



Identity Theft: Frequently Asked Questions

Prevent Fraud by Learning More about Identity Theft



(Reprinted with permission of Nolo, Inc.
Copyright © 2008 Nolo.)

Q: How Can My Identity Be Stolen?

A: Someone could steal your identity very easily by:

- ◆ stealing your wallet;
- ◆ filling out a change of address form for you and collecting your mail;
- ◆ snatching your unshredded pre-approved credit slips from the trash;
- ◆ ordering unauthorized credit reports on you by posing as a potential employer or landlord;
- ◆ looking over your shoulder at phones and ATMs to gather PIN numbers (sometimes with binoculars or listening devices);
- ◆ using phony telemarketing schemes to con you into giving your personal data;
- ◆ illegally tapping a computer at a business to which you have provided information or by which you have been granted credit (this is often done by dishonest or disgruntled employees); or
- ◆ gathering sensitive information and using it as a way to extract revenge (this is usually done by a former friend, lover, roommate, or co-worker—and it's more common than most people realize).

Perhaps the most frightening (and most thorough) way for a thief to steal someone's identity is by purchasing it at one of the identity search companies that have sprouted on the Internet. For as little as \$49.99, these companies will sell you someone's Social Security

number (the heart of identity theft), their mother's maiden name (the second most valuable piece of information), their home and employment addresses, their previous addresses, their credit history, and more.

Q: What Can I Do to Protect My Identity from Theft?

A: Minimizing the disaster of identity theft depends primarily on your vigilance in guarding your privacy. You've got to guard your personal information diligently. Here are some tips for keeping your private information secure:

- ◆ Never carry your Social Security card in your wallet.
- ◆ Don't have your Social Security number or your driver's license number pre-printed on your checks.
- ◆ Use your initials (instead of your first name) and last name on your checks. If some one takes your checks, they will not know if you sign your checks with just your initials or your full name, but your bank will know.
- ◆ If you have a P.O. Box or work address, put that address on your checks instead of your home address. Put your work phone number on your checks instead of your home phone number.
- ◆ When writing a check to a credit card account, do not put the complete account number on the "For" line—just use the last four numbers.
- ◆ Install a locking mailbox or a mail slot that goes directly into your house. Send your mail, especially payments, directly from the post office (don't put it in the mailbox for the postal carrier to pick up).

- ◆ Order your credit report every year. Promptly respond to any inaccurate information.
- ◆ Change your passwords and PIN numbers regularly. Don't use obvious codes such as birthdays, or the name of your spouse, child, or pet. Memorize passwords and PIN numbers and shred any piece of paper on which they are written.
- ◆ Diligently review credit card statements, phone, and utility bills. Call if you don't recognize a charge or phone call.
- ◆ Always take your credit card receipts, and never throw them away in public.
- ◆ Tear up or shred any offers of pre-approved credit cards you don't intend to use and beware of offers from companies you don't recognize. It's easy to create an official-looking and completely phony credit application offering you pre-approved credit if you provide your Social Security number, mother's maiden name (for supposed security reasons), and a signature.
- ◆ Don't give personal information over the phone unless absolutely necessary, and don't ever give it unless you initiated the phone call. If someone calls who says they are calling from your bank or credit company, ask for a number to call them back—and then make sure it's really an official number.
- ◆ Beware of anyone asking for your Social Security number. If they refuse to complete a transaction without it, consider taking your business elsewhere.
- ◆ Pick up your new checks from the bank instead of having them sent to your home.
- ◆ Don't put personal information on a computer home page or personal computer profile.
- ◆ If you find your personal information posted somewhere on the Internet, demand that it be removed.

Q: What Are the Chances My Identity Will Be Stolen and What Can the Thief Do with My Personal Information?

A: Identity theft is a growing national epidemic. The Federal Trade Commission's 2003 report on identity theft called it the fastest growing crime in the nation, with nearly 500,000 victims, costs to businesses of \$48 billion, and costs to consumers of nearly \$5 billion.

An identity thief can cash a check, obtain a loan, open credit accounts and charge them to the max, rent an apartment, buy a car, purchase a cell phone and talk to someone long distance all day, and, worse, commit a serious crime—all in your name.

Q: What Should I Do If I Discover That My Identity Has Been Stolen?

A: As soon as you are aware of the problem, you need to do the following:

- ◆ **Make an identity theft affidavit.** The Federal Trade Commission has an official identity theft affidavit that you can use to alert different companies, including the major credit bureaus, your credit card companies, your banks, and so on. You can download the affidavit at www.consumer.gov/idtheft. Make plenty of copies for yourself.
- ◆ **Contact the police.** File a police report and keep several copies. You may need to send copies to credit bureaus, creditors, collectors, banks, and so on.
- ◆ **Cancel your credit cards, ATM cards, and phone cards.** Notify your bank of the problem and close all existing bank accounts.
- ◆ **Call the credit bureaus.** Ask the credit bureaus to issue a fraud alert and attach a statement to your report. Also, be sure to get copies of your credit report from each of the credit bureaus. You can ask that the reports be free-of charge because you believe they contain inaccurate information due to fraud.

- ◆ **Report stolen checks.** Contact your bank and the following agencies:
 - **Certegy:** 800-437-5120
 - **TeleCheck:** 800-710-9898
 - **TeleCheck** (merchant services): 800-366-1054.
- ◆ **Review your Social Security earnings statement.** Look for evidence that your Social Security number has been used fraudulently. Get a copy of your Social Security Earnings and Benefit Statement and look for earnings for jobs you've never had.
- ◆ **If someone is using your driver's license number fraudulently, obtain a new number.** You should be prepared to show proof of theft and damage.
- ◆ **Take control.** Most important, you need to take control of the situation and not waste time waiting for someone else to step up and help you. Vigilance is essential. Do not pay bills that you are not responsible for. Be persistent with police, credit bureaus, credit card companies, and banks. Continue to call and write letters. Keep track of your efforts to stop the theft and reverse the damage.

Q: Will I Be Held Responsible If a Thief Uses My Identity to Commit a Crime?

A: Yes and no. From a monetary standpoint, if a thief uses your credit card in a credit scam, you'll likely be responsible for only \$50, or possibly nothing. However, you may spend months hassling with credit agencies, financial institutions, and police departments trying to clear your name and repair the lingering damage. Almost certainly you will have to take time off from work to write letters, make calls, collect evidence, and demand action.

There is also the cost of anxiety and mental suffering to consider. Victims of identity theft report that police agencies are sometimes dismissive, credit reporting agencies unresponsive,

credit collection agencies hostile, and credit grantors disbelieving.

When victims are actually accused of committing crimes, they are sometimes repeatedly detained by police and have trouble trying to convince law enforcement officials that the person they're holding is not the person they want. See *Fact Sheet 17(g): Criminal Identity Theft* at www.privacyrights.org.

Q: Are There Any Laws That Specifically Prohibit Identity Theft?

A: Yes. In 1998, Congress passed the Identity Theft and Assumption Deterrence Act. (18 U.S.C. section 1028.) The Act makes the use of another person's identification with the intent to commit any unlawful activity a federal felony. Federal agencies—including the U.S. Secret Service, the FBI, and the U.S. Postal Inspection Service—investigate suspected violations of the Act. The U.S. Department of Justice handles prosecutions. Federal law enforcement agencies usually do not investigate individual cases unless the dollar amount is high, or the victim is one of many people victimized by the same perpetrator or fraud ring.

Additionally, many states have passed or are considering laws related to identity theft. Even if your state does not have a law specifically called an identity theft law, the issue is likely covered under other state laws. To see a list of state identity theft laws, go to www.consumer.gov/idtheft.

More Information About Identity Theft

The federal government maintains a central website devoted to identity theft: www.consumer.gov/idtheft. This site lists all federal and state laws relating to identity theft, discusses pending cases, and alerts consumers about identity scams. It also contains useful links for more information. See especially, "ID THEFT—What's It All About?" and "Take Charge: Fighting Back Against

Identity Theft,” both of which are on the FTC website at www.ftc.gov.

The Federal Trade Commission Consumer Response Center has a thorough collection of reports on identity theft at www.ftc.gov. You can also call the FTC for information on identity theft at 877-ID-THEFT.

The Privacy Rights Clearinghouse maintains an excellent website with reports on a variety of privacy related issues, including identity theft, at www.privacyrights.org.

You can also access a wealth of information about identity theft at www.identitytheft.org.

The State of California’s Office of Privacy Protection (www.privacy.ca.gov) has California-specific information



(Reprinted with permission of Nolo, Inc. Copyright © 2008 Nolo.)

This publication is for general informational purposes only and is not intended to provide any reader with specific authority, advice or recommendations.

Copyright © 2009 LifeCare®, Inc. All rights reserved. LifeCare®, Inc. is the worldwide provider of Life Event Management® Services | www.lifecare.com

#1146_IdentityTheftFAQs_0309

