

# Identity Theft

## WHAT IS IDENTITY THEFT?

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. It is considered the fastest-growing white-collar crime.

In 1992, the financial community reported approximately 35,000 cases of identity theft in the United States. By 1997, the number had risen to more than 500,000. **Today the FTC estimates that as many as 9 million Americans have their identities stolen each year.**

There are over 2000 victims per day that are estimated to lose between \$20,000 and \$30,000 per incident. In the next five years, it is estimated that one in four people will be a victim, or a relative of a victim of identity theft. In fact, you or someone you know may have experienced some form of identity theft.

The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector.

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

### How do thieves steal an identity?

Identity theft starts with the misuse of your personally identifying information such as your name and Social

Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.

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

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

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

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. Unfortunately, many consumers learn that their identity has been stolen after some damage has been done.

- You may find out when bill collection agencies contact you for overdue debts you never incurred.
- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.

- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

## **TYPES OF IDENTITY THEFT**

In some cases, with as little as a stolen name, date of birth, and social security number, the identity thief is able to cause major damage.

**Credit card fraud** is the most common type of identity theft.

- The thief pretends to be the victim, calls the credit card company and changes the mailing address on an existing account.
- Or, more commonly, the thief opens a new credit card account in the victim's name.

Because the bills are being sent to a new address, the victim doesn't realize there's a problem. The thief then uses the credit card without paying the bills, ruining your credit.

They may clone your ATM or Debit card and make electronic withdrawals in your name, draining your accounts.

**Phone or Utility Fraud:** (about half the number of victims as credit card fraud) is where an identity thief signs up for cell phone, long distance service, or utilities in the victim's name.

**Bank Fraud:** (about one third the number of credit card fraud) involves depository accounts. The thief opens a bank account in the victim's name, makes electronic funds transfers, and/or writes bad checks on the account.

**Loan Fraud:** Loan fraud involves using a victim's name to take out a loan.

**Fraud Involving Police:** They may give your personal information to the police during an arrest. IF they don't show up for their court date, a warrant for arrest is issued in

**Tax Fraud:** they may file fraudulent tax returns in your name.

**Social Security Fraud:** signing up for government benefits in your name.

Other types of identity theft include,

- Employment - getting a job using the victims name and identity
- Medical
- Residential Leases
- Securities and Investments
- Bankruptcy Fraud
- Illegal Immigration and Miscellaneous government documents

If it happens to you, the damage to your credit and daily life can be devastating. ID theft victims often are unable to get new credit cards or loans because their credit ratings are harmed so badly.

## **HOW LONG CAN THE EFFECTS OF IDENTITY THEFT LAST?**

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

Victims of identity theft should monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months

in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft.

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

## **Avoid Being a Victim of Identity Theft**

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

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

## **Minimize Your Risk: Protecting Personal Information**

Listed below are some safeguards that you should consider utilizing in order to help you reduce your risk of becoming a victim of credit card and personal identity fraud. You should also consider reviewing these precautions with your spouse, and/or any other individual who is authorized to use your card(s).

While nothing can guarantee that you won't become a victim of identity theft, you can minimize your risk, and minimize the damage if a problem develops, by making it more difficult for identity thieves to access your personal information.

## **Protect your Social Security number**

Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give your Social Security number only when absolutely necessary, and ask to use other types of identifiers. Do not put your Social Security number on your driver's license.

Your employer and financial institutions will need your Social Security number for wage and tax reporting purposes. Other businesses may ask you for your Social Security number to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your Social Security number for general record keeping. If someone asks for your Social Security number, ask:

Why do you need my Social Security number?  
How will my Social Security number be used?  
How do you protect my Social Security number from being stolen?  
What will happen if I don't give you my Social Security number?

If you don't provide your Social Security number, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to these questions will help you decide whether you want to share your Social Security number with the business. The decision to share is yours.

## **Treat your trash and mail carefully:**

To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, always tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.

### **To opt out of receiving prescreened offers of credit in the mail, call:**

**1-888-5-OPTOUT** (1-888-567-8688). The three nationwide consumer reporting companies use the same toll-free number to let consumers choose not to receive credit offers based on their lists. **Note:** You will be asked to provide your

Social Security number which the consumer reporting companies need to match you with your file.

Deposit your outgoing mail containing personally identifying information in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 or online at [www.usps.gov](http://www.usps.gov), to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.

### **Be on guard when using the Internet**

The Internet can give you access to information, entertainment, financial offers, and countless other services but at the same time, it can leave you vulnerable to online scammers, identity thieves and more. For practical tips to help you be on guard against Internet fraud, secure your computer, and protect your personal information, visit [www.OnGuardOnline.gov](http://www.OnGuardOnline.gov).

### **Verify a source before sharing information**

Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers, and other identifying information.

Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book.

### **Safeguard your purse and wallet**

Protect your purse and wallet at all times. Don't carry your Social Security number card; leave it in a secure place.

Carry only the identification information and the credit and debit cards that you'll actually need when you go out.

While shopping, if at all possible, it is suggested that you keep your credit cards and ATM card separate from your wallet or billfold.

**Hide Wallets:** While at home, don't leave your purse or wallet in plain view, while in the presence of company or in the event that you are working in the yard and you leave your door unlocked

**Store information in secure locations:** Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house. Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

### **Safeguard Your Checking Accounts**

When opening a new personal checking account or placing an order for new checks, never have your social security number, middle name, driver's license number and/or telephone number imprinted on the face of the checks. You are just providing more information for an unscrupulous individual to use against you.

**When ordering new checks** have them delivered to the financial institution branch office where you conduct your banking, rather than having them delivered to your residential mailing address. If this is inconvenient, instruct your financial institution to deliver the checks to your post office box. Why take the chance of having one, two or perhaps three or more boxes of personal imprint checks,

unlawfully removed from your mail box?

**Check Your Credit Report:** Order your credit report once a year from each of the three credit bureaus. Check for inaccuracies or fraudulent use of your accounts. Monitoring your credit card statements and your credit report are the most important steps you can take to safeguard your credit identity.

**Pay Bills Securely:** When you pay bills, do not leave the envelopes containing your checks at your home mailbox for the postal carrier to pick up. If stolen, your checks can be altered and then cashed. If stolen, credit card payments contain all the necessary information an identity thief needs.

**Mail at the Post Office:** Due to an increased risk of theft and vandalism, it is best to mail bills and other sensitive items at the post office, rather than from your residence or neighborhood drop boxes.

**Get a Shredder:** Spend a few dollars and purchase a quality shredder (preferably a cross cut shredder.) Use the shredder for destroying your personal and financial receipts (old cancelled checks, credit card receipts, bank statements old tax returns, etc.) instead of just tearing the items up and throwing it in the trash.

Shred envelopes that you receive from your credit card issuers, major department stores and creditors, etc., rather than just throwing these items out with your trash.

## **Credit Cards**

**Reduce the number of credit cards you use.** Carry only one or two of them in your wallet. Cancel unused accounts. Even though you do not use them, these account numbers are recorded in your credit report which is full of data that can be used by identity thieves.

**Photocopy all Credit Card Info:** Keep a list or photocopy of all your credit cards, account numbers, expiration dates, and telephone numbers of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditors if your cards become

lost or stolen. Do the same with your bank accounts.

**Never give out your credit card number** or other personal information over the telephone unless you have a trusted business relationship with the company AND YOU INITIATE THE CALL. Identity thieves have been known to call their victims with fake stories in order to obtain credit card information. (“Today is your lucky day! You have been chosen by the Publishers Consolidated Sweepstakes to receive a free trip to the Bahamas. All we need is your credit card number and expiration date to verify you as the lucky winner.”)

**Watch the mail when you are expecting a new credit card** that you have applied for, or a reissued credit card that has expired. Contact the issuer if the credit card does not arrive in a reasonable time.

One of the benefits for consumers using the Internet is the ability to electronically purchase products and services around the clock from the convenience of their home or office. One of the drawbacks is the potential for fraud and deception. Be very careful before you use a credit card on the Internet or provide personal information (such as your Social Security number or date of birth) on an electronic application.

**When using a major credit card at a gasoline station pump to pay for your fuel purchase, be certain to remove your charge receipt tape from the terminal.** Some merchants still use the older style sales receipt, which include a tissue like “carbon” copy. Always ask for any carbons and take them home with you. Never let the sales clerk retain the carbons. If the charge receipt must be voided, have the clerk/cashier write “void” in big print across the slip and insist that you receive the “customer copy” for your records.

**If the sales clerk asks you for additional identification** when paying with a credit card, go ahead and show him/her your identification. However refrain from letting a sales clerk write the additional information, such as your driver’s license number, social security number or your telephone number, on your charge card receipt. If your signature and personal identification check out, they don’t need it.

**Keep Receipts Secure:** If paying with a credit card, have the sales clerk hand you the paid receipt, rather than place the receipt in the shopping bag. In the event you accidentally misplace the bag or someone else ends up with it, your personal charge information is in your possession and not in the store shopping bag.

**Never hand your credit card to a sales clerk/cashier and let him or her walk away from you with your card,** whenever possible. Make it a practice to keep your credit card in view at all times, after giving it to a sales clerk or cashier. Who knows, maybe he or she could have imprinted an extra “blank” charge receipt with your credit card information.

**Never sign a blank transaction slip.** Insist that the receipt be properly completed prior to signing. When the clerk/cashier hands the sales receipt to you, confirm the amount of the transaction. Additionally, make it a practice to always draw two vertical “squiggly” lines through the blank spaces directly above the total amount prior to signing the transaction receipt.

**Whenever you receive a new or replacement credit card in the mail, check the card for its accuracy.** Review the imprint information to make certain the card is correct. Sign the card in permanent black or blue ink, and immediately remove the old credit card from your purse or wallet and destroy it. In the event that the new card has to be “activated” prior to use, do so at this time. If you cancel an account, also destroy the card.

**If you have a credit card that is about to or has recently expired** and you have not received a new replacement card, immediately contact the card issuer to see if it was sent to the correct address. If the new card was sent to an incorrect address or if it has been fraudulently used during this time period, instruct the issuer to immediately cancel the card and issue a replacement card bearing a new account number.

**Cancel any credit cards that you do not need or use on a regular basis.** As these credit card numbers will show as being opened on your credit report, an inactive account number is an ideal “candidate” for credit card fraud. Be certain that when you cancel the credit card, you have a statement placed on your account record, stating that the

account was Cancelled At Customer Request” and not by the card issuer. You want this statement to be properly reflected on your credit report.

With reference to any billing statements, once you have confirmed them with your charge receipts, if you decide to save them store these items in a safe, secure place. In the event that you decide to discard them afterward, destroy them before doing so.

## **Passwords and Personal Identification Numbers (PINS):**

**When creating passwords and PINs, do not use common words or numbers** or anything else that could easily be discovered by thieves (e.g. the last four digits of your Social Security number, your birth date, middle name, pet’s name, address, consecutive numbers).

Ask your financial institution to add extra security protection to your account. Most will allow you to use an additional code (a number or word) when accessing your account. Do not use the common passwords and PINs listed above.

**Shield your hand when using your PIN** at a bank ATM or when making long distance phone calls with your phone card. “Shoulder surfers” may be spying nearby with binoculars or a video camera.

**Never use the same password or PIN number**, even though it may be easier for you to remember.

**Utilize a different PIN or Password for each card** and never write your password or PIN on your card or on a separate piece of paper, located somewhere in your wallet or purse. Otherwise, you are just inviting more trouble. Memorize all your passwords.

As a safety precaution, consider changing your ATM card PIN number on a quarterly basis. Change PIN numbers on other credit cards at least on a semi-annual basis.

**Don’t Use Your Mother’s Maiden Name:** If you are required to furnish, as a means of account identification,

your mother's maiden name, when opening a new bank account, consider using your "grandmother's" maiden name instead. Your mother's maiden name, which can be used for "fraudulent" purposes, can be easily obtained as it is on your birth certificate, and is considered "Public Information".

## **OTHER TIPS**

**Cell Phones are Not Secure:** If at all possible, refrain from giving your credit card number or other personal financial information to anyone over a cell phone. The same holds true for your home phone or office portable phone. This rule especially holds true in the event that you do not own a phone that scrambles the phone signal. Otherwise you virtually have no phone privacy and it is possible for someone to intercept your phone conversation.

**Don't Sign Up For Giveaways:** Do not sign up for a chance to win a free prize (new car, truck, vacation or cruise packages, etc.) at a county fair, shopping mall, or other public type event. Chances are you may end up on another direct marketing list or have your long distance phone service switched. If you do sign up, read the fine print carefully and never provide any personal or financial information.

**While away from home** on business, traveling or on a family vacation, refrain from signing your name and address to a "out of town" guest book, while visiting a major tourist attraction. Why let everyone know that your home may be currently unoccupied.

If you and your family are going out of town for a length of time, notify your local police department and have them place your residence on their "vacation" watch list.

## **Is Your Teen's Identity Protected?**

The parents of teenagers spend many hours teaching them how to drive safely, discussing the importance of an education and warning about the dangers of illegal drugs.

Now they can add identity theft to the list of items meriting special attention.

Identity theft is an ever-increasing threat for all consumers, but children and teenagers make particularly good targets. That is because they have “unblemished” credit records (indeed, they have no credit records at all!); once their identity is stolen it can go undetected for months, if not years, and teenagers and children are likely to be ignorant to any signs that their identity has been compromised.

What can parents do to protect their teens and pre-teens?

The key to shielding your kids from identity theft is to protect their personal information and teach them to carefully question anyone who requests their Social Security number, bank account number, credit card number or other personal financial information.

Schools, athletic teams and pediatric offices routinely request children's Social Security numbers for registration purposes. Before giving that information, always ask: Is this required? By whom? If you do not like the answer, then decline to provide the data.

Don't carry your child's Social Security card in your wallet or purse and do not permit your teen to do so.

When your teen applies for his or her driver's license, make certain that they do not permit their Social Security number to be used as the driver license identification number.

When your teen opens their first checking account, discuss how important it is to safeguard their checks and their banking account number and advise them to carefully monitor their accounts for suspicious activities. Do the same when they apply for their first credit card.

Limit the copies of your child's birth certificate that you give out. If copies are requested in order to allow your children to participate in sports or other extracurricular activities, ask who will have access to the information and where it will be stored.

Talk to your teen about why he or she should not give out personal financial information in response to phone calls from telemarketers or e-mails from unknown individuals or

businesses. Be sure to stress the importance of safeguarding information on the Internet.

Advise your teen to protect their credit cards and checkbook at all times. Only carry what is absolutely necessary in their wallets or purses. They should not take their credit cards or checkbooks with them when they go out partying, for instance.

If your teen is headed off to college, discuss the importance of safeguarding financial documents, bank account statements, credit cards, and other personal records in their dorm room or apartment. Roommates, friends and casual visitors can have “prying eyes.”

Check your child’s credit report annually for any unauthorized accounts and requests for credit. Some warning signs of identity theft include pre-approved credit card offers arriving in your child’s name; unfamiliar bank, credit card or other financial statements that are in your child’s name; and/or collection agency notifications or calls in your child’s name.

If you believe your child’s identity may have been stolen, contact one of the three major credit bureaus; immediately dispute any bills with fraudulent charges; and, visit the ID Theft Resource Center on the Federal Trade Commission Web site at [www.ftc.gov](http://www.ftc.gov).

*For this article and more on the topic of Identity Theft, visit the Better Business Bureau website: [www.bbb.org](http://www.bbb.org)*

## **Basic Rules for Businesses on Protecting Personal Information**

Nearly all businesses collect some sort of personal information on its clients, customers or employees. This might include such things as the individual's name, address, age, gender, identification numbers, income, employment, assets, liabilities, source of funds, payment records, personal references and health records.

If your business maintains people's personal information, you must protect that information from theft or misuse. Here are some basic rules:

**If you do not need it, do not collect it.** This seems obvious, but many businesses collect more information than they need. The more you have, the more tempting it becomes to a thief and the more damaging it is to your customers if the information is stolen.

**If you need it once, do not save it longer.** Companies sometimes collect information that is necessary to complete a single transaction, then compulsively file that information away (either in a paper file or in a computer file). If you are not required by law to keep the information, and you seldom, if ever, use it, then get rid of it. If you do not keep it, it cannot be stolen.

**If you got it, but you do not need to save it, dispose of it carefully.** A good deal of identity theft happens by thieves going through trash barrels or dumpsters. Even the smallest business can afford an inexpensive paper shredder. Make sure you use yours to destroy customer or employee records.

**If you have to keep it, think security.** First, make sure those paper records that contain personal information are kept under lock and key when they are not in use. Make sure computer terminals are password protected. Only those who have an absolute need-to-know should have access to personal information. Do not allow customers or others to wander around the private areas of your business.

**Do not broadcast personal information.** How often have you stood in line at an office or store behind someone who was being asked to give his/her social security number or telephone number or birth date? How many times have you watched a company's employee pull up personal information on a computer screen that was visible to other customers? Or seen personal information on a file that was left open on a desk or counter. Instruct your employees to be sensitive to these issues. Turn computer screens so they cannot be viewed by anyone other than the operator. Instruct employees who need to have personal information to have customers jot that information down, not repeat it out loud where it can be overheard by others. Do not put personal

information like account numbers in billings or letters where that information is visible through windows in the envelope.

**Do not use Social Security numbers as account numbers.**

While not common, this practice is just downright dangerous - to you and your customers.

**Do not give out employee or customer information to**

anyone whose identity cannot be positively confirmed. Information thieves and stalkers who pose as government agencies or credit grantors or health insurance providers, have found that a well-crafted, believable story can often get past the best locked file cabinets or password-protected computers. Your organization should have very strict policies on when and how employee or customer information is shared.

**Locks and alarms are a real deterrent.** Make sure your business is secure when it is closed. Make sure all vital records and offices are locked during non-business hours. Exterior doors should have deadbolt locks. Hinges on exterior doors should be secured to prevent removal. Exposed windows should be protected with bars, screens or shatter-proof glass. The business' exterior should be adequately lighted from dark to dawn. Naturally, the business should be protected by an alarm system, preferably one that is monitored by the security company. Your business insurance company -- or, in some cases, your local police - may be able to assist you with a security assessment.

*For this article and more on the topic of Identity Theft, visit the Better Business Bureau website: [www.bbb.org](http://www.bbb.org)*

**Identity Theft . . . Help For Ohio Residents**

The Attorney General's Office has help to cut through the hours it takes to restore good credit once a person has become a victim of identity theft. This unique program,

called the *IDENTITY THEFT VERIFICATION PASSPORT* program. Until now, those affected by identity theft have had few ways to establish their innocence and reassert control over their information.

Under the *PASSPORT* program, victims reporting identity theft to local authorities will be given step-by-step information about how to alert creditors to fraudulent activity in their names, and simple, fill-in-the-blank affidavits to send to credit bureaus and creditors. The cornerstone of *PASSPORT* is the card victims are given to show to creditors and law enforcement personnel establishing that they have been the victimized.

*PASSPORT* works by first, contacting local law enforcement to report that you have been a victim of identity theft. Once verification of the crime is confirmed and a police report is taken, A *PASSPORT* application is filled out. The officer provides the victim with identity theft materials from the Attorney General's Office, and can assist in filing the *PASSPORT* application – which should take no more than 10 minutes.

The law enforcement agency accesses the *IDENTITY THEFT VERIFICATION PASSPORT* program through the Ohio Law Enforcement Gateway (OHLEG) at [www.ohleg.org](http://www.ohleg.org).

OHLEG is a special website for law enforcement across Ohio to share information. Basic information is entered into OHLEG, and then the application and police report are instantaneously transmitted to the Attorney General's Office via OHLEG. The Attorney General's Office verifies the information and issues a *PASSPORT* card with a unique identifying number.

The *PASSPORT* card is sent to the victim. The victim activates the card and uses it as a unique method of demonstrating to law enforcement and creditors that their identity has been stolen, and to begin rehabilitating their credit history and identifying any fraudulent criminal charges. For more information on the *PASSPORT* program, visit [www.ag.state.oh.us](http://www.ag.state.oh.us) or call (888) MY-ID-4-ME [888-694-3463].

## Identity Theft Quiz: A Quiz for Consumers

Identity thieves use many ways of getting your personal financial information so they can make fraudulent charges or withdrawals from your accounts. Do you know how you can reduce the risk of becoming a victim of identity theft? Take this simple quiz, and see how you score:

1. When I keep my ATM cards and credit cards in my wallet, I never write my PIN (Personal Identification Number) on any of my cards. Yes or No.

Answer: Yes. Reason: If you lose your ATM or credit card, identity thieves or other criminals can have instant access to your bank or credit-card account.

2. When I leave my house, I take with me only the ATM and credit cards I need for personal or business purchases. Yes or No?

Answer: Yes. Reason: If your wallet or purse is lost or stolen, and you're carrying fewer cards, you'll have to make fewer calls to banks and credit-card companies to report the losses, and the odds of fraudulent charges in your name will be lower.

3. When I get my monthly credit-card bills, I always look carefully at the specific transactions charged to my account before I pay the bill. Yes or No?

Answer; Yes. Reason: Someone who gets your credit-card number and expiration date doesn't need the actual card to charge purchases to your account. If you don't look closely at your credit-card statement each month, you might not have any recourse if fraudulent transactions go through and you don't dispute them promptly with your credit-card company. As soon as you see unauthorized charges on your statement, contact the credit-card company immediately to report them.

4. When I get my monthly bank statements, credit-card bills, or other documents with personal financial information on

them, I always shred them before putting them in the trash.  
Yes or No?

Answer: Yes. Reason: Some identity thieves aren't shy about "dumpster diving" - literally climbing into dumpsters or rooting through trash bins to look for identifying information that someone threw out. Buying and using a shredder on your home or office is an inexpensive way to frustrate dumpster divers and protect your personal data.

5. When I get mail saying I've been preapproved for a credit card, and don't want to accept or activate that card, I always tear up or shred the preapproval forms before putting them in the trash. Yes or No?

Answer: Yes. Reason: If you throw out the documents without tearing them up or shredding them, "dumpster divers" can send them back to the credit-card company, pretending to be you but saying that your address has changed. If they can use the account from a new location, you may not know the account's being used in your name until you see it on a credit report (see below).

6. I request a copy of my credit report at least once a year.  
Yes or No?

Answer: Yes. Reason: Any consumer can request one free copy of his or her credit report per year. Reviewing your credit report can help you find out if someone has opened unauthorized financial accounts, or taken out unauthorized loans, in your name. Contact the three major credit bureaus - Equifax (1-800-685-1111), Experian (1-888-397-3742), or Trans Union (1-800-916-8800) - to request a copy.

7. If the volume of the mail I get at home has dropped off substantially, I always check with my local post office to see if anyone has improperly filed a change-of-address card in my name. Yes or No?

Answer, Yes. Reason: Some identity thieves may try to take over your credit-card and bank accounts, and delay your discovery of their criminal activities, by having your mail diverted to a new address where they can go through it

without your knowledge. Your local post office should have on file any change-of-address cards, and can respond if you find that someone is improperly diverting your mail.

8. If I think that I may be a victim of identity theft, I immediately contact -

The Federal Trade Commission to report the situation and get guidance on how to deal with it.

The three major credit bureaus to inform them of the situation.

My local police department to have an officer take a report.

Any businesses where the identity thief fraudulently conducted transactions in my name.

Yes or No?

Answer Yes. Reason: Identity theft is a crime under federal law, and under the laws of more than 44 states, that carries serious penalties including imprisonment and fines. To help law enforcement in investigating and prosecuting identity theft, the Federal Trade Commission (FTC) maintains a national database of complaints by identity theft victims. The FTC, through a toll-free hotline (1-877-ID-THEFT), can also help you decide what steps to take in trying to remedy the situation and restore your good name and credit. Credit bureaus should also be notified so that they can flag your credit report. Local police, by taking a report and providing you with a copy, can help you show creditors that an identity thief has been conducting certain transactions in your name and without your permission.

**How did you score on this quiz?** If you answered “No” to even two or three questions, it means that you need to take more of the precautions described in this quiz. Remember that identity thieves, unlike robbers or fraudsters, don't have to have any personal contact with you in order to commit their crimes. The more you do to protect your personal information, the lower the odds that you'll become a victim of identity theft.

**Stories of Identity Theft Online:** Read real life experiences from identity theft victims who have reported to the Better Business Bureau.

<http://www.bbbonline.org/idtheft/stories.asp>