of-pocket expense to individuals is \$500.

So who exactly are the people who fall victim to identity thieves? Read the next sections to find out the *who* and *how* of identity theft.

## *Who it affects*

In addition to the statistics noted earlier, the FTC survey findings show that identity theft can happen to anyone who has credit, bank accounts, a Social Security number (SSN), a date of birth (DOB), or other personal identification information. That is, almost every man, woman, or child is a potential target. Yes, even children are susceptible to identity theft because most children (over 16) have a SSN, and all children have a DOB. Identity thieves don't care about age; they just want personal information they can use to obtain credit.

The sad part is that you can be a victim and not know right away. For example, you may find out you're a victim only when you go to buy a car and get turned down for credit because your credit report already shows three cars — and you're not driving any of them. If you catch it early, however, you can minimize the amount of time and money necessary to clear your name.



Anyone, even a celebrity, can become a victim of identity theft. Tiger Woods, Robert De Niro, and Oprah Winfrey have all been victims of identity theft. No one is immune, and straightening out the resulting mess can take years. But you can protect yourself by practicing identity theft prevention (see my crash course in Chapter 3 and find more details in Part III) and looking for the telltale signs in your financial information (see Part II).

## *How it happens*

Unfortunately, it can be fairly simple for identity thieves to obtain other people's personal information and ply their trade. For example, suppose that you lose (or someone steals) your wallet. In your wallet are your driver's license (with your name, address, and DOB), multiple credit cards (gas cards, department store cards, and at least one major credit card), ATM cards (if you're forgetful, with associated PIN numbers written down), and medical benefits cards (with your Social

Security number as the identifier). Some people even carry personal checkbooks and their actual Social Security cards in their wallets. Get the picture? All the information an identity thief needs is right there in one place.

Identity thieves can also obtain your personal information through a midnight garbage safari activity known as *dumpster diving*. Yes, these thieves will literally go through the garbage cans in front of your house and scrounge information such as cancelled checks, bank statements, utility bill statements, credit card receipts, and those preapproved credit card offers you've been discarding. I discuss what thieves may be looking for in your garbage and what you can do to thwart them in "Knowing What Information Is Vulnerable" later in this chapter. You can also find more details in Chapter 2.



Remember this advice: "If you don't shred, it isn't dead." The non-shredded personal information you've tossed in the trash becomes fair game, and the identity thief thanks you for being so thoughtful.

Although identity thieves have many ways — some rather high-tech and sophisticated — to obtain your personal information, wallets and garbage are the most common targets. The point is that after the thief has your personal information, he or she can assume your identity (at least financially) and start making purchases, getting cash or loans, and otherwise using your good credit.

## *Knowing What Information Is Vulnerable*

We live in a numbers society: phone numbers, personal identification numbers (PIN), driver's license numbers, credit card numbers, date of birth (DOB), Social Security numbers, bank account and 401K numbers . . . you get the idea. As the lyrics of the song "Secret Agent Man" tell us, "They have given you a number and taken away your name." Also, employee and medical record numbers and other tidbits of information are used to identify us as persons today, and that fact gives meaning to the term *personal identification information*, because all these numbers are like keys to your identity on the phone, online, or in writing.

The vulnerable personal information that identity thieves use is as follows:

- ✔ **Social Security number (SSN):** This is, of course, the nine-digit personal identification number (compliments of the federal government) that everyone needs to get a job, pay taxes, and apply for credit. The SSN is like the key to the *kingdom* — your financial kingdom, that is. The identity thief uses your SSN to apply for credit, file false tax returns, get a job, open bank accounts, and so on.
- ✔ **Date of birth (DOB):** A DOB is a piece of the personal information puzzle, but if an identity thief has this piece by itself, it's not a problem. When the thief uses your DOB in conjunction with your SSN, he or she can become you.
- ✔ **Mother's maiden name:** This name is used to verify your identity when accessing financial information. Identity thieves use your mother's maiden name to verify their identity as being yours in order to access your financial records and open new accounts in your name.
- ✔ **Personal identification numbers (PINs):** Usually a five or more digit number used to access your bank accounts when using your ATM card.
- ✔ **Passwords:** Your passwords are the keys to any information stored electronically. When the identity thief has your password, he or she has access to the information you are trying to protect and uses the passwords to access the information, such as bank accounts, online bill paying services, and so on.
- ✔ **Driver's license number:** The number used to identify you is printed on your license. When the identity thief has your driver's license number, he or she can have a phony license made that shows your name and driver's license number with the thief's picture.

By using your personal information, identity thieves can party hardy on your nickel and good credit reputation. They spend like there's no tomorrow because they know that someone else (you) is picking up the tab. Identity thieves can use your personal information to open accounts, such as a cellular phone account, in your name. Of course, they don't pay the bills and continue to use the phone until you discover the theft and the heat is on; then they drop that account and move on to another unsuspecting victim.

## Your identity thief doesn't have to be your twin

For those who remember the old *Mission Impossible* TV show, many episodes featured one of the IMF (Impossible Mission Force) personnel assuming the identity of an intended target or someone close to the target. In the show, the person assuming the target's identity would wear a mask that resembled the target's face and would learn to speak and act like the target. In real life, an impersonator (the identity thief) doesn't need to look or act like you to steal your identity. All that's needed is your personal identification information and *bingo*: He or she becomes you.

TV commercials for a major bank's credit card offer the best depiction of this real-life situation. In the commercials, you see the victims talking to you about how much fun they've had buying expensive vehicles, taking lavish vacations, or whatever. What you notice, though, is that the voices you hear don't match the people you see on the screen: a male voice emanates from a female, or vice versa. The voice — gloating over how wonderful it is to get the goods and stick someone else with the tab — is obviously coming from the identity thief while you're looking at the victim.

## *It comes in the mail*

To steal your identity, the identity thief uses some of the information you receive in the mail. In Table 1-1, I outline the most vulnerable information that comes in the mail.

**Table 1-1** Vulnerable Info That Comes in the Mail

<i>Type of Mail</i>	<i>Vulnerable Information</i>
Telephone bills and other utility bills	Your telephone number, address, and account number
Driver's license renewal	Your name, address, DOB, and driver's license number
Monthly credit card statement	Your name, address, card number and type (Visa, MasterCard, and so on), credit limit, and expiration date

<i>Type of Mail</i>	<i>Vulnerable Information</i>
Bank statements	Your name, address, bank name and contact information, account number, and type. For checking accounts: your cancelled checks, account number, and so on
Pre-approved credit card offers	Your name and address
Pay check stubs from direct deposit	Your name and address; your employer's name, address, and pay rate; and sometimes your SSN
401K and other securities statements	Your name, account number, balance, name of company holding account, contact information, and sometimes your SSN
Personal check reorders (blank)	Your name, account number, address, and bank name and address
Blank checks from credit card companies	Your name, address, and account number
Annual Social Security account statement	Your name, address, SSN, DOB, and account balance
W-2s, 1099, tax returns, and other tax information	Your address, your SSN, and your spouse's and dependent's SSN



The best way to minimize the amount of information you receive in the mail — especially those preapproved credit offers and the blank checks from the credit companies — is to opt-out. When you opt out, you remove yourself from mail marketing lists. You can request that your bank not send pre-approved checks, as well.

## *What you throw away can hurt you*

When identity thieves go through the garbage of potential targets, it is called *dumpster diving*. The only tools needed are a pair of gloves and a flashlight. (The favorite time to go on a

garbage hunt is after dark, and the thief must be able to stand the smell — especially on a hot summer night.) The purpose of dumpster diving is to find personal information that you discard without tearing or shredding. What type of information, you may be asking? The following list gives you the answer:

- ✓ **Preapproved credit card applications:** Throwing away those preapproved credit card applications without tearing, shredding or destroying them in some way is inviting trouble. An Identity thief can retrieve the application from your trash, send it in with the address changed, and receive the new cards in *your name*, based on *your credit*. After receiving your card, the thief charges items (or cash advances) to the card up to its maximum in short order. Then, he or she tosses the card and leaves you with the bill.
- ✓ **Credit card receipts:** Although many businesses no longer print your entire credit card number on your receipts, some still do. Check your receipt — if it lists your credit card number, don't leave it behind to fall into the wrong hands.
- ✓ **Financial statements:** Bank and other financial statements containing your account numbers and (often) your SSN are treasures that may lurk in the garbage unharmed and waiting to be “liberated” by the identity thief.



The bottom line is to remember to destroy all personal information before throwing it away. Tear, shred, or otherwise destroy those preapproved credit card applications, financial statements, credit card receipts, and so on. Don't make your house a dumpster diving gold mine; what you throw away can come back to haunt you.

## The Role of Technology in Identity Theft

Technology can play a role in helping you prevent identity theft when you browse the Web, shop online, and log in and out of secure Web sites. The two most common tools at your

disposal are encryption and authentication. If you know the tricks to these tools, they can help you make sure your information is safe when you're online.

## Encryption

*Encryption* uses digital keys to lock and unlock data while it's being transmitted over the Internet, which makes it incredibly difficult for anyone but the intended recipient to see or tamper with that data. With encryption, a key on the sending end scrambles data, and a key on the receiving end unscrambles it. While the data in *en route*, good encryption makes it virtually impossible for outsiders to peek at or tamper with the data — in your case, your personal and financial data. Secure Sockets Layer (SSL) is the standard form of data security on the Internet. SSL uses digital certificates to verify that the two computers in a transaction are who they claim to be before exchanging the keys that encrypt the data.



Before you use your credit card to purchase merchandise online — in fact, before you enter any of your data online — you want to make sure the site uses 128-bit SSL to keep your data secure. Checking this is easy — in the bottom-right corner of your Web browser, just look for the lock shown in Figure 1-1. If you hover your mouse pointer over the lock, you may even see a ToolTip that says SSL 128. When you double-click the lock, you see information similar to that shown in Figure 1-2, which indicates that the site's identity is authentic and the data is encrypted.

Encryption can also be used to protect e-mail messages and attachments as well as files of personal information that you store on your PC or CD. The encryption software Pretty Good Privacy (PGP) has software that enables you to encrypt this data yourself. PGP offers a freeware version (software that you don't have to pay for) for home use. (You can download the freeware version at <http://www.pgp.com/products/freeware.html>.) For about \$50, PGP offers the software with more features, such as the ability to encrypt content on your hard drive when you're not using it (you may want to do this if, for example, you travel often with a laptop that might be stolen or lost).



Lock

Figure 1-1: Picture of lock on Windows toolbar.

VeriSign offers another method to help you know that the Web site you are on is authentic (that is, the site is who it says it is and is encrypting data). You're most likely to find the VeriSign logo on the site's privacy and security page. When you click the VeriSign logo, you see a screen that tells you what security measures that site is using through VeriSign.

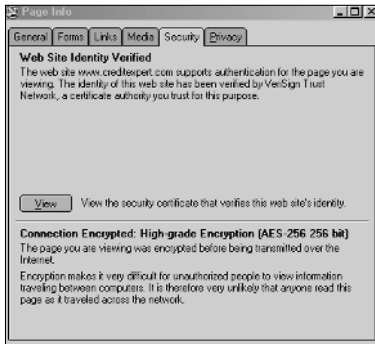


Figure 1-2: Web site verification.



Because well-known names and logos like VeriSign offer people assurance, of course, online scammers try to use them in unscrupulous ways. Savvy identity thieves can forge a site, copy a logo, or make their own digital certificates. Use SSL and the VeriSign digital certificates and logo as one of many tools to make sure the site you're visiting really represents the company or organization it claims to be, and see Chapter 9 for more on spotting and avoiding online scams.

## *Authentication*

Authentication is the method used to identify you when, for example, you access your personal information on your PC, Web sites for bank accounts, online bill paying services, and so on. When you authenticate yourself to a PC or a secure Web site, you enter a user name and a password or PIN to log in.



The best way to protect your identity through authentication is by using a good password. Choose a password that is hard to guess but one you will not need to write down. The password should include a minimum of eight characters using a combination of letters, numbers, and special characters. An example is TGIF!\*49. If you have the opportunity to choose secret questions to help prompt you in the event that you forget your password, choose good questions that no one but you can answer, like a favorite teacher. (People could have access to your mother's maiden name or spouse's middle name.)

## Safeguarding Your Information in Everyday Ways

With identity theft on the rise, you need to be your own watchdog. Table 1-2 lists some everyday do's and don'ts that will help keep your information out of the hands of thieves. I go into more details about preventing identity theft in Part III.

**Table 1-2 Do's and Don'ts to Safeguard Personal Information**

<i>Do or Don't</i>	<i>Why</i>
DO buy a shredder.	Use it to shred those credit card applications you receive in the mail and any other personal information you are going to discard.
DO opt-out.	So you don't receive credit card applications in the first place.
DON'T leave credit card receipts behind.	Take them with you so that they don't fall into unscrupulous hands.
DO check monthly credit card statements regularly.	You have 60 days to dispute a charge.
DO check your monthly bank statement religiously.	So you can find out if there is any suspicious activity on your account.
DO close unused credit card accounts.	To prevent their use without your knowledge.
DON'T give out your SSN.	You only need to give it to the government, your employer, and when you apply for credit.

<i>Do or Don't</i>	<i>Why</i>
DON'T leave your mail in the box overnight.	You don't want your mail falling into the wrong hands.
DON'T Give personal information in response to e-mails.	You don't want to be the victim of a scam.
DO check for the VeriSign or the lock at the bottom right hand corner of your Web browser window.	So you know when you type in your personal data the information gets encrypted when transmitted.
DO sign your credit card.	Your signature will match the receipt when you sign it.
DO make sure your bills are current.	You know whether your address is current and your bills are not being forwarded to another address.

## *Finding Your Allies*

You are not alone in the fight against identity theft. From the federal government and credit card companies to your local police, your allies abound and can help you with many aspects of identity theft. Here are some of your key sources of help:

- ✔ **The Federal Trade Commission (FTC):** The FTC provides information useful for preventing identity theft and knowing what to do if you are a victim. Its Web site ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) is chock full of statistics, information, forms, and more to help you understand and prevent identity theft as well as what to do if you're a victim.
- ✔ **The Social Security Administration (SSA):** Has guidelines for reporting fraud on its Web site (<http://www.ssa.gov/>). Also, you need to submit a fraud reporting

form to the SSA Office of Inspector General (OIG), which is an investigative branch. The SSA recommends downloading the form, completing it, and then sending it via fax or regular mail to ensure confidentiality.

- ✔ **Most local law enforcement agencies:** Provide information on how to prevent identity theft and what to do if you become a victim. For example, the City of Stockton, CA Police Department, does seminars for employees at businesses in the city, and civic groups. They also provide tips on their Web site: visit [www.stocktongov.com](http://www.stocktongov.com) and then click **Police Department**. When you report the crime of identity theft to the Stockton, CA Police Department, you call the Telecommunications Center to file a report. The report is taken over the phone. You will be given a report number. Most active federal law enforcement agencies investigating ID theft are the U.S. Postal Inspection Service and the U.S. Secret Service.
- ✔ **Internet Fraud Center (IFC):** [www.fbi.gov/hq/cid/fc/ifcc/about/about\\_ifcc.htm](http://www.fbi.gov/hq/cid/fc/ifcc/about/about_ifcc.htm). Is a partnership between the FBI and the National White Collar Crime Center. The IFC does report the complaints to the proper local authorities.
- ✔ **Financial institutions and credit card companies:** Most financial institutions provide tips about preventing fraud and knowing what to do if you are a victim. Some institutions provide discounts and links to sites that charge an annual membership fee for providing identity theft protection. For example, I subscribe to a service called **Credit Expert.com**, and the site is part of the credit bureau Experian. Chapter 6 has more details.

To help stem the upward trend of credit card fraud, the card-issuing companies monitor and look for irregular patterns of use. What you charge on a monthly basis is monitored, and when something varies for the normal pattern, the card company will call you and ask if you made the purchase. For example, when people go on vacation and do not notify the card company, they will probably receive a call asking if they made a purchase in X country or Y state. The card companies have used this method for the last ten years, and it has helped reduce some credit card fraud.

✓ **Experienced attorneys:** Although the resources I've just listed are usually quite helpful, you may want to contact an attorney to help you restore your credit and name if creditors are not cooperative in removing fraudulent accounts from your credit report or charges from accounts. Contact the American Bar Association or Legal Aid office in your area and ask for the names of attorneys that specialize in the Fair Credit Reporting Act (FCRA), consumer law and the Fair Credit Billing Act.

## *Getting Back Your Identity and Your Good Reputation*

If you have been a victim of identity theft, do not panic. There are things you can do to restore your identity and good reputation. However, it won't be easy. Estimates of the time spent on getting back your credit and good name are around 600 hours of work, according to a study done by the Identity Theft Resource Center, a nonprofit organization ([www.idtheftcenter.org](http://www.idtheftcenter.org)). The study found the 600-hour figure is a 300 percent increase from 2001, when people spent an average of 175–200 hours regaining their names and credit.

After you suspect your identity has been stolen, you need to take four steps as soon as possible and begin documenting your case. The FTC outlines these first four steps on its identity theft site ([www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)), as shown in Figure 1-3.

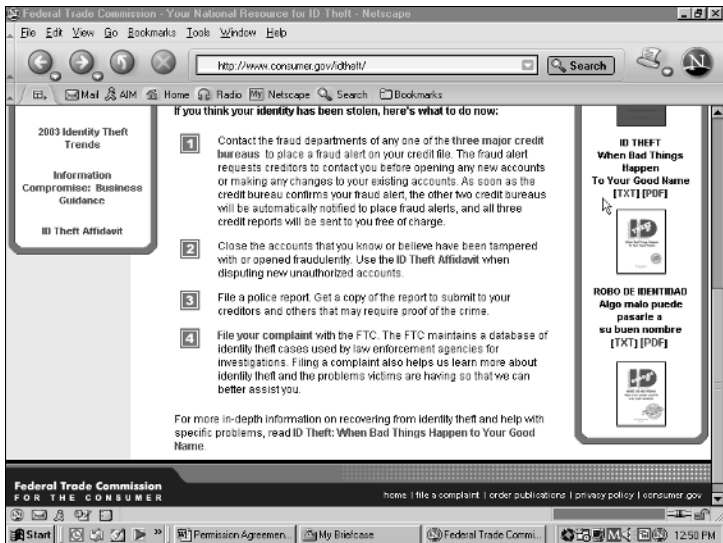
Following is a simplified version of the steps that the FTC outlines:

- 1. Place a fraud alert on your credit reports and review the credit reports that you receive as a result.**

You can contact any one of the three major credit bureaus to place the fraud alert.

- 2. Close any accounts that have been tampered with or opened fraudulently.**
- 3. File a report with your local police or the police in the community where the identity theft took place.**





**Figure 1-3:** Take these steps right away if you think your identity has been stolen.

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

Chapter 3 gives more details about this four-step process for reporting and thwarting identity theft. In Chapter 10, I explain the details of filling out the required reports. Chapter 11 has helpful information for speeding up the process of closing accounts.

As you begin the process of reclaiming your identity, the paper work will start to roll in and out of your life. Keeping a good paper trail will help you assemble and support your case. The Identity Theft Resource Center ([www.idtheftcenter.org](http://www.idtheftcenter.org)) offers some helpful guidelines for organizing the data. The FTC also gives you tips for organizing your case. The tips shown on the FTC Web site are as follows:

- ✔ Follow up in writing with all contacts you've made on the phone or in person. Use certified mail, return receipt requested.
- ✔ Keep copies of all correspondence or forms you send.

- ✔ Write down the name of anyone you talk to, what he or she told you, and the date the conversation occurred.
- ✔ Keep the originals of supporting documentation, like police reports, and letters to and from creditors; send copies only.
- ✔ Set up a filing system for easy access to your paperwork.
- ✔ Keep old files even if you believe your case is closed. One of the most difficult and annoying aspects of identity theft is that errors can reappear on your credit reports or your information can be recirculated. Should this happen, you'll be glad you kept your files.

