

**ID Theft Manual**  
© 2003 National Utility Services, LC



**ID-THEFT-SECURITY.COM**

## Table of Contents

<b>Introduction</b>	3
<b>Section I: How do I know if I am a Victim of ID Theft?</b>	5
<b>Section II: I am a Victim of ID Theft. What should I do?</b>	7
<b>A. Create a Record</b>	7
<b>B. Contact the Three Major Credit Bureaus</b>	8
<b>C. Contact Creditors</b>	9
<b>D. Contact Other Affected Institutions</b>	9
<b>E. Report the Crime to the Authorities</b>	12
<b>F. Repair your Credit</b>	12
<b>Section III: How can I reduce the chances of being a victim of ID Theft?</b>	14
<b>A. Preventative Steps</b>	14
<b>B. Limiting the Damage—Credit Monitoring Services</b>	17
<b>Section IV: Federal and State Laws</b>	18
<b>A. Federal Laws</b>	18
<b>B. State Laws</b>	18
<b>Appendices (can be downloaded for free from our web site)</b>	
<b>Appendix A: <u>Federal Trade Commission ID Theft Affidavit</u></b>	
<b>Appendix B: <u>The Identity Theft and Assumption Deterrence Act</u></b>	
<b>Appendix C: <u>The Fair Credit Reporting Act</u></b>	
<b>Appendix D: <u>Electronic Funds Transfer Act</u></b>	
<b>Appendix E: <u>Fair Credit Billing Act</u></b>	
<b>Appendix F: <u>Fair Debt Collection Practices Act</u></b>	

## **Introduction**

This manual is written for the victims of the crime of ID Theft and those who wish to do what they can to protect themselves from such a fate. If you are reading this manual because *you know or suspect that you are a victim of ID Theft, time is of the essence* so you may want to skip to *Section I* and begin putting a stop to the damage to your financial life.

This document was written by attorneys and is an outgrowth of the personal experience of the authors in trying to combat Id Theft in their own lives. Those of us who are victims of ID Theft can relate to the sense of violation, which we all felt when we discovered that persons unknown to us were utilizing our private information to enrich them, and do us harm.

In 2002 alone, there were approximately 700,000 instances of ID Theft in the United States. Due to the sheer volume of occurrences, law enforcement is overwhelmed, making it all the more important that we do what we can to protect ourselves.

### **Just what is ID Theft?**

We all have personal information, which identifies us to creditors, the government and society at large. This information includes our birth certificate, driver's license, Social Security number, credit card numbers, loan information, credit report....the list goes on. When this information is misappropriated for gain by third parties, the crime of ID Theft has occurred. It often leaves the victim with years of "picking up the pieces" and reestablishing his or her financial and personal identity.

No one is completely immune from risk of ID Theft. Newspapers are full of stories about celebrities who are the targets of such scams. But, in most cases, the crime of ID Theft is perpetrated upon average citizens going about their everyday working lives. The FTC estimates that persons harmed by ID Theft don't discover that they are victims until, on average, 14 months after the crime occurs.

### **What can be done to protect myself against ID Theft?**

While there is no absolute protection from ID Theft, there are things, which can be done to minimize one's vulnerability to the crime. Just like locking the doors to a home may help prevent a theft of household items, vigilance over one's "financial house" can help prevent ID Theft or limit the damage done should it occur. These preventative measures are covered in depth in *Section III* of this manual.

### **What laws protect me?**

Recent years have seen an improvement in State and Federal laws designed to protect us from ID Theft. The citations to these laws are set forth in *Section IV*. Additionally we have provided links and contact information to various federal agencies such as the IRS and the FBI, which have specifically addressed problems of ID Theft. Also useful to consumers is the Federal Trade Commission document entitled, "ID Theft, When Bad Things Happen To Your Good Name". We hope these additional resources are helpful to your specific situation.

### **Thoughts and Comments?**

ID Theft is a frequent and evolving crime. If you have had a particular experience, which you think it would be useful for us to know, or specific comments about the content of this manual, feel free to email us **at**. We would love to hear from you.

## **Section I**

### **How do I know if I am a Victim of ID Theft?**

(If you are reading this manual and already know you are a victim of ID Theft, you may wish to skip to Sections II and III.)

First, let's define ID Theft. Anytime you use personal information in today's high tech world, you are revealing some tidbit of information about yourself, which in the wrong hands can be misused. When a thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft, an ID Theft has occurred.

Most cases of ID Theft are limited a single aspect of the victim's financial life. One classic example is the theft of a credit card number. Another is the forging of a check from a victim's bank account. These cases are the easiest to remedy because they are quickly discoverable and limited to the card or account at issue.

Other cases are more extensive and involved the misappropriation of many aspects of one's financial life. Such cases involve the impersonation of the victim in setting up multiple accounts, using the victim's social security number to obtain work and even impersonating the victim in civil court actions or with law enforcement.

The source and extent of ID Theft in each individual situation dictates the nature of the remedy. This concept is discussed in more detail in Section II.

#### **How do I know if I am a victim of ID Theft? Here are some possible indicators:**

- Your credit card statement shows purchases or charges you never made and cannot account for.
- Your bank statement shows debits to your account from checks you have not written or ATM withdrawals you have not made.
- A creditor or collection company contacts you regarding debts you have never incurred.
- A creditor acknowledges an application for credit, which you never made.
- You receive notice from a creditor that you have been approved or denied on a credit application which you never made.

--You receive a monthly statement from a creditor such as the power company, phone company or from a credit card, which you do not recognize and for which you never applied.

--You stop receiving statements in the mail from one or several creditors (indicates those statements may have been re-routed to another address).

--You learn an adverse civil judgment has wrongly been entered in your name.

--You learn someone has filed bankruptcy in your name to shed debts they have incurred in your name.

--Criminal warrants are issued in your name (happens when someone is arrested and falsely gives your identifying information as their own).

These are just some examples. There are many other signs of ID Theft, which might occur. The important point is to be vigilant. In Section III we discuss Credit Monitoring Services and other means of discovering and protecting against ID Theft. The more we protect ourselves, the less the chance of serious damage to our personal and financial reputation.

## **Section II**

### **I am a Victim of ID Theft. What should I do?**

If you are, or suspect that you are a victim of ID Theft, the first thing you should do is take a deep breath. Understand two things. First, you are a victim of a crime, which is estimated to have been committed 700,000 times in 2002 alone. Thus, you are not alone, and there are institutions and resources available to help you. Second, you will need to be determined and thorough in resolving the effects of this crime upon you. Rarely are the effects of ID Theft resolved quickly. Be patient and thorough and you will get through this!

As a preliminary matter, you will have to make a judgment. If you think you know the origin of the ID Theft against you, and it is confined to one source, like stolen checks from one bank account, you may be able to address your situation without taking all the steps outlined below. That said, if you have any questions about the extent to which your identity has been misappropriated, you should take full advantage of the advice provided herein.

**Now, let's get started!**

#### ***Things to Do:***

##### **A. Create a Record**

Prepare a record beginning on the day you learned of the crime committed against you. List every action you are taking to resolve your ID Theft situation. We suggest doing this on a computer if possible so that you can easily add to, update, and edit your record. The report should be divided into categories of actions so that you can easily refer to the right section if the list gets long. You should include both a record of written communications AND oral communications (whenever possible, written communications are preferred). Four basic headings for your record would be:

1. Credit Bureau Communications.
2. Communications with your Creditors, Banks and Credit Card Companies.
3. Communications with Law Enforcement.
4. Costs and Time Associated with Correcting the Fraud.

This record is important, as you may need proof of communications to protect your legal rights later. A record of the costs (including receipts) and your time spent will help you prove the damages to you in the event a judge orders the fraudster to reimburse you.

## **B. Contact the Three Major Credit Bureaus**

As soon as possible, you should contact all three major credit bureaus (see contact information below). In each case ask for the “fraud department”. Your goal right now is to check your credit report for evidence of ID Theft and put a stop to it. We have included information on repairing your credit in subsection F below. But this is something you will do later. Now, we want to do the following:

### **1. *Obtain your credit report.***

The credit bureaus will send you a free credit report once you have notified them that your personal information is being used by someone else to fraudulently obtain credit. Time may be of the essence, so ask about obtaining your free credit report over the Internet.

### **2. *Place a “security alert” on your account.***

When asked, credit bureaus will also place a “security alert” (sometimes called a “credit alert”) on your account. This alert will notify creditors to contact you and confirm your identity before granting additional credit in your name. Such alerts are typically good for at least 90 days, but it is important to ask each credit bureau how long the alert will last.

### **3. *File a “victim statement” (optional).***

Next, if you are so inclined, you may ask the credit bureau how to file a “victim statement”. These statements require some affirmation by you in *writing* that your credit is being misused. Once the statement is recorded with the credit bureau it has the effect of requiring creditors to contact you by phone before issuing credit in your name. Unlike with the security alert, this requirement may stay in effect for up to 7 years.

## **Credit Bureau contact information:**

### **Equifax ([www.equifax.com](http://www.equifax.com))**

Fraud number: (888) 766-0008  
Main number: (800) 685-1111  
Address: P.O. Box 740241  
Atlanta, GA 30374-0241

### **Experian ([www.experian.com](http://www.experian.com))**

Fraud number: (888) 397-3742  
Main number: (888) 397-3742  
Address: P.O. Box 9532  
Allen, TX 75013

### **TransUnion ([www.transunion.com](http://www.transunion.com))**

Fraud number: (800) 680-7289

Main number: (800) 888-4213  
Address: P.O. Box 6790  
Fullerton, CA 92634-6790

### **C. Contact Creditors**

**1. Review your credit report.** Carefully review your credit report. It will list the credit accounts you have had or currently have, and the status of those accounts. Some may be valid, but for one reason or another you may not recognize or remember them. Make sure you get to the bottom of any suspicious notations.

**2. Call the creditors.** Once you identify any items on your credit report, which are suspicious or clearly fraudulent in nature contact, those creditors by the fastest means possible. If a phone number is listed, use it. Tell the creditor that you have reviewed your credit report and that the item listed by them was fraudulently obtained. Or, in the event there are unauthorized charges on your credit card, inform the credit card company that the charges are fraudulent. Your liability for the unlawful use of your lost or stolen credit card should be limited to \$50.

**3. Complete a "fraud affidavit".** Most creditors will request what is called a "fraud affidavit". By executing this document, you are certifying under oath that the charge or charges against your credit were NOT made by you and were not authorized by you. Some creditors may ask you to have the fraud affidavit notarized. Others will accept the signatures of witnesses in lieu of notarization.

We have supplied you with a fraud affidavit form prepared by the Federal Trade Commission. (See Appendix A, which you may download for free from our web site). We suggest that you use it unless a creditor requests another form. In any event, it may be useful to review it prior to calling creditors so you have an idea what kind of information they will be asking you.

**4. Close accounts.** Where credit accounts have been improperly opened in your name, ask that they be closed immediately. If you wish to start or continue a relationship with the creditor, set up new accounts, with new numbers, and, if appropriate, establish password access to the account. We strongly urge you to employ a credit monitoring service to monitor future account use. Credit monitoring services are discussed in *Section III (B)* below.

### **D. Contact Other Affected Institutions**

- 1. Banks.** If your checks have been stolen or bank accounts have been violated, contact your bank immediately to inform it. You may issue “stop payment” orders on individual checks (usually for a small fee). Close your accounts and open new ones. If your ATM card has been stolen, talk to the bank about issuing a new one associated with your new account. Very importantly, change your password for the new card.

The sooner you report stolen ATM cards the better for you. If you report the theft BEFORE unauthorized use, you have no liability for the unauthorized use. If you report the theft within two business days of learning of the theft, your liability is limited to \$50. If you wait until after two business days, but before 60 days, you’re potential liability goes up to \$500. After 60 days, your potential loss is unlimited. So, report any ATM card thefts or losses as soon as possible. (For more information see the Federal Trade Commission summary of Electronic Banking rules which is Appendix D and may be downloaded for free from our web site)

If you find that merchants are not honoring your checks, it may be because they use a check verification service. If so, ask them what service they use and the 800 number of the service. Call and find out why your check has not been honored, and notify them you are a victim of ID theft.

- 2. Social Security Numbers.** ID Theft using a stolen social security number and fraud in connection with obtaining a social security number are violations of the Social Security Act and can result in both civil and criminal consequences. If you think someone has used your Social Security number to obtain work, you may order a copy of your Social Security Statement. If you're age 25 or older and not already receiving Social Security benefits, you'll automatically receive a Social Security Statement each year. The Statement lists earnings posted to your Social Security record and provides an estimate of benefits you and your family may be eligible to receive now and in the future. You should receive your annual statement about three months before your birth month.

If you don't receive a statement, you can ask for one by submitting a Request for Social Security Statement (Form 7004). You may download Form 7004 from the Social Security Administration web site at [www.socialsecurity.gov/online/ssa-7004.pdf](http://www.socialsecurity.gov/online/ssa-7004.pdf). Or, you can call the Social Security Administration at 800-772-1213 or visit your local Social Security office. It generally takes 4-6 weeks to receive a copy of your statement.

If you confirm misuse of our Social Security number has occurred, it is possible to obtain a new number, but doing so is usually not advisable unless the damage to your identity is extensive. Call the Social Security Administration's Fraud Hotline 1-800-269-0271. Speak to a Social Security representative about your particular circumstances, and view their information at <http://www.ssa.gov/>

- 3. Driver Licenses.** If your drivers license has been stolen or someone is using your drivers license number in check fraud or other schemes you will need to contact your state Motor Vehicle Department. Each state DMV has its own procedure for processing cases of driver's license misuse. Most have a complaint process and will issue you a new license and number. Some also have a process for issuing a fraud alert on your license. Explain your situation to the local office and let them guide you through the process.
- 4. Mail Delivery.** Some ID thieves will change your mailing address in order to intercept mail and hide their thievery from you. The US Postal Service is helpful in correcting such problems. Contact the US Postal Inspection Service to report your problem. The nearest office to you can be found using the locator service at <http://www.usps.com/ncsc/locators/find-is.html>. Or, you can call your local post office and ask for assistance. For more information about the U. S. Postal Inspection Service, visit their web site at: <http://www.usps.gov/postalinspectors>
- 5. Telephone Service and Calling Cards.** If you find unauthorized calls on your phone bill, check to make sure that a missing calling card is not the sources of the calls. If so, cancel the card and ask for a new one with a different number. Some phone companies will allow you to create a password to be used anytime you make changes to your account.
- 6. Bogus Legal Judgments.**

  - A. Criminal Judgments:** Sometimes those who steal identifications do more than simply misuse credit. They impersonate you in front of law enforcement and the courts. When this happens, it can result in wrongful convictions against you, false warrants for arrest and other serious consequences. If this happens, the FIRST thing you should do is contact an attorney. That attorney can then contact the authorities in the subject jurisdiction and correct the error. We advise against trying to do this on your own, as you could end up in jail or under arrest before matters are cleared up.
  - B. Civil Judgments.** In the event you discover that a bogus civil judgment has been entered against you as a result of ID Theft, we

also recommend contacting an attorney to correct the record. He or she may need to petition the court to overturn the judgment base upon fraud. With the proper documentation, this should not be a problem but may take several months to accomplish. If you cannot afford an attorney, call the court clerk's office for the court that issued the ruling and explain to them that you have been a victim of ID Theft and ask for help. They may refer you to legal aid services or may have a local procedure for resolving your problem.

### **E. Report the Crime to the Authorities**

ID Theft cases should be reported to law enforcement. Cases of credit card theft, stolen or forged checks or stolen ATM cards should usually be reported locally, to your police or sheriff's department. Your bank may also report the crime. If you know the theft occurred elsewhere, try to report the crime to the local authorities in the jurisdiction where it occurred. They are usually in the best position to investigate and prosecute the case. In all likelihood, you are not the only victim and reporting the crime may prevent the fraudsters from repeating the crime.

Reporting the crime also creates an independent record of the events, which you can use with others to help verify what has happened to you. A police report may be requested by current or future creditors. Therefore, be thorough in the information you provide to the authorities, and include a listing of every account or creditor relationship which has been damaged by the crime. Make a few copies of the report, which you can use as needed.

Filing a police report also provides you with at least a chance of restitution, should law enforcement successfully prosecute the person or persons responsible for the fraud. If the fraud is partially due to the negligence of a legal caretaker of your private information, the evidence of a criminal proceeding may be helpful in resolving a claim for negligence against that caretaker, even if that caretaker did not itself commit the fraud.

In addition, you may want to make a complaint to the Federal Trade Commission. We recommend that you call the ID Theft Clearinghouse toll-free at 1.877.ID.THEFT (1.877.438.4338) to report the theft. The Identity Theft Hotline gives consumers a place to report the theft to the federal government and receive helpful information and statistics.

### **F. Repair your Credit**

You may find that many months after providing the Credit Bureaus with evidence of the ID Theft committed against you some of the negative credit references on your credit report remain. Also, you may be receiving calls or letters from creditors who have not accepted the fact that the credit they

extended was to someone other than you. We have found that such instances are few when someone has followed the suggestions in this manual.

The Fair Debt Collection Practice Act protects you from harassment in the collection of debts. You can download a copy for free from our web site. See Appendix F.

You may choose to retain an attorney to resolve such problems. Perhaps you have some negative credit references on our credit report that are NOT the result of ID Theft, but need to be corrected. There are a multitude of credit repair agencies available who offer to resolve such matters for a fee. However, we urge you to be careful in contracting with such organizations. Credit repair organizations are regulated by Federal Law and may not make false claims or charge in advance for their services. The Federal Trade Commission suggests that self-help may be best. See their advice on credit repair at:

<http://www.ftc.gov/bcp/online/pubs/credit/repair.htm>

## **Section III**

### **How can I reduce the chances of being a victim of ID Theft?**

No one living in today's economy is totally immune from the threat of ID Theft, but there are some prudent steps one can take to diminish the chance of becoming a victim. We have outlined some protective steps below in Subsection A. We have also included in Subsection B a suggestion for electronically monitoring your credit report. This, of course, may help you limit the damage to your credit should someone begin misusing your identity because it gives you notice that something is amiss before too much time has passed. We believe the best strategy is to employ measures that are both *preventative* (Subsection A) and *limiting* (Subsection B).

#### **A. Preventative Steps**

##### **1. *Mail and Garbage.***

--The US Postal Service advises to remove mail from your mailbox as soon as you can after it is delivered. It also advises, if possible, to deposit outgoing mail in a blue postal service box rather than leaving it unprotected in your mailbox at home for pickup.

--Shred pre-approved credit applications and other financial documents before discarding them.

--If possible, empty your trash from your home on the day of garbage pickup, so it does not sit for days in an outside trash receptacle, which can be searched by others for personal information about you.

--Shred all documents, which contain personal information on them before putting them in the garbage.

##### **2. *Telephone and Internet.***

--Never give personal or financial information over the telephone or the Internet unless *you* initiated the contact or are sure of the identity of the person with whom you are speaking. Many scam artists call pretending to be someone they are not in an effort to obtain your personal information.

--Don't disclose credit card or other financial account numbers on an Internet Web site *unless* the site offers, "secure transactions", otherwise such communications can be intercepted.

##### **3. *Bank Accounts.***

- On accounts with passwords, choose passwords, which are not obvious choices to someone trying to access your account. For instance, do not use your birth date or mother's maiden name. It is best, if possible to use a mixture of letters and numbers.
- Never leave transaction receipts at ATM machines, or in the trash nearby, on counters at financial institutions, or at gasoline pumps.
- Watch for your monthly financial statements and bills. If you don't get them when they normally arrive contact the bank or creditor.
- Put your work phone number on your checks instead of your home number.
- If you have a PO Box use that address instead of your home address. If you do not have a PO Box use your work address if possible.
- Do not have your Social Security number printed on your checks you can add it if it is necessary but if you have it printed anyone can get it.
- The next time you order checks have only your initials (instead of first name) and last name put on them (e.g. "J.A. Smith", instead of "James A. Smith"). That way if someone steals your checkbook they will not know your full name.

#### **4. *Your Wallet or Purse.***

- Don't carry your Social Security card or birth certificate with you unless you need them that day. Keep them in a secure location like a safe deposit box.
- Photocopy your credit cards and other important cards (like your drivers license). Copy both sides of each license, credit card, etc. That way you will know what you had in your wallet or purse and all of the account numbers and toll free phone numbers to call and cancel. IMPORTANT: Keep the photocopy in a safe place!

#### **5. *Passwords and Social Security Number.***

- Memorize your Social Security number and passwords.
- Do not use your date of birth or mother's maiden name as your password and don't record passwords on papers you carry with you.
- Change your password if you think it may have been compromised.

#### **6. *Credit Cards.***

- Be aware of the expiration dates on your credit cards and contact the issuer if you don't receive a replacement card prior to the expiration date of your existing card. Not receiving a card may mean it has been intercepted in the mail.

- When you receive a new credit card, sign the back immediately. That signature will be matched by merchants against the signature you use when making purchases. Without it, a thief may sign your name however they choose.
- As mentioned above, photocopy both sides of the card so that you have a record of the account numbers and the toll free number to call should your card be lost or stolen.
- If you apply for a credit card and don't receive it as expected, call the issuing institution to insure that it has not fallen into the wrong hands.
- Scrutinize your monthly bills for accuracy. Confirm any suspicious charges immediately. If a thief is using your card, you may be able to stop them from doing further harm.

## **7. Scams.**

- Beware of mail or telephone solicitations that offer prizes or awards--especially if they ask you for personal information or financial account numbers.
- For job seekers, make sure that a purported employer is a bona fide entity before giving it any personal information. There have been many instances of bogus employers asking prospective employees for personal information which was then used for ID Theft.
- Do not respond to incoming phone calls asking you to "confirm" your password, account number, social security number or other personal information. Never give such information to anyone unless you know his or her identity.
- "Nigerian" scams. If someone contacts you to help them move money from their foreign bank account to the US, you are probably the target of what is called the "Nigerian Scam". Have nothing to do with such offers.
- Sign up rosters for school enrollment often ask for social security numbers. Do not give include your number. Rather, go to the school and give it to them in person so others cannot view it.
- If you receive emails offering you a "free credit report", make sure that the sender is a reputable agency. Check with the Better Business Bureau, and also check to see if the return email address really belongs to the agency. It is best also to call the agency to make sure they are legitimate.

--Beware of emails, which purport to be from legitimate companies and ask you to “confirm” information on your account, such as date of birth, social security number, or mother’s maiden name. Legitimate companies will not seek such information in an unsolicited email.

It is impossible to list all the scams currently being perpetrated on the public. Every day there are new ones. If you would like to keep abreast of the latest ploys, one source for information is the “Scambusters” free report on Internet scams. See <http://www.scambusters.org/>

### **B. Limiting the Damage—Credit Monitoring Services**

The FTC estimated that during the year 2000, the average time it took for a person to discover that he or she was the victim of ID Theft was 14 months. That is a lot longer than it takes for significant damage to happen to one’s financial life.

We strongly encourage the use of “credit monitoring services”. Such services typically cost about \$70-\$90 per year and will send you email notifications whenever your credit report is accessed or changes to your credit report occur. That way, you can immediately tell if wrongdoing is afoot and act to prevent it. One such service can be accessed through <http://www.ID-Theft-Security.com/>

## Section IV

### Federal and State Laws

#### A. Federal Laws and Links

**Federal Trade Commission ID Theft Affidavit:** See Appendix A which you may download for free from our web site).

**The Identity Theft and Assumption Deterrence Act:** makes it a federal crime to use another person's identification with the intent to commit any unlawful act. (See Appendix B, which you may download for free from our web site).

**The Fair Credit Reporting Act:** The FCRA establishes the guidelines for credit reporting agencies and dictates timetables and procedures for correcting credit reports. (See Appendix C, which you may download for free from our web site).

**Summary of Electronic Funds Transfer Rules:** FTC summary of Electronic Funds Transfer Act provisions providing protection for transactions involving ATM/debit cards and other electronic transactions. (See Appendix D, which you may download for free from our web site).

**Fair Credit Billing Act:** Dictates the process for correcting billing errors on credit card statements. (See Appendix E, which you may download for free from our web site).

**Fair Debt Collection Practices Act:** This act regulates the practice of debt collection. (See Appendix F, which you may download for free from our web site).

**The Social Security Administration:** <http://www.ssa.gov/>

**U. S. Postal Inspection Service:** <http://www.usps.gov/postalinspectors>

**The Federal Trade Commission:** <http://www.ftc.gov/>

**The Federal Bureau of Investigation:** <http://www.fbi.gov/>

#### B. State Laws

**Alabama** [Alabama Code § 13A-8-190 through 201](#)  
(search Alabama Code for "Identity Theft")

**Alaska** [Alaska Stat § 11.46.565](#)  
(Click Title 11, Chapter 46, Section 565)

**Arizona** [Ariz. Rev. Stat. § 13-2008](#)

**Arkansas** [Ark. Code Ann. § 5-37-227](#)

**California** [Cal. Penal Code § 530.5-8](#)

**Colorado** Does not have specific ID Theft law.

**Connecticut** [Conn. Stat. § 53a-129a \(criminal\)](#)  
[Conn. Stat. § 52-571h \(civil\)](#)

**Delaware** [Del. Code Ann. tit. II, § 854](#)

**District of Columbia** Does not have specific ID Theft law.

**Florida** [2000-Ch0817-Section%20568"Fla. Stat. Ann. § 817.568](#)

**Georgia** [Ga. Code Ann. § 16-9-120, through 128](#)

**Hawaii** [HI Rev. Stat. § 708-839.6-8](#)  
(See statutes and documents)

**Idaho** [Idaho Code § 18-3126](#) (criminal)  
[Idaho Code § 28-51-102](#) (civil)

**Illinois** [720 Ill. Comp. Stat. 5/16 G](#)

**Indiana** [Ind. Code § 35-43-5-3.5](#)

**Iowa** [Iowa Code § 715A.8](#) (criminal)  
Iowa Code § 714.16.B (civil)

**Kansas** [Kan. Stat. Ann. § 21-4018](#)

**Kentucky** [Ky. Rev. Stat. Ann. § 514.160](#)

**Louisiana** [La. Rev. Stat. Ann. § 14:67.16](#)

**Maine** [ME Rev. Stat. Ann. tit. 17-A § 905-A](#)

**Maryland** [Md. Code Ann. art. 27 § 231](#)

**Massachusetts** [Mass. Gen. Laws ch. 266, § 37E](#)

**Michigan** [Mich. Comp. Laws § 750.285](#)  
(See Michigan compiled laws section)

**Minnesota** [Minn. Stat. Ann. § 609.527](#)

**Mississippi** [Miss. Code Ann. § 97-19-85](#)

**Missouri** [Mo. Rev. Stat. § 570.223](#)

**Montana** [Mon. Code Ann. § 45-6-332](#)

**Nebraska** [NE Rev. Stat. § 28-608 & 620](#)

**Nevada** [Nev. Rev. State. § 205.463-465](#)

**New Hampshire** [N.H. Rev. Stat. Ann. § 638:26](#)

**New Jersey** [N.J. Stat. Ann. § 2C:21-17](#)

**New Mexico** [N.M. Stat. Ann. § 30-16-24.1](#)  
(Go to statutes section, Chapter 30)

**New York** [NY CLS Penal § 190.77-190.84](#)

**North Carolina** [N.C. Gen. Stat. § 14-113.20-23](#)

**North Dakota** [N.D.C.C. § 12.1-23-11](#)  
(See consumer protection)

**Ohio** [Ohio Rev. Code Ann. § 2913.49](#)

**Oklahoma** [Okla. Stat. tit. 21, § 1533.1](#)

**Oregon** [Or. Rev. Stat. § 165.800](#)

**Pennsylvania\*** 18 Pa. Cons. State § 4120

**Rhode Island** [R.I. Gen. Laws § 11-49.1-1](#)

**South Carolina** [S.C. Code Ann. § 16-13-500, 501](#)

**South Dakota** [S.D. Codified Laws § 22-30A-3.1.](#)

**Tennessee\*** TCA § 39-14-150 (criminal)  
TCA § 47-18-2101 (civil)

**Texas** [Tex. Penal Code § 32.51](#)

**Utah** [Utah Code Ann. § 76-6-1101-1104](#)

**Vermont** Does not have specific ID Theft law.

**Virginia** [Va. Code Ann. § 18.2-186.3](#)

**Washington** [Wash. Rev. Code § 9.35.020](#)  
(click on title 9, then chapter 35)

**West Virginia** [W. Va. Code § 61-3-54](#)  
(scroll down to § 61-3-54)

**Wisconsin** [Wis. Stat. § 943.201](#)

**Wyoming** [Wyo. Stat. Ann. § 6-3-901](#)

### **U.S. Territories**

**Guam\*** 9 Guam Code Ann. § 46.80

**U.S. Virgin Islands\*** Does not have specific ID Theft law.

