



## Identity Theft Prevention Tips and Commentary

May 11, 2005

An updated version of this report is available at <http://www.demartek.com/IDTheft>

---

*Identity theft*, also known as *ID theft* and *identity fraud*, is a widespread and fast-growing crime. Although potentially anybody can be targeted, there are a number of things that can be done to reduce the risk of becoming an identity theft victim. The recent well-publicized security breaches, ruin of financial reputations and even mistaken arrests of many victims have triggered calls to action by individuals, businesses and government.

This report lists suggestions for individuals and organizations to help reduce the risk of identity theft. The areas covered include the handling of paper documents, telephone-related and computer-related issues. This report also provides references from government agencies for information and assistance and discusses some current and proposed laws. Information specific to the USA and Canada is included.

This free Demartek report is provided for our clients and friends due to the tremendous attention generated by identity theft.

---

## Legal Notices

Copyright © 2005 Demartek. All rights reserved.

**Reproduction guidelines:** you may make copies of this document in its entirety to be distributed free of charge unless otherwise noted. If you quote or reference this document, you must appropriately attribute the contents and authorship to Demartek, and include the Demartek web site [www.demartek.com](http://www.demartek.com) in the attribution.

Opinions presented in this document reflect judgment at the time of publication and are subject to change.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS DOCUMENT, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT AND THE IMPLIED WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. NOTHING CONTAINED IN THIS DOCUMENT IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM DEMARTEK.

Products, brand names or corporate names referenced in this document may be trade names, service marks, trademarks or registered trademarks of their respective companies.

## Table of Contents

Legal Notices.....	2
Table of Contents.....	3
Introduction .....	4
Paper Document Handling.....	5
Get a Good Shredder.....	5
Out-going Mail .....	5
DO NOT MAIL.....	6
Bank Checks.....	7
Retirement Program Cards and Numbers .....	8
Driver’s Licenses.....	8
Military Separation Records (US DD 214) .....	9
Telephone Privacy .....	10
Non-listed and Non-published Numbers .....	10
DO NOT CALL.....	10
Computer Security .....	12
Anti-virus Software .....	12
Firewalls.....	12
Anti-spyware .....	13
Web Browser “Cookies” .....	13
Updates.....	13
Old Computers .....	13
“Phishing” Scams .....	13
Passwords.....	14
Children .....	15
Other Sources of Information and Assistance .....	16
Organizations .....	16
Identity Theft Stories .....	16
Laws and Regulations.....	16
Identity Theft Passport.....	17
Identity Theft Insurance .....	18
Government Agencies.....	19

## Introduction

*Identity theft*, also known as *ID theft* and *identity fraud*, is currently among the fastest growing crimes. Its victims span all categories of people, including those from all age groups, economic backgrounds, race, gender, etc. In many cases the victims and the perpetrators have never met. In some cases, it can be weeks or months before the victims know that the crime has been committed against them and by then the damage has been done.

The most common ways identity thieves obtain information is from stolen or lost wallets and purses and from stealing mail from mailboxes. Sometimes, “dumpster diving” can provide useful information for an identity thief. Dumpster diving is the practice of going through trash looking for documents containing useful information. Some identity thieves use computers to gain information through clever technical attacks or by going through computer security holes left open by organizations that should know better.

It seems that businesses and other organizations have been very efficient, perhaps too efficient, at the distribution of information about their customers and prospective customers. In their efforts to increase sales and consumption in general, they have not given enough thought to the “side-effects” of this widespread distribution of personal data. Many organizations have given little thought to the ways that data can be stolen.

Although some government agencies pass laws to penalize criminals and assist victims, and some businesses establish procedures to reduce the potential for identity theft, individuals must take a fair amount of action to either prevent or recover from identity theft. The serious effect of identity theft is frequently underestimated, as recovery from identity theft often takes years of work. Victims are subjected to embarrassment, are required to repeatedly explain the circumstances of the crime against them, and in some cases have been mistakenly arrested and put in jail.

Security, including physical security and electronic security, is inversely related to convenience. That is, taking steps to increase security will result in less convenience. Conversely, increased convenience results in less security. Identity theft prevention is a discussion about security which is basically an assessment of risk and tradeoffs between practices, procedures, time, money, and convenience. You can't eliminate all identity theft threats, as new threats will emerge. But you can take specific steps to reduce your vulnerabilities to these threats. The suggestions provided in this document may seem inconvenient or perhaps extreme. Each situation is different and so you must analyze the risks and determine which steps are appropriate to take in your setting.

Although government agencies and businesses will find useful information here, it is primarily for the benefit of the individual that we have produced this document.

## Paper Document Handling

Although identity theft has a certain high-tech connotation, much of the prevention and recovery efforts are relatively low-tech. Identity thieves are looking for personal information that they can use, and much of it is readily available. One of the motives for these thefts is the ability to create “instant credit”, purchase goods with this credit, and get somebody else to pay for it. There are several steps that can be taken to reduce or eliminate information about you that might be profitable to identity thieves.

### Get a Good Shredder

To prevent dumpster diving and other techniques that are used to obtain printed information, purchase and use a good office shredder. The shredder should be of the cross-cut variety that produces small pieces of paper. Some shredders are strong enough to shred thin plastic, such as old credit cards. The older variety that simply cuts the paper into long strips does not provide adequate protection, as the strips can be re-attached together. Some recycling centers do not accept shredded paper, so the shredded paper should be put in the trash.

All old financial documents should be shredded. These include banks statements, credit card statements, insurance company documents and any other documents that have your name, address or account number or any other personally identifying information on them. This also includes the envelopes that contain these documents, if they have your name or account number printed on them. Documents such as old checks and deposit slips from closed accounts should also be shredded. Some documents are considered “old” before others. Certain income tax-related documents must be kept for seven years. However, other financial documents can be destroyed before seven years.

In addition, all pages of junk mail that contain your name, address or other information specific to you should be shredded. This would also include the envelopes if they have your name printed on them.

In short, there should be no trash or recycled paper leaving your residence that includes your name and other personal information that is legible.

### Out-going Mail

Take all out-going mail and packages to the post office, package delivery office, etc. Do not leave out-going mail or packages in your mailbox at home or on your front doorstep for pickup. Identity thieves are looking through mail left in home mail boxes for any checks you may have written, or anything with your name and account number information on it. Identity thieves also look for mailboxes in obscure locations or mailboxes that are stuffed full of envelopes. The thieves will take mail from these mailboxes. Once in their possession, they can alter the checks or copy your account number and reproduce checks

using your account number and other personal information pre-printed on your original checks.

## DO NOT MAIL

One way to help prevent theft of personal information through the mail is not to have various offers created and sent to you. There are many organizations who want to sell you their products, probably far more than you can realistically use or afford. There are many businesses that generate revenue by simply selling lists of existing or prospective customers to other businesses. There are some things you can do to slow down the distribution of your name and other personal information. You can ask to have your name removed from mailing lists in several ways, all of which we recommend. Some of these are general lists and some are more specific.

- **US Direct Marketing Association (DMA) Mail Preference Service (MPS)** – This service will allow you to significantly reduce the amount of unsolicited national advertising you receive at home. When you register with MPS, your name and address are placed on a "do-not-mail" file. All DMA members are required to run their list of prospective customers against the MPS file to remove the individuals who have registered with MPS from their mailings. This service is also available to non-DMA members. To register to be removed from the DMA-controlled mailing lists, visit their website at: <http://www.dmaconsumers.org/cgi/offmailinglist> or write to:

Mail Preference Service  
Direct Marketing Association  
PO Box 643  
Carmel, NY 10512

- **Canadian Marketing Association (CMA) Do Not Contact Service** – Similar to the US Direct Marketing Association. They have a service that allows you to get your name, address and telephone number removed from mailing, telephone and fax lists in Canada by visiting: [http://www.cmaconsumersense.org/marketing\\_lists.cfm](http://www.cmaconsumersense.org/marketing_lists.cfm).
- **Opt Out Prescreen Service** – This service will allow you to reduce the number of pre-approved credit offers sent to you. Your rights as a consumer include the ability to "Opt-Out", which prevents consumer credit reporting companies from using your credit file information for pre-approved offers of credit or insurance. You may request to Opt-Out from pre-approved offer lists for five years or permanently. Be sure to specify which you prefer. To register for this Opt Out service, visit their website at: <https://www.optoutprescreen.com> or call 888-5-OPT-OUT (888-567-8688).
- **Other Credit Offers from Banks** – This requires slightly more action on your part than the first three items above. When you receive unsolicited credit card offers from banks, airlines and other businesses, the application will include a telephone number that you can call to enroll. Rather than applying for their credit card, call the telephone number and ask to be placed on their "DO NOT MAIL" list for

credit card offers. They must honor this request, and their customer service representative will generally follow the “script” they use for this process. You will have to repeat this process for each credit card offer you receive, but after a short time, you will no longer receive these offers. After they have confirmed that your name and address are on their DO NOT MAIL list, you should shred the application as described in the “shredder” section above.

- **Preprinted Credit Card Checks** – You may receive pre-printed checks from your credit card company that can be used like regular checks but charge your credit card account, often with extra fees. These are a favorite of identity thieves because once in their possession, these are especially easy to use. The thieves look for credit card checks in your mail and like to steal them before you can retrieve your mail. You can call your credit card company and ask them to not send you credit card checks in the future. If you have received these already and actually plan to use them, you should keep them in a secure location. If you don’t plan to use these credit card checks you should shred them and get them discontinued.

## Bank Checks

Your regular bank checks should be kept in a secure location. In addition, your pre-printed checks should be the “high-security” type checks with at least eight security features included. Some of these security features are visible and some are invisible. These high-security checks are more difficult to forge. Don’t take checks with you unless you plan to write a check for a specific purpose.

Do **NOT** have your Social Security Number, driver’s license number or other government identification numbers printed on your checks.

Some people do not have their full name printed on their checks, but only first and middle initials with their full last name. If the identity thief does not know your full name and has stolen your checks, they won’t necessarily know how to sign the check.

**Check Washing** is the process of using household cleaning products to erase the ink on selected portions of checks, changing the payee and typically increasing the amount of the check. Some identity thieves have become quite good at employing this technique. Use a pen that writes with an indelible ink, such as some gel inks, that soaks into the paper fibers when writing checks, as these tend to be more difficult to erase.

When sending checks through the mail, wrap the check and other items inside a blank sheet of paper, or use a security envelope, as some envelopes provided with statements are relatively cheap and are see-through.

When you mail checks, be sure to take them directly to the post office.

## Retirement Program Cards and Numbers

Several countries have national retirement programs with an account number for each individual who is eligible. In Canada, this number is known as the Social Insurance Number (SIN). In the United States, this is known as the Social Security Number (SSN). Although the programs are not identical, the basic uses of these numbers are similar. They are used primarily for national tax and retirement programs, and the numbers should be kept confidential. However, over time, especially in the USA, these numbers have been used as an identifier for many purposes, without regard to potential data privacy problems.

The numbers appear on an official card issued by the government. You may need to show your card to your employer when you start a job, but sometimes employers will just want the correct number. Otherwise, these cards should be kept in a secure location and not carried in your purse or wallet. If found or stolen, these numbers are priceless in the hands of an identity thief. You should not put your SIN or SSN on your checks. It should not appear on your driver's license. Do not post it on the Internet.

In the USA, the Social Security Administration provides a statement annually to workers and former workers aged 25 and older, and at for workers of any age who request them. It is a good idea to compare the information included in this statement to the amounts of money you report on your taxes. If the amount for a given year is larger on the Social Security statement than is on your taxes, it is possible that somebody else has been using your Social Security Number for payroll purposes, and may also be applying for credit using your Social Security Number.

These numbers should not be given out casually. If you are asked for your SSN or SIN, you should ask several questions:

- Is this required by law?
- How will this number be used?
- Can you or the organization asking for it substitute an alternative identifier?

## Driver's Licenses

Make sure that your driver's license does not have your SSN or SIN printed on it. Although you may be required by law to provide this number to the Driver's License officials, be sure to ask if this number will be printed on your driver's license, and indicate that you do not want it printed on the license.

Be very reluctant to give your driver's license or driver's license number to anybody except legitimate law enforcement officers. There have been cases of identity theft that began with unscrupulous businesses requesting driver's license information for "insurance purposes" who then sold the information on the driver's licenses to identity thieves.

In some jurisdictions, one can get a report of outstanding tickets associated with a particular driver's license. It may be worth the small fee to see if somebody else has been getting tickets under your name.

### **Military Separation Records (US DD 214)**

In the USA, the *Report of Separation*, Form DD 214, also known as "military discharge papers", is issued to members of the military when they leave military service. Form DD 214 contains personal information that could be used by an identity thief. As an option, many states allow the filing of these forms with the local county courthouse so that copies can be more easily obtained rather than requesting official copies from the National Personnel Records Center (NPRC). These forms, either the originals or certified copies, are sometimes needed in order to obtain veterans benefits. The disadvantage of filing copies of DD 214 with the county courthouse is that the information on the form becomes a public record, available to anyone. In the last few years, many states have changed their laws to provide for some measure of confidentiality concerning DD 214. Some states still regard DD 214 as a public record with no confidentiality. Some states do not record form DD 214.

The states have taken different approaches with respect to form DD 214. To help reduce identity theft, some states allow for some of the information on DD 214 to be redacted that has been recorded in the local courthouses. Some jurisdictions allow for a *Request for Exemption from Public Disclosure of Discharge Papers* so that only the veteran, veteran's next of kin, or other specifically designated representative can access these records. Some jurisdictions automatically restrict access to DD 214. Some jurisdictions allow historical and genealogical research on DD 214 records after 75 years or other similarly long time period after the recording date.

There have been cases of identity theft where the thief gathered information regarding many veterans obtained from DD 214 filings in their local area.

## Telephone Privacy

Sometimes identity thieves attempt to obtain your personal information via the telephone. There are some things you can do to make your telephone information less visible.

### Non-listed and Non-published Numbers

There are three basic categories of telephone numbers. These are main listing, non-listed and non-published telephone numbers. Of the three types, the non-published number is the most secure.

- **Main Listing** – Your name, address and telephone number are included in the printed telephone directories and are available through Directory Assistance. Your name and telephone number are also included on lists the telephone company sells to other companies for marketing purposes.
- **Non-listed** – Your name, address and telephone number are not included in the printed telephone directories, but are available through Directory Assistance. This is also known as an “unlisted” number.
- **Non-published** – Your name, address and telephone number are not included in the printed telephone directories and not available through Directory Assistance. Your name and telephone number are not included on lists the telephone company sells to other companies for marketing purposes.

The non-listed and non-published “service” is usually available for a monthly fee. You have to ask for either non-listed or non-published numbers.

### DO NOT CALL

There are national and local government “DO NOT CALL” registries available. There are also voluntary commercial registries available. Adding your telephone number to these registries will reduce the numbers of unsolicited telephone calls you receive, and reduce the publication and distribution of your telephone number.

- **USA DO NOT CALL Registry** – In the USA, the federal national “DO NOT CALL” registry is available at <https://www.donotcall.gov> or in Spanish at: [https://www.donotcall.gov/default\\_es.aspx](https://www.donotcall.gov/default_es.aspx). You can also call 1-888-382-1222. This allows you to put your telephone number on the “DO NOT CALL” list for five years. Placing your number on the National Do Not Call Registry will stop most telemarketing calls, but not all. Because of limitations in the jurisdiction of the FTC and FCC, calls from or on behalf of political organizations, charities, and telephone surveyors are still permitted, as are calls from companies with which you have an existing business relationship, or those to whom you’ve provided express agreement in writing to receive their calls. Although the national registry exists,

some companies choose to ignore it and are given citations and/or fined. A listing of these companies can be found at: <http://www.fcc.gov/eb/tcd/DNCall.html>.

- **States DO NOT CALL Registry** – In addition, many of the States in the USA have their own state-wide “DO NOT CALL” registries. You can find these by using your favorite Internet search engine and looking for the phrase “do not call” and your State name or by contacting your State consumer protection agency.
- **Canada DO NOT CALL Registry** – In Canada, similar legislation to the US “DO NOT CALL” registry is being discussed due to the popularity of the US program. In 2004, the Telecom Decision CRTC 2004-35, Review of Telemarketing Rules, the Canadian Radio-television and Telecommunications Commission (CRTC) concluded that a national Do Not Call List has considerable merit. However, the commission found it could not establish a list without changes to legislation that would enable it to impose fines for non-compliance, establish a third-party administrator to operate a database, and set fees to recover costs associated with maintaining the list. There is ongoing discussion in this area.
- **US Direct Marketing Association Telephone Preference Service** – In the USA, the Direct Marketing Association maintains a “Telephone Preference Service” list similar to its “Mail Preference Service” list. You can add your name and telephone number to this list by visiting <http://www.dmaconsumers.org/cgi/offtelephone> or writing to:  

Telephone Preference Service  
Direct Marketing Association  
PO Box 1559  
Carmel, NY 10512
- **Canadian Marketing Association (CMA) Do Not Contact Service** – Similar to the US Direct Marketing Association. They have a service that allows you to get your name, address and telephone number removed from mailing, telephone and fax lists in Canada from one screen by visiting [http://www.cmaconsumersense.org/marketing\\_lists.cfm](http://www.cmaconsumersense.org/marketing_lists.cfm).

## Computer Security

Much has been written about computer security so the focus here will be on some basics with the goal of reducing your vulnerability to identity theft via computer. The best defense is a multi-layered one, and several layers will be discussed here. There are many advanced topics in these areas for which you can easily find additional information.

### Anti-virus Software

Some computer viruses and worms are designed to look for personal information on your computer and send it to an external location. The variants of *Antinny*, *Dumaru*, *PWSteal*, *Goldpay* and *Trojan.Upbit* are just a few of the known examples that look for personal information.

Get a good anti-virus package from one of the well-known vendors in this area, and make sure that you keep up with the weekly updates to the virus definitions.

### Firewalls

Especially if you have a broadband or “always-on” connection to the Internet, firewalls are a necessity. There are two basic types: hardware and software. We recommend that you use both types of firewalls.

Windows XP Service Pack 2 (SP2) has a software firewall in it. If you don't have a better software firewall, use this one. There are many other good software firewall solutions for Windows, Linux systems and others. Get one and use it.

In addition, we recommend that hardware firewalls also be deployed, even in homes and small offices, if you have a broadband connection. Hardware firewalls provide consistent protection to all computers connected in a small network even if one of those computers does not have its defenses turned on or is otherwise compromised. Hardware firewalls also provide another layer of defense and help to slow down or prevent certain incoming attacks. Hardware firewalls are generally pre-configured to close or “stealth” TCP/IP ports for traffic originating from the outside. If a computer behind a hardware firewall is compromised so that it opens certain of its own TCP/IP ports and “listens” for commands from an external source, the hardware firewall will block that traffic before it gets to the computer on the internal network. There are several good brands of firewalls or firewall-routers available. The models designed for home use are relatively simple and low cost.

Hardware firewalls also make it possible to block access to specific sites or sites with certain text strings in their name for all traffic originating from within your network.

## Anti-spyware

Spyware has generated much media attention recently. Its purpose is to gather information from your computer and make it available to an external entity. Some of it is advertising-related, and some of it is looking for personal information or keystrokes (user names and passwords). There are several good anti-spyware solutions, and some of the anti-virus software companies either have or soon will have anti-spyware solutions. Make the relatively small investment to protect yourself from spyware.

## Web Browser “Cookies”

Many Internet web sites use “cookies”. These are small files with data about you or your current Internet session. Some of these cookies are useful for some sites that you visit frequently, but many are only useful to companies that like to track your Internet usage. You might be surprised at how many cookies you have, even for sites that you did not specifically visit. Periodically, you should delete the cookies from sites that you don’t want tracking you.

In addition, most web browsers allow you to “always block” cookies from certain sites. We recommend that you add advertising and other sites that you don’t want tracking you to the “always block” category.

## Updates

All computer operating systems have security holes in them, and most have a procedure for obtaining patches and security updates over the Internet. Some also provide security updates that can be ordered on a CD-ROM. Good security practice requires diligence, and keeping up with security updates is part of good security practice.

## Old Computers

If you are in a position to donate a computer to a charity, relative, friend, etc., be sure that you have properly removed any personal data from that computer and its storage components (disk drives, backup tapes, USB drives, memory cards, etc.) before it leaves your control. You need to do more than simply delete the files. When you delete a file, the computer simply removes the entry from the table of contents, but does not actually delete the data where the file resides. Each piece of storage media (disk, tape, memory card, etc.) should be at least reformatted before you give it away. You can also get programs that will write random data patterns (multiple times) so that any data that might exist is scrubbed. These programs are sometimes known as “wipe” utilities.

## “Phishing” Scams

Many criminals attempt to get you to give them your personal information via email. They send you requests for your information, disguised as an email from a bank, Internet Service

Provider (ISP) or other institution that you might trust. The text of the email generally refers to a system upgrade, possible fraudulent activity with some accounts or some other bogus reason that information needs to be “confirmed”. Sometimes these emails suggest that some accounts may be suspended until the information is confirmed.

The best course of action is to consider these emails as junk email and simply delete them. The legitimate bank or other organization already has your information and does not need you to confirm it.

If you feel the need to take additional action, you can forward the email to the email fraud address for the bank. Banks generally provide information about attempted email fraud on their websites. Banks work with law enforcement and some Internet service providers to shutdown the source of these emails as quickly as possible.

## Passwords

There are at least four categories of bad passwords. You should choose passwords that do not fall into any of these categories. Strong passwords use a mixture of letters, numbers and special characters. Choose a password that you can remember but is strong enough to protect the data behind it. You should also memorize passwords and not write them down.

1. **Blank password** – No password at all is no security and simply invites theft.
2. **Simple password** – Simple passwords are those that take little thought for you to create and little effort for a thief to guess. The word *password* and the word *secret* are two prime examples. There are automated attack tools that will attempt to guess passwords. A few other examples of this type of password (taken from some of these automated attack tools) are: *abc, admin, administrator, debug, diag, god, guest, home, owner, pass, root, server, sexy, test, user, xyz, 111, 123, 321, 1234, 4321, 111111, abcdefg, abc123, asdfgh* and others.
3. **Default password** – Any vendor-supplied default password. These are easily obtainable over the Internet in a few minutes. You should change the default password for any system in your control as soon as possible.
4. **Personal information password** – Anything based on personal information. This would be names of your spouse, children, pets, favorite sports team, favorite singer or band, birthdays, special license plates, etc. If a thief knows something about you (and sometimes they do), it might be a clue towards guessing your password.

## **Children**

In addition to protecting one's own identity, many people need to also consider protecting the identity of their children. Some identity theft cases have happened to infants or very young children, because their personal information was stolen. In some divorce cases, a parent who has bad credit may use the child's identity to get services such as telephone, utilities, etc.

It is a good idea to take the same steps provided in the previous sections for your children, or if they are old enough, teach them to take these steps.

## Other Sources of Information and Assistance

There are numerous sources of information regarding identity theft, including what to do if you are a victim of identity theft. Some of these sources have been victims themselves and describe the kinds of troubles they experienced on the way to cleaning up after the identity theft mess. Some are privacy rights organizations with excellent information. Others are government agencies that can provide some assistance. Other sources provide background on laws that have been passed or are bills that have been proposed to address identity theft.

### Organizations

These organizations have excellent information on identity theft and explain what to do about it. They also provide information in related areas such as privacy. Their Internet links are simply listed here for your reference. Some are non-profit organizations.

- <http://www.privacyrights.org/identity.htm>
- <http://www.idtheftcenter.org>
- <http://www.pirg.org/consumer/credit/>
- <http://www.identitytheft.org/>
- <http://www.vaonline.org/fraud.html>
- <http://www.prevent-id-theft.com/>
- <http://www.identity-theft-help.us/>
- <http://www.identity-theft-protection.com/>

### Identity Theft Stories

These are actual accounts from identity-theft victims. Problems encountered by identity theft victims include checks not being accepted, collection letters arriving for things purchased by the identity thief, and numerous others. One victim was mistakenly arrested, strip-searched and jailed.

- <http://www.christianitytoday.com/tcw/2004/006/11.70.html>
- <http://www.kaimin.org/viewarticle.php?id=2887>
- <http://www.bbbonline.org/idtheft/stories.asp>

### Laws and Regulations

Laws have been passed and regulations approved that are an attempt to bring attention to the problem of data security breaches. These are a response to a somewhat cavalier attitude on the part of some businesses, universities and government agencies with respect to protecting the confidentiality of certain data. Various people have accused these organizations of being irresponsible or negligent. We would not be surprised if class-action lawsuits were brought against some of these organizations. A number of organizations have made news headlines for the wrong reasons. ChoicePoint, Bank of America, Seisint

(owned by LexisNexis), University of Mississippi, Boston College, University of California at Berkeley, The Wharton School of Business and others have apparently had some of their data stolen or possibly even sold it to criminals.

- **California Security Breach Information Act** (effective July 1, 2003) – This law, also known as SB 1386, requires businesses and governments to notify individuals if a database containing certain personal data is compromised. It affects those organizations that have California residents as their customers or clients. It specifies that either individual notification is required, or in cases where a large number of people may be affected, that notification can come through the news media.
- **US Federal Reserve Board** (effective March 23, 2005) – In response to some of the recently publicized security breaches, the US Federal Reserve issued a ruling that states "when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused... If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." The details can be found at: <http://www.federalreserve.gov/BoardDocs/Press/bcreg/2005/20050323/default.htm>

Other States are considering legislation similar to the California law. In addition, there is discussion in the United States Congress of a national law similar to the California law.

Another idea that is gaining momentum as a way for consumers to protect themselves before an identity theft occurs is the concept of a credit "freeze". This would prevent anybody from opening new instant credit accounts. The states are in various phases of discussion for legislation in this area. A good article describing this appeared in March 2005 on MSNBC's web site at: <http://www.msnbc.msn.com/id/7276133>.

### **Identity Theft Passport**

Some states have an interesting program called the *Identity Theft Passport* that provides government verification that a person is an identity theft victim in order to prevent false arrest and provide some other assistance. Arkansas, Montana, Ohio, Oklahoma and Virginia currently have these programs. Other states, including Nebraska, Nevada, New Mexico, Rhode Island and others are considering similar legislation.

The programs are not identical, but function in similar ways. The basic premise is that an identity theft victim completes an affidavit certifying that they are a victim. This affidavit includes information about the police report and other specific information about the victim and the crime. This affidavit is submitted to the Attorney General or state Bureau of Investigation. Typically a photo, fingerprints or other forms of positive identification are required along with the affidavit. After some period of investigation, the state agency issues

the “Identity Theft Passport” that can be presented to law enforcement officials as needed. When presented to law enforcement, they will perform a check into a special identity theft database to verify the identity of the person holding the identity theft passport. The process of obtaining an identity theft passport may also include expungement of mistaken records such as arrests, charges, etc. Typically, the information about a specific identity theft passport is sealed and not considered a public record. Because each case of identity theft may be unique, the specific steps taken for each case may differ slightly.

Virginia was the first state to create an identity theft passport program. Its law went into effect on July 1, 2003. They have a well-defined process for identity theft victims. Ohio and Oklahoma created their programs in 2004. Ohio also has a well-defined process for identity theft victims. Oklahoma’s process is not yet widely promoted, but they are working with identity theft victims. Arkansas and Montana passed their laws in March 2005, but the processes in those states are not fully defined yet.

Because this is a relatively new initiative, currently the main challenge is for awareness of the programs, both for individual identity theft victims and for law enforcement.

It is unclear if the identity theft passport issued in one state would be accepted in a different state. We believe that other states will also create identity theft programs. It is possible that the federal government will create a national identity theft passport.

Resources for the identity theft passport programs are listed below.

- Virginia: [http://www.oag.state.va.us/Protecting/Consumer%20Fraud/identity\\_theftfaq.htm](http://www.oag.state.va.us/Protecting/Consumer%20Fraud/identity_theftfaq.htm)
- Ohio: [http://www.ag.state.oh.us/site\\_map/id\\_theft.htm](http://www.ag.state.oh.us/site_map/id_theft.htm)
- Oklahoma: <http://www.osbi.state.ok.us/Investigative/ComputerCrime.htm>
- Arkansas: <http://www.ag.state.ar.us/itp/passport.htm>
- Montana: <http://www.doj.state.mt.us/enforcement/computercrime.asp>

Similar to some aspects of the identity theft passport program is the process in some states to have certain court records expunged for identity theft victims. Victims need to petition the court in specific jurisdictions, and this process is not as centrally organized as the identity theft passport programs.

### **Identity Theft Insurance**

Recently, insurance has become available that provides some assistance for identity theft victims. Some insurance companies are offering identity theft insurance as an endorsement to a homeowner’s or renter’s insurance policy or as stand-alone policies. Some banks are offering it with checking accounts. Some employers are offering it as a fringe benefit.

These policies typically cost less than \$100 and provide \$15,000 to \$25,000 of coverage. This insurance provides reimbursement for expenses related to recovery from identity

theft. Some of the expenses, such as attorney's fees, may require prior consent of the insurer.

## Government Agencies

Government agencies provide a wealth of information about identity theft and what to do about it. Many are listed here for the USA and Canada.

### Canada

- [http://www.safecanada.ca/identitytheft\\_e.asp](http://www.safecanada.ca/identitytheft_e.asp)
- [http://www.privcom.gc.ca/fs-fi/02\\_05\\_d\\_10\\_e.asp](http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp)

### USA – National

- <http://www.consumer.gov/idtheft>
- <http://www.usdoj.gov/criminal/fraud/idtheft.html>
- [http://www.ncjrs.org/spotlight/identity\\_theft/programs.html](http://www.ncjrs.org/spotlight/identity_theft/programs.html)
- [http://www.pueblo.gsa.gov/cic\\_text/money/identity-reduce/identity-reduce.htm](http://www.pueblo.gsa.gov/cic_text/money/identity-reduce/identity-reduce.htm)

### USA – 50 States

The National Conference of State Legislatures has a good listing of identity theft laws by State. Not all States have specific identity theft laws.

- <http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm>

Most states provide some identity theft resources, although some have done a better job than others. These are often found through the Attorney General or Consumer Protection Agencies. Some are through State or local police departments.

Some of these URLs are rather long, but they are functional as of the date of this publication.

### Alabama

- <http://www.familyprotection.alabama.gov/identity.cfm>

### Alaska

- <http://www.law.state.ak.us/department/civil/consumer/cpindex.html>
- <http://www.law.state.ak.us/consumer>

### Arizona

- <http://www.azag.gov/cybercrime>
- <http://www.dps.state.az.us/azvictims/identity/default.asp>
- <http://www.ci.phoenix.az.us/POLICE/idthef1.html>

## Arkansas

- <http://www.ag.state.ar.us/consumer/ca32.htm>
- <http://www.ag.state.ar.us/citserve/home.htm>

## California

- <http://www.ag.ca.gov/idtheft>
- <http://www.idtheftsummit.ca.gov>

## Colorado

- <http://www.ago.state.co.us/idtheft/welcome.htm>

## Connecticut

- <http://www.ct.gov/dcp/cwp/view.asp?a=1629&Q=289476&PM=1>

## Delaware

- <http://www.state.de.us/attgen/fraud/consumerprotection/consumerprotection.htm>

## Florida

- <http://www.fdle.state.fl.us/Fc3/NewFC3Site/idtheft.html>

## Georgia

- <http://www2.state.ga.us/GaOCA/broidtheft.htm>
- [http://www.gadbf.org/phishing\\_scams.htm](http://www.gadbf.org/phishing_scams.htm)
- [http://www.cobbsheriff.org/Operations/Identity\\_fraud.htm](http://www.cobbsheriff.org/Operations/Identity_fraud.htm)

## Hawaii

- [http://www.hawaii.gov/dcca/helping\\_hand/identity\\_theft](http://www.hawaii.gov/dcca/helping_hand/identity_theft)
- <http://www.honoluluupd.org/community/idtheft.htm>

## Idaho

- <http://www2.state.id.us/ag/consumer/privacy.htm>
- <http://www2.state.id.us/ag/consumer/tips/IdentityTheft.pdf>

## Illinois

- [http://www.ag.state.il.us/consumers/consumer\\_publications.html](http://www.ag.state.il.us/consumers/consumer_publications.html)
- <http://www.state.il.us/treas/PersFinance/ID-theft.htm>
- <http://illinoisissues.uis.edu/features/2002mar/name.html>

## Indiana

- [http://www.in.gov/attorneygeneral/consumer/prevention/identity\\_theft.html](http://www.in.gov/attorneygeneral/consumer/prevention/identity_theft.html)
- <http://www.in.gov/dfi/education/IdThieve.html>
- [http://www.in.gov/legislative/senate\\_democrats/idtheft.html](http://www.in.gov/legislative/senate_democrats/idtheft.html)

## Iowa

- <http://www.state.ia.us/government/ag/idavoid.htm>
- <http://www.state.ia.us/government/ag/ncpw-id.htm>
- [http://www.iowaattorneygeneral.org/consumer/brochures/avoid\\_identitytheft.html](http://www.iowaattorneygeneral.org/consumer/brochures/avoid_identitytheft.html)
- <http://www.dot.state.ia.us/mvd/omve/theft.htm>
- <http://www.iowastatebanks.com/banking/identityTheft.htm>

## Kansas

- <http://www.ksag.org/Publications/ConsumerCorner/ID/>
- [http://www.ksag.org/Publications/ConsumerCorner/ID/111204\\_id\\_protection.htm](http://www.ksag.org/Publications/ConsumerCorner/ID/111204_id_protection.htm)
- [http://www.ksag.org/Publications/ConsumerCorner/ID/100803\\_id\\_theft\\_protection.htm](http://www.ksag.org/Publications/ConsumerCorner/ID/100803_id_theft_protection.htm)

## Kentucky

- <http://ag.ky.gov/cp/idtheft.htm>
- <http://ag.ky.gov/cp/idthefttips.htm>

## Louisiana

- <http://www.ag.state.la.us/publications/identitytheft.htm>

## Maine

- <http://www.state.me.us/sos/IDfraud.htm>
- <http://www.maine.gov/ag/index.php?r=protection&s=identitytheft&t=>

## Maryland

- <http://www.oag.state.md.us/consumer/idtheft.htm>
- <http://www.oag.state.md.us/Press/2003/0203b03.htm>

## Massachusetts

- <http://www.ago.state.ma.us/sp.cfm?pageid=1153>
- <http://www.ago.state.ma.us/sp.cfm?pageid=1610>
- [http://www.masschiefs.org/hottopics/hot\\_identity.html](http://www.masschiefs.org/hottopics/hot_identity.html)
- <http://www.mass.gov/portal/index.jsp?pageID=ocasubtopic&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca>
- [http://www.worcesterda.com/Consumer\\_Info/textversions/identity\\_theft\\_protectt.htm](http://www.worcesterda.com/Consumer_Info/textversions/identity_theft_protectt.htm)

## Michigan

- [http://www.michigan.gov/documents/ID\\_Theft\\_94764\\_7.pdf](http://www.michigan.gov/documents/ID_Theft_94764_7.pdf)
- [http://www.preventcrime.net/identity\\_theft.htm](http://www.preventcrime.net/identity_theft.htm)

## Minnesota

- <http://www.ag.state.mn.us/consumer/Privacy/default.htm>
- <http://www.ag.state.mn.us/consumer/privacy/guardingyprivacy/default.htm>
- [http://www.hsem.state.mn.us/Hsem\\_Subcategory\\_Home.asp?scatid=63&catid=4](http://www.hsem.state.mn.us/Hsem_Subcategory_Home.asp?scatid=63&catid=4)

## Mississippi

- <http://www.ago.state.ms.us/divisions/consumer>

## Missouri

- <http://ago.missouri.gov/publications/publications.htm>
- <http://missourifamilies.org/features/consumerarticles/idtheft.htm>

## Montana

- <http://www.doj.state.mt.us/enforcement/computercrime.asp>

## Nebraska

- [http://www.ago.state.ne.us/content/id\\_theft\\_info.html](http://www.ago.state.ne.us/content/id_theft_info.html)
- <http://www.nebankers.org/public/consumer/consumeralerts/idfraud.html>

## Nevada

- <http://ag.state.nv.us/privacy.htm>
- <http://ag.state.nv.us/agpress/2005/IDENTITY%20THEFT%20PREVENTION.pdf>

## New Hampshire

- <http://doj.nh.gov/consumer/sourcebook/identity.html>
- [http://www.state.nh.us/liquor/fictitious\\_identification.shtml](http://www.state.nh.us/liquor/fictitious_identification.shtml)

## New Jersey

- <http://www.state.nj.us/lps/ca/brief/id.htm>
- <http://www.state.nj.us/lps/dcj/idtheft.htm>
- [http://www.state.nj.us/lps/dcj/idtheft/id\\_actions.htm](http://www.state.nj.us/lps/dcj/idtheft/id_actions.htm)
- <http://www.state.nj.us/lps/njsp/tech/identity.html>
- <http://www.state.nj.us/dobi/identitytheft.htm>
- <http://www.state.nj.us/dobi/creditreport6.htm>

## New Mexico

- <http://www.nmaging.state.nm.us/idtheft.html>
- <http://www.ago.state.nm.us/know/idtheft/idtheft.htm>
- <http://www.ago.state.nm.us/pio/onyourbehalf/Identity%20Theft.htm>
- <http://www.ago.state.nm.us/pio/onyourbehalf/idtheft04creditcards.htm>

## New York

- [http://www.oag.state.ny.us/consumer/tips/identity\\_theft.html](http://www.oag.state.ny.us/consumer/tips/identity_theft.html)
- [http://www.oag.state.ny.us/consumer/tips/id\\_theft\\_victim.html](http://www.oag.state.ny.us/consumer/tips/id_theft_victim.html)
- [http://www.nyc.gov/html/nypd/pdf/chfdept/identity\\_theft.pdf](http://www.nyc.gov/html/nypd/pdf/chfdept/identity_theft.pdf)
- <http://www.newyork.bbb.org/identitytheft/resources.html>
- <http://www.longislandexchange.com/identity-theft.html>

## North Carolina

- [http://www.ncdoj.com/consumerprotection/cp\\_idtheft.jsp](http://www.ncdoj.com/consumerprotection/cp_idtheft.jsp)
- [http://www.ncdot.org/dmv/other\\_services/licensetheft/identityTheft.html](http://www.ncdot.org/dmv/other_services/licensetheft/identityTheft.html)
- <http://www.ncdoj.com/DocumentStreamerClient?directory=PressReleases/&file=IDtheftlegislation05.pdf>

## North Dakota

- <http://www.ag.state.nd.us/cpat/idtheft/idtheft.htm>
- <http://www.ag.state.nd.us/cpat/consumerinfo.htm>

## Ohio

- [http://www.ag.state.oh.us/site\\_map/id\\_theft.htm](http://www.ag.state.oh.us/site_map/id_theft.htm)
- <http://www.ag.state.oh.us/contact/hotline.htm>
- <http://www.ohioconsumers.org>
- <http://www.ohioconsumers.org/slides/IDtheft2005.pdf>

## Oklahoma

- <http://www.odl.state.ok.us/usinfo/pubs/idtheft.pdf>
- <http://www.insurancejournal.com/news/southcentral/2004/06/09/42995.htm>

## Oregon

- [http://www.leg.state.or.us/comm/commsrvs/background\\_briefs2004/Public%20Safety/IF\\_Identity\\_Theft2004.pdf](http://www.leg.state.or.us/comm/commsrvs/background_briefs2004/Public%20Safety/IF_Identity_Theft2004.pdf)

## Pennsylvania

- [http://www.attorneygeneral.gov/press/cons\\_advis/Feb03.cfm](http://www.attorneygeneral.gov/press/cons_advis/Feb03.cfm)
- <http://www.pccd.state.pa.us/pccd/lib/pccd/press/pccdidtheftrelease120604.doc>
- <http://www.pccd.state.pa.us/pccd/lib/pccd/publications/miscellaneous/identitytheftlawsresources.pdf>

## Rhode Island

- <http://www.risp.state.ri.us/identity.php>

## South Carolina

- [http://www.scconsumer.gov/publications/consumer\\_alert/protect\\_privacy.pdf](http://www.scconsumer.gov/publications/consumer_alert/protect_privacy.pdf)
- <http://www.scfederal.org/IDTheft/info.html>

## South Dakota

- <http://www.state.sd.us/attorney/applications/documents/oneDocument.asp?DocumentID=703>
- <http://www.state.sd.us/attorney/office/publications/pdf/Privacy.pdf>

## Tennessee

- <http://www.tennessee.gov/safety/idtheft.htm>
- <http://www.attorneygeneral.state.tn.us/cpro/idtheft.htm>

- <http://www.state.tn.us/consumer/idtheft.html>

## Texas

- <http://www.oag.state.tx.us/consumer/idtheft.shtml>
- [http://www.oag.state.tx.us/AG\\_Publications/pdfs/idtheft\\_pf.pdf](http://www.oag.state.tx.us/AG_Publications/pdfs/idtheft_pf.pdf)
- <http://www.oag.state.tx.us/newspubs/opeds/200302blues.shtml>

## Utah

- <http://www.idtheft.utah.gov>
- [http://www.sbi.utah.gov/finanical\\_crimes/idtheft.html](http://www.sbi.utah.gov/finanical_crimes/idtheft.html)
- [http://hsdaas.utah.gov/protect\\_your\\_id.htm](http://hsdaas.utah.gov/protect_your_id.htm)

## Vermont

- [http://www.dps.state.vt.us/vtsp/id\\_theft.htm](http://www.dps.state.vt.us/vtsp/id_theft.htm)

## Virginia

- [http://www.oag.state.va.us/Protecting/Consumer%20Fraud/identity\\_theftfaq.htm](http://www.oag.state.va.us/Protecting/Consumer%20Fraud/identity_theftfaq.htm)
- [http://www.oag.state.va.us/PDF\\_files/IDTheftBook02.pdf](http://www.oag.state.va.us/PDF_files/IDTheftBook02.pdf)
- <http://www.oag.state.va.us/oagstuff/protecting/consumer%20fraud/identity%20theft.doc>

## Washington

- [http://www.atg.wa.gov/consumer/idprivacy/idtheft\\_index.shtml](http://www.atg.wa.gov/consumer/idprivacy/idtheft_index.shtml)
- <http://www.atg.wa.gov/consumer/idprivacy/>

## West Virginia

- <http://www.wvs.state.wv.us/wvag/consumer/online.html>
- <http://www.wvs.state.wv.us/wvag/press/2004/march/ID%20Theft.htm>

## Wisconsin

- [http://www.doj.state.wi.us/columns/per\\_info.asp](http://www.doj.state.wi.us/columns/per_info.asp)
- [http://www.doj.state.wi.us/dci/financial/identity\\_fraud.asp](http://www.doj.state.wi.us/dci/financial/identity_fraud.asp)
- <http://enterprise.state.wi.us/home/Privacy/Identity%20Theft%20home.htm>
- [http://www.datcp.state.wi.us/cp/consumerinfo/cp/factsheets/stolen\\_identity.html](http://www.datcp.state.wi.us/cp/consumerinfo/cp/factsheets/stolen_identity.html)

## Wyoming

- <http://www.uwyo.edu/CES/FRM/Consumer/ConsumerProtectionAddresses.htm>
- <http://attorneygeneral.state.wy.us/consumer.htm>
- <http://www.uwyo.edu/CES/FRM/Consumer/ConsumerIssues/PrivacySurvivalGuide.PDF>