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
- Safeguarding your information every day
- Finding help against identity theft
- Fighting back if your identity is stolen

In this chapter, I explain who identity theft affects, how it happens, and what personal information it involves. Although identity theft is pretty unnerving, a greater understanding of it 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 three primary forms: financial, criminal, and medical. *Financial* identity theft includes activities like 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 is used to commit crimes in another person's name and to finance criminal activities with the use of credit cards in someone else's name, selling people's identities, and even terrorism. *Medical* identity theft is when someone assumes your identity for medical reasons and/or for someone else to foot the bill.

In 2007, the U.S. Congress recognized the growth of identity theft and amended the Identity Theft and Assumption Deterrence Act (which was originally introduced in 1998), 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:

- 8.4 million Americans have been the victims of identity theft in 2007.
- The total cost of this crime to financial institutions is $49.3 billion, and the direct cost to consumers is $5 billion.
- The FTC noted identity theft as the fastest growing crime. The FTC will conduct an "Experiences of Identity Theft Victims" study with data from 2008. The FTC is also seeking comments on "Credit Freezes: Impact and Effectiveness in 2008." The results will be available in 2010.
- In 2007, identity theft led the list of top ten consumer complaints to the FTC.

Identity theft continues to be a concern for Americans, and it's still the number one complaint filed with the FTC. If the economy continues on a downward trend, identity theft will continue to be an issue for those with good to excellent credit. The number of people with stellar credit is dwindling because of the recession the U.S. is currently experiencing. So if you have good to excellent credit, you need to be even more vigilant to prevent your identity from being stolen.

Identity theft isn't just using someone's stolen credit card to make purchases, it is actually opening accounts in someone else's name and using them. Stealing the credit card is fraud but does not entail assuming the cardholder's identity. This distinction is important because when you report a stolen credit card, it isn't classified as identity theft. Stolen credit cards are still an issue though, and you must protect your credit card(s). I discuss how to accomplish this task in Chapter 6.

Some other interesting stats from the FTC study that you may 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 a 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 upcoming sections to find out the *who* and the *how* of identity theft.

Who identity theft affects

In addition to the statistics I note earlier, the FTC survey findings show that identity theft can happen to anyone with 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 all children have a SSN and all children have a DOB. Identity thieves don't care about age; they just want personal information that they can use to obtain credit. The credit bureaus will not have a file for a minor until the first application for credit is made. If someone is using the child's SSN to obtain credit, there will be a file. There have been cases where minor children have a number of open accounts that they did not open, and it is a headache to clear up the mess.

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 you own three cars, but you aren't driving any of them. If you catch identity theft early, however, you can minimize the amount of time and money necessary to clear your name.

A current trend shows that people steal their children's or other family member's SSN to obtain credit. In these cases, the children are under the age of 18 and aren't aware that their credit is being ruined by a family member. In some cases, an *infant's* credit has been ruined — and the child can't even talk or walk yet. When these children get older, they face a tough world at a disadvantage of having bad credit and may not even be able to get a job based on their ruined credit history.

Anyone, even a celebrity, can become a victim of identity theft. For instance, Tiger Woods, Robert De Niro, and Oprah Winfrey have all been victims. 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 2 and find more details in Part III) and looking for the telltale signs in your financial information (see Part II).

How identity theft happens

Unfortunately, identity thieves can easily 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 birth date), multiple credit cards (gas cards, department store cards, and at least one major credit card), ATM cards (if you're forgetful, with associated personal identification numbers [PIN] numbers written down), and medical benefits cards (with your SSN 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 in one place.

Identity thieves can also obtain your personal information through *dumpster diving* — a midnight garbage safari activity. Yes, these thieves 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 the section "Knowing What Information Is Vulnerable" later in this chapter. You can also find more details in Chapter 6. Those who work for a company and handle personal information are also a threat, and they can steal personal information and sell it to those who want to use it.

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 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 (PINs), 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 people as persons today, and that fact gives meaning to *personal identification information* because all these numbers are 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 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, 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 yours to access your financial records and open new accounts in your name.
- **Personal identification numbers (PINs):** Usually a four- (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 has access to the information you're trying to protect, such as bank accounts, online bill paying services, and so on.
- **Security questions:** You see these questions — such as what was your first pet's name and where did you go to high school — sometimes when you're setting up an online account. These are not real security questions, so don't use real information when answering the questions. The real answers can be easily guessed by potential thieves or, in the case of your alma mater, are a matter of public information. You can make up the answers so they are not easily guessed; you need to remember the answers you choose, though, so if you forget your password, you can still verify your identity by answering the security questions correctly (with your made-up answers).
- **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, 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 hard 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

Many episodes of the old *Mission Impossible* TV show 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.

A world of companies — you've probably seen the TV commercials — today pitch that they can help protect your identity from thieves. For a monthly fee, these companies will help keep your identity safe. In Chapter 9, I show you some of these companies that provide services to prevent identity theft from occurring in the first place. Preventing identity theft should be your goal. However, identity theft may occur even if you guard your identity like Fort Knox guards the gold reserves of the U.S.

Vulnerable info 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

Type of Mail	*Vulnerable Information*
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
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

Type of Mail	*Vulnerable Information*
Preapproved credit card offers	Your name and address
Paycheck 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 dependents' SSNs.

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. You can do so by going to `www.optoutpresceen.com` or calling 888-5OPTOUT. When you opt out, you remove yourself from mail marketing lists. You can request that your bank not send preapproved checks, as well.

With the current economy, fewer credit card offers seem to be coming in the mail than in previous years when the economy was booming. This doesn't, however, make it less of a problem for other bills and information you may get in the mail that can be used to steal your identity. For example, the federal government still sends annual Social Security statements in the mail. On the statement, you'll find your full Social Security Number. Your DOB as well as your address is also on the statement. So protecting yourself from identity theft still means that you need to guard your incoming mail from the United States Postal Service deliveries. This means *not* leaving your mail in the box for a long period after delivery even in locked mailboxes. Several years ago I was the victim of stolen mail because I left the mail in a locked cluster mailbox overnight. Read about this scenario in the nearby sidebar, "Never leave your mail in the mailbox overnight."

Never leave your mail in the mailbox overnight

Several years ago during the Christmas season, I discovered missing mail when I went to retrieve the mail the morning after it was delivered. As I approached the cluster box, I noticed that several mailbox doors were open, including mine. Of course, nothing was inside. A thief had used some kind of tool to pry open the box and then cut the locks. On the way to the post office to report the incident, I noticed that several other cluster boxes in the neighborhood were also broken into.

Now this is when the "fun" began. At the post office, I spoke to a supervisor and told him to hold my mail at the post office until they repaired the lock on the box. The supervisor then said I needed to report the crime to the police department in my city. So off I went to the police department to report the crime. I waited with all the others in the lobby. When it was my turn, the clerk asked me why I was there. I said my mail was stolen along with several others in my neighborhood. The clerk then said that I needed to report it to the post office. I said I did and he replied that "it's their jurisdiction." I knew this wasn't right, so I went to the main post office to report the crime to the law enforcement arm of the United States Postal Service, the postal inspectors.

Much to my chagrin, the postal inspectors were no longer located at the main office in my city, and I had to call San Francisco to file a complaint. I left a message. (To this day, I have never heard anything from the postal inspectors, and I assume that the perpetrators were never caught.) I returned to my branch's post office to pick up my mail for the day. The supervisor said that I should file a report with the local police to investigate the crime. So I was off to see the police department *again* to file a complaint and report the theft.

The police report is necessary to file a fraud alert on my credit report for a 7-year, but not for a 90-day, alert. At the police department, I told the clerk I wanted to file a report for stolen mail. She asked what monetary loss I suffered. Without that information, she couldn't file a report. I said, "I don't know; if I knew I would have my mail or wait a minute, let me contact the thieves and ask them. At least maybe I can get them to pay any bills that may have been in the mailbox."

Ultimately, I did get the report without knowing the monetary loss and immediately filed fraud alerts on my credit report. When you file a fraud alert, you need a police report number. Luckily, nothing ever happened from the stolen mail incident with my credit or identity. I was lucky, and none of my bills were late, so either the thieves paid my bills (ha) or only "junk" mail was in the box. So the moral to the story is never, ever, ever, leave your mail overnight in the mailbox even it is locked.

What you throw away can hurt you

Dumpster diving occurs when identity thieves go through the garbage of potential targets. The only tools they need 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 she tosses the card and leaves you with the bill.

  Note: Not as many credit card applications are sent in the mail as in previous years. With so many people delinquent in paying their credit cards, it's no surprise that the days of the preapproved credit card applications may be done for — at least until the economy gets better and more people are working. The credit card issuers are hurting because they're seeing a loss in revenue with more credit card defaults occurring than ever before.

- **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.

- **Other paperwork:** Old job applications, insurance forms, and benefits summaries are just a few other forms where your information can be found.

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. Technology can also play a role in helping you lose your identity. Online banking, online shopping, e-mail, and blogs are places where people post information about themselves for friends to see. Would-be thieves can see the same information and have a vast arena from which to steal your identity, and they don't have to get smelly going through the garbage. They don't even have to leave the comfort of their home to steal your identity.

The Internet makes it possible

The Internet isn't owned or governed by any country. Laws do exist against the distribution of certain materials — such as child pornography— in some countries, which is important. But when it comes to e-mails, blogs, and shopping, it is *user beware.* The Internet is a minefield and is potentially dangerous to the user. The best advice I can give you is to be careful regarding what you do, what you post, or where you go on the Internet. I explore ways to protect yourself and your identity on the Internet in Part V of this book.

The two most common technological tools at your disposal are encryption and authentication. If you know the tricks to these tools, they can help you make sure that 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 is 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 that 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) enables you to encrypt this data. PGP offers a *freeware* version (software that you don't have to pay for) for home use. (You can download the freeware version at `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).

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

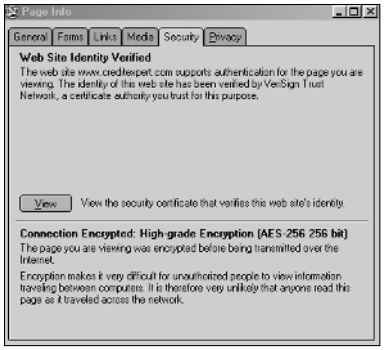

Figure 1-2: Web site verification.

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

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 that the site you're visiting really represents the company or organization it claims to be, and see Chapter 10 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 username 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's hard to guess but you don't need to write down. The password should include a minimum of eight characters with 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, such as 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

Do or Don't	*Why*
DO buy a shredder.	Use it to shred those credit card applications you receive in the mail and any other personal information you're going to discard.

Do or Don't	*Why*
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 whether any suspicious activity is 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.
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 or text messages.**	You don't want to be the victim of a scam.
DO check for the VeriSign logo or the lock at the bottom-right corner of your Web browser window.	So you know that when you type 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 ask for EOBs (explanation of benefits) and yearly records from medical providers and insurance carriers.	To make sure that no one is using your medical insurance.
DO limit the personal information you put on social networking sites.	The less you post, the better — to keep your personal information personal.
DON'T leave purses and wallets in the car, even if the car is locked.	Thieves will break into cars to steal purses/wallets that are visible. If the car is stolen, the thieves have access to your personal information from your wallet or purse.
DO make sure that your bills are current.	You know whether your address is current and your bills aren't being forwarded to another address.

** Find out what protections your financial institution offers. Many offer a password in place of PII (personally identifiable information), so that people with knowledge of that information cannot access your accounts. Some even offer one-time use credit card numbers for online purchases.*

*** Text messaging-phishing by SMS is known as Phexting.*

Finding Your Allies

You aren't 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're a victim. Its Web site (`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. When you file a complaint online, the report will be forwarded to law enforcement as well.
- **The Social Security Administration (SSA):** The SSA has guidelines for reporting fraud on its Web site (`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. When you report the use of your SSN for identity theft, the SSA will not investigate the identity theft but will look into benefit fraud. The SSA will not issue a new SSN if you have been the victim of identity theft.
- **Most local law enforcement agencies:** These 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 gives seminars for employees at businesses in the city and for civic groups. They also provide tips on their Web site: Visit `www.stocktongov.com`, click the City Departments link, and then click the Police Department link. 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, and you're 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 Crime Complaint Center (IC3):** The IC3 (`www.ic3.gov`) is a partnership between the FBI, the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA). At the Web site, you can file a complaint and read about recent scams and other news. The IC3 reports the complaints to the proper local authorities.
- **Federal Bureau of Investigation (FBI):** Go to `www.fbi.gov` and look for the Be Crime Smart and Use Our Resources links (on the left side of the page) to find more information.

- **Financial institutions and credit card companies:** Most financial institutions provide tips about preventing fraud and knowing what to do if you're 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 CreditExpert.com service, and the site is part of the credit bureau Experian. See Chapter 5 for 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 from the normal pattern, the card company calls and asks whether you made the purchase. For example, when people go on vacation and don't notify the card company, they'll probably receive a call asking whether they made a purchase in X country or Y state. The card companies have used this method for the last ten years, and it's 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 aren't 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.

- **Your state's Attorney General office:** Check the Web site for your state's Attorney General office, which has resources about identity theft prevention.

Getting Back Your Identity and Your Good Reputation

If you have been a victim of identity theft, don't panic. You can do things to restore your identity and good reputation; however, it isn't 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`). 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 that 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`), as shown in Figure 1-3.

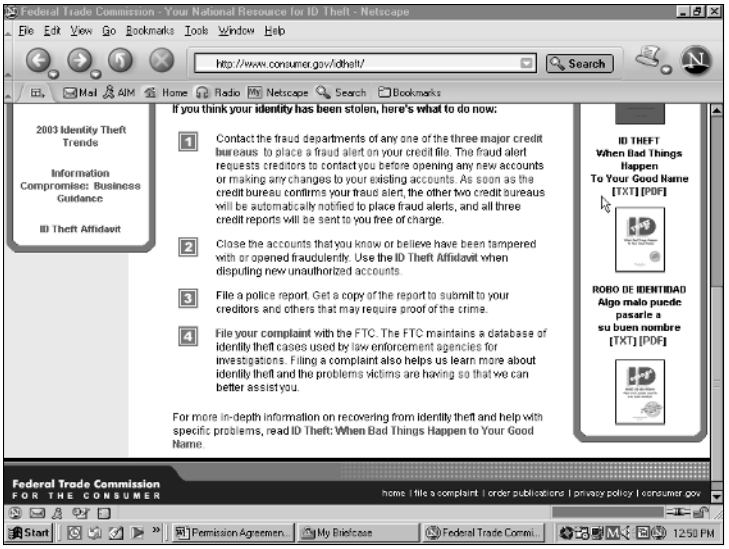

Figure 1-3: Take these steps right away if you think your identity has been stolen.

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. By contacting one, that bureau is required — by law — to contact the other two bureaus to place a fraud alert on them as well. I discuss the three major credit bureaus in detail in Chapter 5. A new tool that you can add to your toolbox is the credit freeze, which I discuss at length in Chapter 2. If, however, you have filed a fraud alert, you are entitled to a free credit report from each bureau.

2. **Close any accounts that have been tampered with or opened fraudulently.**

   

   Make sure that you receive a letter stating that the account has been closed and that you receive a clearance letter.

3. **File a report with your local police.**

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

   Chapter 2 gives more details about this process for reporting and thwarting identity theft. In Chapter 13, I explain further the process of filling out the required reports. Chapter 14 has helpful information for speeding up the process of closing accounts.

As you begin the process of reclaiming your identity, the paperwork 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`) 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, such as 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.