Identity Theft Prevention Tips and Commentary

Identity Theft, commonly referred to as *ID theft* and/or *identity fraud*, is a widespread and rapidly changing crime tactic. Although potentially anyone 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, loss of a job, 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, as well as ways identity theft is being implemented with new forms of technology. 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. This document is an updated version of the document we published in 2009.

Legal Notices

Dennis Martin, Demartek President, is available to speak on this topic to civic groups and other interested parties. Call the Demartek office at (303) 940-7575 to make arrangements.

Most Current Version: The most current version of this document is available at http://www.demartek.com/Demartek_Identity_Theft_Prevention_Tips_and_Commentary.html.

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

Table of Contents

Introduction

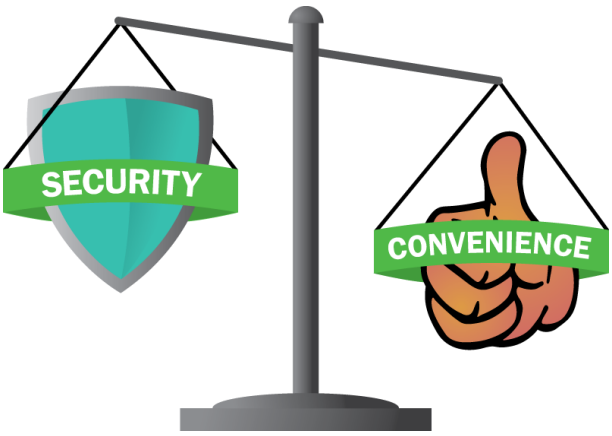
Identity theft, also known as ***ID theft*** and ***identity fraud***, continues to be among the fastest growing and constantly changing crimes. Its victims span all categories of people, including those from all age groups, economic backgrounds, race, gender, etc. In many cases the victims and the perpetrators have never met, however, theft by a friend, family member, or co-worker is on the rise. 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.

Businesses and individuals alike face a sophisticated worldwide fraud system run by organized crime. These criminals are constantly adapting their tactics in an attempt to steal identities and money. Although cybercriminals are increasingly targeting businesses and their intellectual property, real threats remain for individuals. Some of the information provided in this report is specific to a particular geography. However, criminals are increasingly directing their activities so that they operate across many different jurisdictions and geographies, making it considerably more difficult to trace and prosecute thieves.

One of the most common ways identity thieves obtain information is from lost or stolen wallets and purses or security-sensitive mail stolen from a mailbox. 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. A growing method of identity theft occurs through a vast array of computer scamming and hacking tactics that trick or manipulate the individual into providing money or information to an unfamiliar person, a thief. These methods allow the thief to gain access to monetary fund accounts or areas with information that, when combined with information found on other personal pages, can be used to commit fraud.

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 myriad ways that data can be stolen and ways to protect their customers' vital information.

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 can and should take action to prevent identity theft. Individuals also bear the brunt of the burden when it comes to the effort and trauma of recovering 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 extreme cases have been mistakenly arrested and put in jail.



Security and convenience are two factors contributing to an individual's threat level. Are you willing to sacrifice one for the other?

Security, including physical security and electronic security, is inversely related to convenience. That is, taking steps to increase security will reduce convenience. Conversely, increased convenience results in reduced 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 cannot 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; therefore 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.

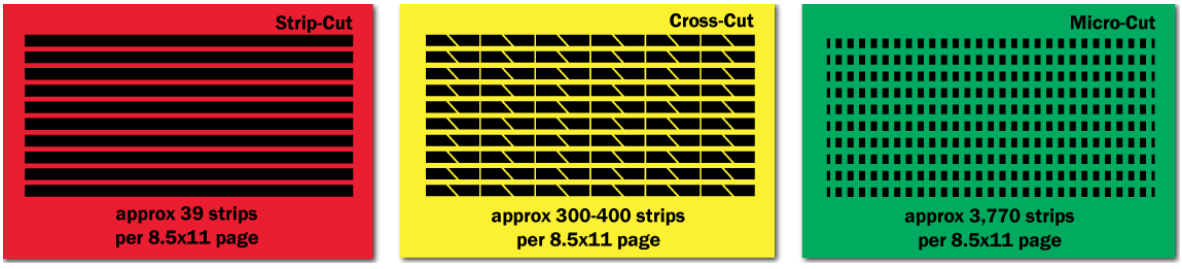
Paper Document Handling

Although identity theft has a certain high-tech connotation, many 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 someone 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, 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. Consult your legal, financial, or tax advisor for retention periods for specific documents.



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.

If you do not own a paper shredder or if you find the prospect too time consuming, check to see there are any public shredding events in your area. Some cities and states organize periodic shredding parties that are open to members of the community.

In short, there should be no trash or recycled paper leaving your residence that includes your name and other personal information that is legible. If you are debating whether something needs to be shredded, it is often best to do so.

Out-going Mail

Taking all out-going mail and packages to the post office, package delivery office, etc. is the best practice to avoid mail-tampering. Do not leave out-going mail or packages in your mailbox at home or on your front doorstep for pickup. Identity thieves look 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.

If you will be away from home for more than a day or so, it is a good idea to have a trusted person check and secure your mail daily. The post office can also place a hold on your mail for a minimum of 3 days and a maximum of 30 days. After you return home, you may reschedule your mail delivery, including all accumulated mail, or pick up your mail at the post office. Canada Post has a similar holiday hold mail service, but there is a fee for this service and the hold is for up to 15 days.

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, you are given the option to manage the types of mail you receive. The mailing offers are separated into four categories—credit offers, catalogs, magazine offers, and other offers. You can choose which offers, if any, you would like to receive in each category. It may take up to 90 days for your choices to take full effect, and your information will only remain on the MPS for three years. The register with the Mail Preference Service, visit http://www.DMAchoice.org.
- **Canadian Marketing Association (CMA) Do Not Contact Service** – A service that allows you to remove your name and address from mailing lists in Canada. This service can take up to six weeks to take effect and names will only remain on the list for three years. Unlike the US Direct Marketing Association's MPS, this service does not require you to manage your mailing offers; it simply adds your information to a "do-not-mail list." To add your name and address, go to http://www.the-cma.org/consumers/do-not-contact.
- **Opt Out Prescreen Service** – This service will allow you to reduce the number of pre-approved credit offers sent to you. Currently, this is only available in the USA. 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 the company has 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.

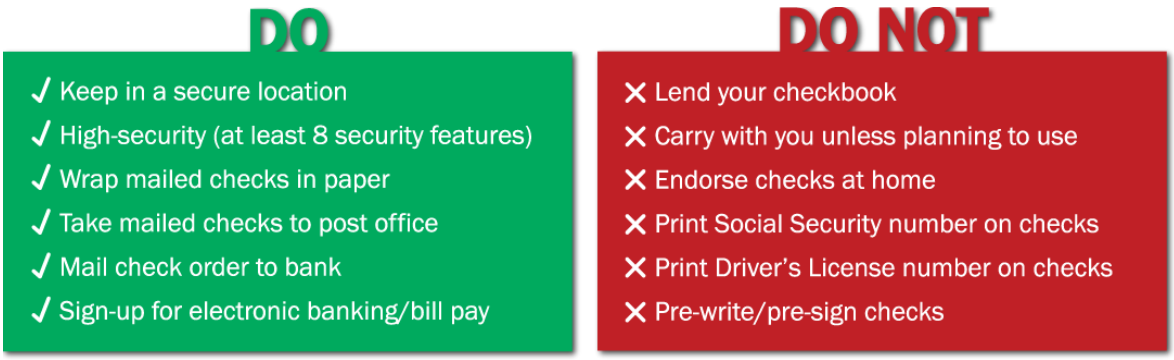
- **Preprinted Credit Card Checks** – You may receive pre-printed checks from your credit card company that can be used like regular checks but charge your credit card account, often with extra fees. These are a favorite of identity thieves because once in their possession, these are especially easy 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 do not plan to use these credit card checks, you should shred them and get them discontinued.
- **All Other Mailing Offers** – You can follow the same procedure as you would for unwanted banking or credit card offers for any unsolicited mail. Call the company's phone number or visit the company's website and request to be removed from the mailing list. For loose-leaf bundles or supermarket flyers, call the advertising agency listed on the mailing label. Since mail carriers routinely deliver one to each house, you may also need to notify them of your decision.

Bank Checks

The use of bank checks is on the decline with the wide-spread implementation and acceptance of other forms of payment, such as credit and debit cards and online payment methods. However, this doesn't mean secure check-handling practices should be over-looked; it can provide would-be thieves with much of your banking information. 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. Avoid carrying 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 an identity thief does not know your full name and has stolen your checks, they will not necessarily know how to sign the check. In places where you choose to provide personal information, it is a best practice to only provide the necessary/required information. It is also important to not pre-write or pre-sign checks before the payment transaction takes place. If a checkbook is lost or stolen with a signature already written, it is easy for a thief to fill in the other lines and cash 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 transparent. If you mail checks, be sure to take them directly to the post office.

When ordering new checks from your financial institution, opt to have them delivered to the financial institution. It is regular practice for a bank to send the check order to your residence; however, it is best to have them sent to the bank for your approval and pick-up. This is in an effort to keep security-sensitive information out of your mailbox. If you suspect your mailbox is not secure, has been tampered with in the past, or is part of a large group of mailboxes (i.e. and apartment complex mail station), inform your bank of this and have them delivered to the bank for secure retrieval.

Frank Abagnale is a former con-artist turned security consultant whose life inspired the film ***Catch Me If You Can***. He wrote a piece that gives extensive advice on how to be protected from check fraud. You can view this document at: http://www.abagnale.com/pdf/protection_b.pdf.

Consumers are switching to electronic banking and electronic bill payments, as it is becoming more popular, convenient, and secure in efforts to avoid some of the problems with physical checks.

Credit and Debit Cards

You should always know where your credit and debit cards are. Do not leave your card unattended at work or in the glove box of your car. These are two of the most frequent places credit card thefts occur. If you are using your card at a store or restaurant, be sure to check that it is in your possession when you get back. It is easy to forget your card or for cards to get mixed up when merchants are handling several transactions at once.

When you first receive your card, sign the back of it using permanent ink. Unsigned cards are not considered valid. If you want a merchant to ask for photo identification, you must still sign your card, but you can write "See ID" in addition to your signature. Never write your Personal Identification Number (PIN) on your card; it is best to memorize it.

It is extremely important that you do not give out your card number over the phone unless you initiated the call or are completely certain of who is on the other side of the line. Many scam artists trick people by pretending to be legitimate businesses. Do not lend your card to friends or relatives. Credit card companies and banks will consider that user to have your permission, and you will be liable for all charges incurred. In many cases, for security reasons, banks will close accounts of those who let others use their credit or debit cards. If you have let someone use your card in the past and no longer want him/her to have the information, the only way to ensure they don't have access is to request a new card with a new number and a new PIN.

It is a good idea to make photocopies of your cards and store the copies in a secure location, such as a locked filing cabinet. If your card is lost or stolen, you will have the phone number to call as well as all of the pertinent information. Check your bank statements or online banking account frequently to make sure that all of the charges belong to you. If you see suspicious activity or if you lose your card, report it to your

credit card company or bank immediately and inform them that it was lost or stolen. They will then cancel the card and reissue you a new card with new information. It is a best practice to inform your financial institution of all reasons for requesting new cards so they can better assist you and potentially track unauthorized uses of lost or stolen cards.

In addition, when travelling domestically or internationally, inform your financial institution and/or credit/debit card company of your travel location and dates.

As the use of checks declines and the use of credit and debit cards increases, so do the ways thieves can compromise your accounts and security. It is important to always use general caution when purchasing or making bank transactions with a credit or debit card.

ATM/Card Reader Fraud

ATMs (Automatic Teller Machines) are a widely used way for financial institutions to get their customers money in a fast and convenient manner. Thieves are starting to target these transactions because of the convenience and speed of the transaction, as well as the lack of attention paid by the individual when making these transactions.

When using an ATM, before inserting your card, do a visual scan of the machine and the area around the machine for anything unusual. A new practice for thieves is attaching a "fake" card insert slot over the pre-existing slot. These, upon a quick glance, appear to be normal, but are applied to the machine to read your card numbers and magnetic strip to send and store this information on an external device. In addition, check the keypad on the machine for false keypads placed on top of the existing keypad that can record buttons pressed, such as your PIN, and sent to an external device. Also be aware of cameras in use that might not be part of the machine. Lastly, make a mental note of those around you when using the ATM. If at any time you feeling uneasy about the situation at the ATM, do not insert your card, inform the financial institution immediately, and use another machine. It is always faster to travel to another ATM than to use one that is bugged and try to recover funds lost to a thief.

The above practices should also be used at gas station card readers as this is quickly becoming a place where card readers can be attached and important information can be read and stored by thieves offsite. As stated before, visually inspect any card reading device before inserting a debit or credit card.

Retirement Program Cards and Numbers

Several countries have national retirement programs with an account number for each individual who is eligible. In the United States, this is known as the Social Security Number (SSN). In Canada, this is number is known as the Social Insurance Number (SIN). 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 SSN or SIN on your checks. It should not appear on your driver's license. Do not post it on the Internet. It is illegal to use a false, counterfeit, or stolen SSN or SIN to obtain employment, loans, credit, or other goods and services. The penalties include jail time and fines, and when used by non-citizens, it can result in deportation.

> ***Keep card numbers private and in a secure location when not in use. If asked for sensitive information, ask questions first.***

In the USA, the Social Security Administration provides a statement annually to workers and former workers aged 25 and older, and 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.

The government of Canada provides an online service called a "My Service Canada Account" that allows you to view, update, and print records of your Canada Pension Plan (CPP), Employment Insurance (EI), and Old Age Security (OAS). First-time users of this

service will need to apply for a Personal Access Code before they can apply for an account. The account requires a user name and password called an "epass." In the future, an epass is all that is needed to access a "My Service Canada Account." Check your account regularly to make sure the information is accurate and reflects your work history.

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?

More information about Social Security in the United States can be found at: http://www.ssa.gov or in Spanish at http://www.ssa.gov/espanol. To learn more about Social Insurance in Canada, visit http://www.servicecanada.gc.ca/eng/sc/sin/index.shtml.

Driver's Licenses

In the United States, you are required by law to provide proof of your Social Security number to the Driver's License officials, but it should not be printed on your license. The Intelligence Reform and Terrorism Prevention Act of 2004 prevents states from displaying your SSN on driver's licenses, state ID cards, or motor vehicle registrations. Canadian residents are not required to provide a Social Insurance number to obtain a license, but it can be used as a secondary form of identification. An SIN will not be printed on a driver's license.

Be very reluctant to give your driver's license or driver's license number to anyone 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, while some states do not record form DD 214 at all.

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. Each state has a different confidentiality policy; it is best to contact your County Veteran Service Officer who will explain the extent, meaning, and application of the laws where you live. To find a service officer, visit NACVSO.org.

Telephone Privacy

As more and more communications are taking place via the internet, phone scams are on the decline. However, they still exist. When speaking on the phone with an individual or a business, verify that you know the person you are speaking with. Also, if a business is contacting you, make sure that the reason they are calling and potentially requesting information from you makes sense. Oftentimes a thief, or group of thieves, will pose as a

legitimate business, and potentially a business related to a service you often need or find beneficial. Many times, when confronted or questioned, the caller will talk around the situation and continue to try and pull information from you. If you do not know the person or company, do not provide any information and hang-up. If it seems like a thief posing as a legitimate business, hang up and contact that business directly and discuss the occurrence. They will be able to inform you of the caller's validity and also be warned if there is a person falsely claiming affiliation for information or monetary gain. Demartek recently discussed a common phone scam, including a recording of the telephone conversation, in the Demartek IRS Telephone Scam Report.

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 numbers 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 numbers are not included in the printed telephone directories and are 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.

- **Non-published** – Your name, address, and telephone numbers are not included in the printed telephone directories and are 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.
- **USA DO NOT CALL Registry** – In the USA, the federal national "DO NOT CALL" registry is available at https://www.donotcall.gov. You can also call 1-888-382-1222. In February 2008, the Do-Not-Call Improvement Act of 2007 became law. This means that once registered, a phone number will remain on the list permanently. 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** – The Canadian government passed a law allowing for the creation of a national "DO NOT CALL" list in 2006. The registry is available at: https://www.lnnte-dncl.gc.ca. You can also call 1-866-580-3625. Once on the list, your number will be registered for five years. Telemarketers are now required by law to subscribe to the list and must update their records every month. Similar to the "DO NOT CALL" list in the United States, registration does not prevent calls from registered charities, organizations conducting polls or surveys, political parties, or newspapers looking for subscriptions.

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. There are several known variants of this type malicious software and the information regarding these is available at the major anti-virus software company websites.

A threat that is becoming more prevalent is rogue security software, or "scareware." These fake antivirus programs offer to remove malicious software from computers, but actually install viruses, Trojans, and often advise the user to purchase (fake) protection. Beware of pop-up windows or advertisements that simulate legitimate displays as these are common methods used by cybercriminals. Some advertisements might even claim to be for a well-known antivirus business. Instead of clicking on those types of links, manually type the URL of your desired, reputable company.

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 regular updates to the virus definitions. In order to keep up with the volume of criminal activity on the Internet, some of the major anti-virus vendors make updates available multiple times per day.

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 include anti-spyware technology with their anti-virus solutions. Make the relatively small investment to protect yourself from spyware.

Firewalls

Firewalls help provide protection from malicious users on the Internet and on internal networks and should be considered mandatory. Firewalls inspect incoming and outgoing network traffic and drop incoming traffic that is not in direct response to outgoing requests. Optionally, firewalls can also block outgoing traffic. This report provides a basic understanding of computer network firewall technology, but is not intended as complete tutorial on the subject.

It is always better to feel over-protected than under-protected when it comes to important information.

There are two basic types of computer network firewalls: hardware and software. We recommend that you use both types of firewalls together as part of a multi-layered defense strategy. Both types of firewalls can be set to ignore ("stealth") incoming requests. This is a good strategy as there are criminals in all parts of the world who constantly scan the Internet looking for computers with open ports.

Most computer operating systems provide a software firewall. For the Windows environment, software firewalls that were introduced with Windows XP Service Pack 2 (SP2) were improved in subsequent versions of Windows 8 and 8.1. Apple Macintosh and many Linux systems include a software firewall. In addition, third-party software firewalls are available. It is import to use a firewall on each computer connected to any network, whether it be the one that comes with your operating system or a third-party version.

We recommend that hardware firewalls also be deployed in homes and small offices that have connections to the Internet. Hardware firewalls provide consistent protection to all computers connected in a home or small business 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 ignore 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. These firewalls are available for wired and wireless networks.

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.

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 do not want tracking you.

Many web browsers now offer privacy mode. This feature prevents the browser from storing data like cookies, temporary internet files, and history. Users need to initiate private browsing from the browser's menu. The private browsing session will then continue in the current browser, or open a new browser window.

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 do not 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 a minimum, reformatted before you give it away. You can also get programs that will write random data patterns (multiple times) over the media so that any data that might exist is scrubbed. These programs are sometimes known as "wipe" utilities. Some of these wipe utilities conform to US Department of Defense (DoD) data security standards. Some computer storage systems have their own "secure erase" features.

For instructions on how to fully delete data from your personal computer, Demartek has produced a reference guide called How to Fully Delete Data from a Disk Drive.

For those who need additional security due to highly sensitive data, there are more serious enterprise and military-grade data erasure methods available, but at a significantly higher cost. These data erasure methods require specialized equipment and, in some cases, special contained environments. These methods prevent more sophisticated hackers or organizations from attempting to recover data that may be possible to find even after some of the "lightweight" data erasure methods have been performed. These methods include the use of powerful magnets to de-gauss the magnetic media surface, disassembling the disk drives and sanding off the magnetic oxide material, applying acids and other chemicals to the media surface and crushing, melting or otherwise physically destroying the media. Variations of these methods can be applied to disks, tapes, optical media, and flash-based media such as USB flash drives, memory cards, etc.

"Phishing" Scams

Many criminals attempt to get you to give them your personal information via email using a technique known as "phishing." They send you requests for your information, disguised as an email from a bank, Internet Service Provider (ISP), social networking site, or other institutions that you might trust. The text of the email generally refers to a system upgrade, possible fraudulent activity with some accounts, or some other fabricated reason that information needs to be "confirmed." Sometimes these emails suggest that some accounts may be suspended until the information is confirmed. In some cases, these attempts at fraud include some sort of "customer form" attached to the email. Other attempts direct people to bogus websites that have names similar to genuine websites. Take note of what emails from your bank and other secure sites look like. Oftentimes, a fraudulent email will look similar, but something tends to be a bit different.

"Spear phishing" is a more targeted form of phishing that can come in form of emails that appear to be from a boss, co-worker, supplier, etc. These could include requests for user names and passwords. Some sophisticated criminals will do some research on their intended victim in order to select a subject line that might be more likely to be opened and bypass spam filters.

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. When in doubt, call the person or organization using a well-known telephone number to confirm the email.

It's also a good habit to password lock your computer at work when leaving your desk. This is especially true if your computer contains security-sensitive information. This will deter wondering eyes or individuals that could access your information without your knowledge.

It is becoming increasingly popular to receive emails from companies after setting up an account (generally consumer/shopping accounts). When providing any bank information to a company, be sure to read the small print. Where it was once required when setting up these accounts to "check" boxes to sign up for services, it is now customary that these boxes are "pre-checked." In these cases, you uncheck them to opt out of additional products and services. It is also becoming regular practice for businesses to have a "Terms and Conditions" or "Privacy Policy" when doing business with them that requires your agreement. Don't skip over these and agree without reading what you are agreeing to. This is an area where not reading the fine print can lead to additional charges or fees that can't be reversed because you previously agreed to them.

If you feel the need to take additional action, you can forward the email to the email fraud address for that organization. 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.

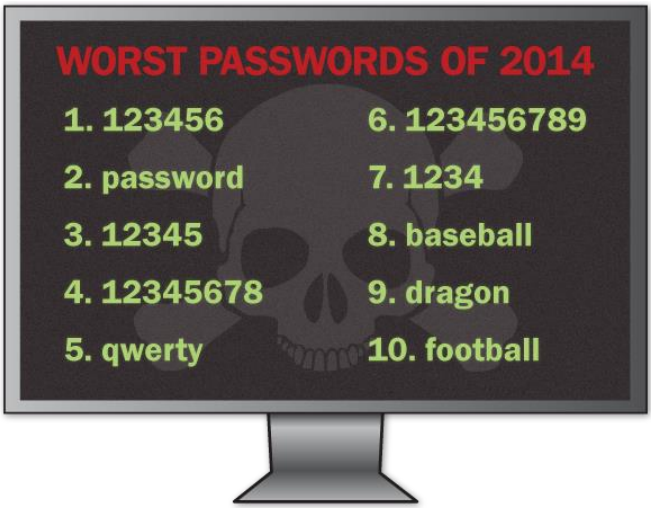
Passwords

There are at least five 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 should not write them down. For the best protection, change passwords periodically, especially on websites that contain financial information.

Below are tips to keep in mind when choosing a password.

- Blank password – No password at all is no security and simply invites theft.

- 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. There are numerous examples of these types of bad passwords available on the Internet that can be found with a simple search.
- 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.
- 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.
- Repeating passwords – Using the same password for all websites. If a thief successfully hacks into one of your accounts, that person can log in wherever you do and can steal all of your sensitive information. It is a good idea to have multiple passwords and to make your online banking password completely different from your email or social networking site passwords.



Mobile Devices

Though many consumers are aware of the dangers the Internet poses to personal computers, it is important to remember that many of these same threats apply to web-use from mobile devices. Though some mobile devices provide basic protection against "phishing" sites, it is impossible to block everything, so do not enter confidential information on questionable sites. Make sure that passwords are not stored on your mobile device—this will make it easy for thieves to access all of your personal information. If you must store passwords on your mobile device, be sure to use a strong, well-known encryption algorithm. As a good rule of thumb, mobile device users should exercise the same caution as they would when using a computer.

Social Networking Sites

With the popularity of social networking websites such as Facebook, LinkedIn, Twitter, etc., there are some common sense "best practices" to follow in order to reduce the possibility of identity theft. The basic thing to remember is that things posted onto the Internet tend to have a long life, and once published on the Internet, get copied to multiple locations and are extremely difficult to remove. Once out "into the open," the many search engines dutifully index and list all this data for anybody in the world, including criminals, to find.

As more and more social networking sites emerge and users have accounts on multiple sites, we start to face issues with the amount of potentially damaging information individuals make public. Be wary of the amount of personal information you input into these social media sites and keep a fairly low-profile across all sites. It is best to omit information such as address, phone numbers, birth years, multiple email address, etc. The more information you make public, the more information a thief has to construct a picture of you, thus making it easier to get sensitive information.

> ***The more personal information you make public, the easier it is to become a victim of identity theft.***

In addition to limiting the amount of information you provide publicly, it is wise to regularly familiarize yourself with the privacy settings on your account. Unless a person is a friend or family member, it is best to make it hard for strangers to access your

information and images. Also, before you allow someone to see your profile or account in full ("friending" or accepting a "friend request") make sure that you know the person involved. Thieves can easily friend you to obtain information about you and then use it elsewhere to access your private data.

In addition to these tips, some social media outlets (i.e. Twitter) have increased security levels for their consumers in the way of two-factor authentication. This requires the user to have two known passwords, one often in the form of a code sent to the viewer via cell phone text, to access accounts. While this increases the level of security, it also lowers the individual's level of convenience.

With this basic premise in mind, carefully consider any personal information that you post on any social website. Thoroughly review the privacy policies of these sites and customize the account privacy settings so that your personal information remains as private as possible.

Common Fraud Attempts

The following list contains some of the prevalent scams that are in circulation. There are numerous variations of each scheme, but the basic elements are the same. It is essential that people be skeptical and remember that if it sounds too good to be true, it probably is.

> ***When it comes to offers providing goods or services remember, if it seems too good to be true it probably is.***

- **Nigerian 419/Foreign Lottery Scams** – A common mail and email scam is from someone claiming to be a foreigner who needs help moving a large amount of money out of the country. The number "419" refers to the Nigerian penal code that addresses these crimes. As an incentive, the sender offers the recipient a percentage of the money in exchange for their help. The scammer will ask the recipient to cover some of the upfront costs with promises of reimbursement, and then make excuses for the transfer of the fortune to be postponed. The best way to protect yourself is to delete this email immediately. A similar scam involves a phony representative from a foreign lottery who claims you have won a fortune; they just need your account number to transfer the money. As with all scams of this type, do not reply.

- **Craigslist Scams** – When making any purchases on Craigslist, or other similar websites, most notably large purchases like vehicles or rental property make certain you know the party involved. Many times, a deal on Craigslist will seem too good to be true, and if often is. Frequently, sellers will request money to be wired to them for various reasons, perhaps because they live out of state. Always be hesitant to send someone money electronically. Many times, scammers will request that you send money for goods or services promised and then stop communication once they have the money. Also, avoid taking checks as a method of payment; these can "bounce" when taken to a bank to be cashed. It is a best practice to make transactions in person, and if needed, both parties involved in the transaction should make sure funds are available (i.e. cash out checks or payments) together. This will ensure the transaction happens without any loss of money or possessions.
- **Charity Scams** – After a natural disaster or crisis, many people feel the overwhelming urge to help, often offering cash donations to charities. Unfortunately, many fraudulent organizations spring up after these types of events that falsely claim to be collecting money for victims. Some will even use phishing schemes, sending emails that try to obtain your personal and banking information. It is better to donate to reputable organizations, like the Red Cross.
- **Grandparent Scams** – A thief calls a senior citizen, frequently in the middle of the night, and impersonates a child or grandchild. The caller will say that they are in some kind of trouble, generally in another country or distant location, and ask the victim to wire some money. The scammer will add that they do not want the family finding out about their situation, so as to convince the victim not to make calls to verify the facts. If in this situation, do not give out any banking or credit card numbers. Ask specific questions that only your real relative would know. If the person on the phone still seems legitimate, tell him/her that you will call back. Even if you are given another number over the phone, dial the number that you have on file for that person or the number of a parent or spouse. You will likely find that your relative is actually safe at home. Finally, notify the authorities.
- **Social Networking Scams** – In this modern version of the Grandparent scams noted above, a hacker will obtain the password to your social networking website, such as Facebook, LinkedIn, Twitter, etc. and send a message apparently from you to many or all of your online friends indicating that you are in some sort of trouble and need money. The hacker may also change your password so that you cannot access your own social networking account. It is important to have a strong

password for social networking sites and to keep them separate from your other passwords. If you notice that someone you know seems to be behaving uncharacteristically on a social network, send him/her a personal email to say that an account may have been hacked.

- **Health Insurance Fraud** – People sometimes learn they are victims of identity fraud when they receive a medical bill or a notice from their health insurance company for medical attention they did not receive. Though some hospitals are now employing iris and palm scans to verify patients' identities, no technology is foolproof. These cases of identity theft arise less often from lost insurance cards and more often from "inside jobs." Victims of health insurance fraud should file a police report and contact the medical provider and health insurance company in writing with the details of the fraud, being sure to include the police report.
- **US Census Scams** – The US Census Bureau warns of possible scams surrounding the census. Though you may receive an email or telephone call regarding the census, know that the Census Bureau will not ask for Social Security numbers, PIN numbers, bank accounts, or credit cards. To report email fraud, visit http://www.census.gov/survey_participants/related_information/phishing_email_scams_bogus_census_web_sites.html. A census worker may visit you at your home, but they will show you a badge, and you may ask to see another form of picture identification. If you feel uncomfortable, know that you are not legally required to allow a census-taker into your home.
- **Jury Duty Scams** – Several states have issued warnings about scams that involve people posing as court officials. The phony officials may say that there is a warrant out for your arrest after you failed to show up for jury duty. If you say that you did not receive a jury duty notice, they ask for your Social Security number and birthdate to clear up the matter. They may also ask for credit card information to charge a fine. If you receive a call like this, do not give out any personal information and contact your local authorities. Court officials will never ask for confidential information over the phone and most communication between courts and jurors is done through mail. For more information about jury duty summons, contact your local court offices.
- **Employment Scams** – Before giving personal information in regards to a job posting, be sure of the person/company you are dealing with. It is a best practice to only provide this information in person and not over the phone or through email.
- **Child Pornography Scams** – Unsuspecting users can be exploited by viruses that deposit child pornography on their personal computers. Pedophiles can use your

computer to accumulate these types of images without worrying that they will get caught. The next thing you know, a coworker or family member might stumble across this stash. If brought before the authorities, it could land you in jail, cause the loss of a job, and cost thousands of dollars to clear your name. The best way to avoid this horrifying situation is to protect your computer from viruses by using a good firewall, an antivirus program, and always being careful about the websites you use.

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 also becoming more common for a child's social security number to be obtained and used to apply for loans, credit cards, jobs, etc. This is on the rise because of the lack of oversight pertaining to a child's personal information. Many people don't think about their child's personal information being used to commit fraud, thus the fraud can happen for an extended period of time, or in many different ways, before being seen.

It is a good idea to take the same steps provided in the previous sections for your children, and when they are old enough, teach them to take these steps. It is also good practice to inform your children of the importance of keeping private information safe. If your children have access to any of your sensitive information, or were present when establishing sensitive information, it is best to remind them of the importance of not letting others know this information. If you suspect there might be an issue with a child's unauthorized use of any private information, steps can be taken to change this information and avoid any information breaches in the future.

It is good practice to inform your children of the importance of keeping private information safe.

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 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.html
- http://www.idtheftcenter.org
- http://www.identitytheft.org
- http://www.vaonline.org/fraud.html
- http://www.identity-theft-help.us
- http://www.abcfraud.ca

Identity Theft Stories

There are innumerable accounts available of identity-theft victims. Problems encountered by identity theft victims include checks not being accepted, collection letters arriving for things purchased by the identity thief, loss of job, mistaken arrest and strip search, and numerous others. Visit your favorite news source, and you are certain to find several stories of identity fraud. It is a good idea to stay current with the latest scams.

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. These types of security breaches are perfect fodder for class-action lawsuits. A number of organizations have made news headlines for the wrong reasons. There are too many instances to list here, but a search for

"data breach" or "security breach" will provide plenty of information about companies that have suffered data security breaches.

- **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.
- **US Federal Trade Commission** (effective July 8, 2008) – Financial institutions and creditors are required to develop and implement written identity theft prevention programs under the new "Red Flags Rules." The Red Flags Rules are part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. Under these Rules, financial institutions and creditors with covered accounts must have identity theft prevention programs in place by November 1, 2008, to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. The details are available at: http://ftc.gov/opa/2008/07/redflagsfyi.shtm.

California was the first state to pass a security breach notification law, and most states followed suit, enacting laws that require notification of security breaches involving personal information. There is discussion in the United States Congress of a national law similar to the California law, though no such legislation has been passed yet. As of this writing, 47 U.S. states have passed legislation similar to the California law.

Credit Freezes and Fraud Alerts

Another tactic available for consumers to protect themselves before an identity theft occurs is the concept of a credit "freeze." Once you have frozen your credit files, new lenders will not be able to access your account information. This will prohibit thieves from opening new accounts in your name. While this may be a viable prevention system for some, it can cause extra headaches if your credit report is accessed often. Anytime you want to open a new account, you will have to call the credit bureaus to "thaw" your account. Most states have enacted security freeze laws, though the rules differ by state.

Currently, Canada does not have any laws regarding credit freezes. However, the credit bureaus in Canada and the US will place a fraud alert on your account if you suspect that you have been a victim of identity theft. When a fraud alert is attached to your credit report, creditors need to contact you before opening a new account in your name. An initial fraud alert stays on your credit report for 90 days. An extended fraud alert stays on your credit report for 7 years, but requires an Identity Theft Report from the police to confirm that you have been a victim.

Credit Bureaus

The major credit reporting agencies in the United States and Canada are listed below. In the case of identity theft, be sure to contact them to place a fraud alert or credit freeze on your credit report. They can also be contacted to get a copy of your credit report or raise disputes.

Equifax
1-866-685-1111
http://www.equifax.com

Experian
1-888-397-3742
http://www.experian.com

TransUnion Canada
1-800-663-9980
http://www.transunion.ca

Equifax Canada
1-800-465-7166
http://www.consumer.equifax.ca/

TransUnion
1-800-888-4213
http://www.transunion.com

TransUnion Canada (Echo Group)
1-877-713-3393
http://www.transunion.ca

In the US, The Fair Credit Reporting Act, enforced by the Federal Trade Commission, guarantees consumers access to a free annual credit report. To request a copy of your free credit report, visit https://www.annualcreditreport.com. Residents of Canada are also entitled to a free credit report once a year, though they are required to send a request to the credit bureaus, along with copies of identification and proof of address. Visit the credit bureaus' websites for more information.

Identity Theft Passport

Some US 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. 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 the removal 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.

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. Other states are considering similar identity theft passport programs, and we will likely see more in the future. It is possible that the federal government will create a national identity theft passport. Resources for the identity theft passport programs are listed below.

State	Link to identity theft passport resources
Arkansas	http://arkansasag.gov/programs/schools-educators-and-communities/id-theft/id-theft-passport/
Delaware	http://attorneygeneral.delaware.gov/consumers/protection/idtheft.shtml
Iowa	http://www.iowa.gov/government/ag/helping_victims/contents/IDPP.html
Maryland	http://www.oag.state.md.us/idtheft/IDTpassport.htm
Mississippi	Passport offered to victims with false criminal records. Contact state Attorney General.
Montana	https://doj.mt.gov/consumer/for-consumers/identity-theft
Nevada	http://ag.nv.gov/Hot_Topics/Victims/IDTheft_Passport
New Mexico	http://www.nmag.gov/consumer/investigations/nm-identity-theft-passport
Oklahoma	http://www.ok.gov/osbi/Criminal_History/Identity_Theft_Passport_Program
Virginia	http://www.oag.state.va.us/Programs%20and%20Resources/Identity_Theft

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. Many 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. It is important to note that these types of policies do not cover direct monetary losses incurred as a result of identity theft. 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 – National

- http://www.publicsafety.gc.ca/prg/le/bs/consumers-eng.aspx /////
- **[FR]** http://www.securitepublique.gc.ca/prg/le/bs/report-fra.aspx /////
- http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm
- **[FR]** http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-fra.htm
- http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp
- **[FR]** http://www.priv.gc.ca/fs-fi/02_05_d_10_f.cfm

USA – National

- http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html
- **[ES]** http://www.consumidor.ftc.gov/destacado/destacado-s0014-robo-de-identidad
- **[ES]** http://www.ftc.gov/index_es.shtml
- http://www.justice.gov/criminal/fraud/websites/idtheft.html
- http://www.ojp.gov/programs/identitytheft.html
- **[ES]** http://www.ojp.usdoj.gov/ovc/library/espanol.html
- http://www.irs.gov/uac/Identity-Protection
- http://www.secretservice.gov/criminal.shtml
- http://publications.usa.gov/USAPubs.php?NavCode=XA&CatID=12
- **[ES]** http://publications.usa.gov/USAPubs.php?NavCode=XA&CatID=13

Canada – Provinces and Territories

Alberta

- http://www.servicealberta.gov.ab.ca/560.cfm
- http://www.servicealberta.gov.ab.ca/pdf/tipsheets/Identity_theft.pdf
- http://www.albertacanada.com/immigration/living/identitytheft.html /////
- http://www.lawcentralalberta.ca/LawCentralAlberta/default.aspx

British Columbia

- http://www2.gov.bc.ca/gov/topic.page?id=2A477231EF934E22B0FBC8C43A98B9D9

- http://www.nwpolice.org/community-services/crime-prevention9/crime-prevention-education/identity-theft/
- http://www.richmond.ca/safety/police/personal/idtheft.htm

Manitoba

- http://www.gov.mb.ca/cca/cpo/identity.html
- http://www.gov.mb.ca/finance/cca/consumb/identity.html /////

New Brunswick

- http://www.gnb.ca/cnb/promos/justice/theft-e.htm
- http://www.gnb.ca/0062/Rentalsman/CA/faqs-e.asp

Newfoundland and Labrador

- http://www.servicenl.gov.nl.ca/consumer/consumer_affairs/ident_en.html
- https://www.nlcu.com/Home/ProductsAndServices/YourMoney/FraudAwareness

Northwest Territories

- http://www.justice.gov.nt.ca/VictimServices/index.shtml
- http://www.gov.ns.ca/snsmr/pdf/ans-consumer-identity-theft.pdf

Nova Scotia

- http://www.gov.ns.ca/just/prevention/tips_consumer_IDtheft.asp
- http://www.gov.ns.ca/snsmr/access/individuals/consumer-awareness/consumer-alerts/identity-theft.asp
- http://novascotia.ca/seniors/partners_against_fraud.asp

Ontario

- http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00084.html
- http://www.opp.ca/ecms/index.php?id=133
- **[FR]** http://www.opp.ca/ecms/index.php?id=355

Prince Edward Island

- http://www.cliapei.ca/content/page/front_news/id/40

Quebec

- **[FR]** http://www4.gouv.qc.ca/FR/Portail/Citoyens/Evenements/proteger-identite-Internet/Pages/accueil.aspx
- **[FR]** http://cacq.ca/Vol-d-identite-Attention

Saskatchewan

- http://www.justice.gov.sk.ca/identity-theft
- http://www.justice.gov.sk.ca/TipIdentityTheft-Jan2008.pdf

USA – States, Commonwealths, Territories, and District of Columbia

Most states provide some identity theft materials online, although some have made their information more available and easier to find than others. These resources 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.ago.state.al.us/Page-Consumer-Protection
- http://www.ago.state.al.us/File-Consumer-Protection-Brochure-Identity-Protection
- http://alabamaidtheft.com/
- http://www.identitytheftportal.com/alabama.html

Alaska

- http://www.law.alaska.gov/department/civil/consumer/IDtheft.html
- **[ES]**http://www.law.state.ak.us/department/civil/consumer/cp_spanish_brochures.html
- http://www.identitytheftportal.com/alaska.html

Arizona

- http://www.azdps.gov/Services/Crime_Victims/
- http://www.azag.gov/cybercrime/ID_Theft.html
- http://identitytheftnetwork.org/arizona
- http://www.identitytheftportal.com/arizona.html

Arkansas

- http://arkansasag.gov/programs/schools-educators-and-communities/id-theft
- http://gotyourbackarkansas.org/identity/
- http://www.identitytheftportal.com/arkansas.html

California

- http://oag.ca.gov/idtheft
- https://www.ftb.ca.gov/individuals/id_theft.shtml
- **[ES]** https://www.ftb.ca.gov/individuals/id_theft_spanish.shtml
- http://www.identitytheftportal.com/california.html

Colorado

- http://www.coloradoattorneygeneral.gov/initiatives/identity_theft
- https://www.colorado.gov/cbi
- http://www.identitytheftportal.com/colorado.html

Connecticut

- http://www.ct.gov/dcp/cwp/view.asp?a=1629&Q=289476&PM=1
- http://www.ct.gov/ag/cwp/browse.asp?A=2066&BMDRN=2000&BCOB=0&C=19200
- http://www.identitytheftportal.com/connecticut.html

Delaware

- http://attorneygeneral.delaware.gov/fraud/cpu/idtheft.shtml

Florida

- http://myfloridalegal.com/pages.nsf/Main/CBBEBA3F2583433385256DBA004BC600
- **[ES]**http://www.myfloridalegal.com/pages.nsf/0/CBBEBA3F2583433385256DBA004BC600?Open&LN=SP
- http://www.identitytheftportal.com/florida.html

Georgia

- http://consumer.georgia.gov/consumer-topics/identity-theft-1
- http://law.ga.gov/00/article/0,2086,87670814_87670971_88025112,00.html
- http://investigative.gbi.georgia.gov/identity-theft
- http://www.identitytheftportal.com/georgia.html

Hawaii

- http://ag.hawaii.gov/quick-links/id-theft/if-you-are-a-victim/
- http://www.hawaii.gov/dcca/helping_hand/identity_theft
- http://honolulupd.org/information/index.php?page=identity
- http://www.identitytheftportal.com/hawaii.html

Idaho

- http://cybersecurity.idaho.gov/identity_theft.html
- http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf

- **[ES]** http://www.ag.idaho.gov/publications/spanish/InternetSafetySpanish.pdf
- http://www.identitytheftportal.com/idaho.html

Illinois

- http://www.ag.state.il.us/consumers/hotline.html
- http://www.ag.state.il.us/consumers/consumer_publications.html
- **[ES]** http://www.ag.state.il.us/consumers/consumer_publications_span.html
- http://illinoisissues.uis.edu/features/2002mar/name.html

Indiana

- http://www.in.gov/idoi/2561.htm
- http://www.in.gov/attorneygeneral/2349.htm
- http://www.in.gov/attorneygeneral/2409.htm
- http://www.in.gov/dfi/idtheft.pdf

Iowa

- http://www.iowa.gov/government/ag/consumer_advisories/credit_finance/protect_privacy.html
- http://www.iowa.gov/government/ag/images/pdfs/Identity_Theft_GUIDE.pdf
- http://www.iowaattorneygeneral.org/consumer/brochures/avoid_identitytheft.html

Kansas

- http://ag.ks.gov/consumer-protection/consumer-tips/protect-yourself
- http://www.ksinsurance.org/consumers/id_theft.htm

Kentucky

- http://ag.ky.gov/civil/consumerprotection/idtheft

Louisiana

- http://www.revenue.louisiana.gov/forms/Fraud/IdentityTheftChecklist.pdf

Maine

- http://www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml
- http://www.maine.gov/pfr/consumercredit/documents/identity_theft.htm
- http://www.maine.gov/pfr/financialinstitutions/consumer/credit_report.htm

Maryland

- http://www.oag.state.md.us/idtheft/index.htm
- http://www.oag.state.md.us/consumer/idtheft.htm

Massachusetts

- http://www.mass.gov/ago/consumer-resources/consumer-information/scams-and-identity-theft/identity-theft/
- http://www.mass.gov/ago/docs/consumer/id-theft-guide.pdf

Michigan

- http://www.michigan.gov/ag/0,4534,7-164-17337_20942-230557--,00.html
- http://www.michigan.gov/msp/0,1607,7-123-1589_35832---,00.html
- http://www.michiganlegalaid.org/library_client/resource.2005-05-29.1117417906674
- http://www.michigan.gov/documents/ID_Theft_94764_7.pdf

Minnesota

- http://www.ag.state.mn.us/Consumer/Handbooks/GuardingYPrivacy/default.asp
- https://dps.mn.gov/divisions/ojp/help-for-crime-victims/Pages/Identity%20Theft.aspx

Mississippi

- http://www.ago.state.ms.us/publications/identity-theft-what-to-do-when-theres-more-than-one-you/
- http://www.ago.state.ms.us/publications/identity-theft-brochure-protecting-your-good-name/
- http://www.ago.state.ms.us/consumer-protection/identity-theft-affidavit/

Missouri

- http://ago.mo.gov/publications/idtheft.htm
- http://missourifamilies.org/features/consumerarticles/idtheft.htm

Montana

- https://doj.mt.gov/enforcement/investigations-bureau/computer-crime/
- https://doj.mt.gov/consumer/for-consumers/identity-theft/

Nebraska

- http://www.ago.ne.gov/resources/dyn/files/392571za5a5011a/_fn/AGO_IDTheftBroch_122910.pdf
- http://www.dmv.ne.gov/dvr/pdf/theftpacket.pdf

Nevada

- http://ag.nv.gov/About/Consumer_Protection/Bureau_of_Consumer_Protection/
- http://fightfraud.nv.gov/IdentityTheft_new.htm

New Hampshire

- http://doj.nh.gov/consumer/sourcebook/identity-theft.htm
- http://www.doj.nh.gov/consumer/identity-theft/

New Jersey

- http://www.state.nj.us/lps/dcj/idtheft.htm
- http://www.state.nj.us/lps/njsp/tech/identity.html
- **[ES]** http://www.state.nj.us/lps/ca/espanol/spbrief/identitytheftbus.pdf
- http://www.state.nj.us/dobi/division_consumers/finance/identitytheft.htm
- http://www.state.nj.us/dobi/creditreport6.htm

New Mexico

- http://www.nmag.gov/consumer/for-students/identity-theft
- http://www.nmag.gov/consumer/investigations/nm-identity-theft-passport
- http://www.cabq.gov/police/prevention/identity.html

New York

- http://www.ag.ny.gov/consumer-frauds-bureau/identity-theft
- http://www.nyc.gov/html/dca/html/initiatives/identity_theft_prevention.shtml
- http://www.nyc.gov/html/dca/downloads/pdf/shredfest_biztips.pdf
- http://www.longislandexchange.com/identity-theft.html

North Carolina

- http://www.ncdoj.com/Protect-Yourself/2-4-3-Protect-Your-Identity.aspx
- http://www.ncdot.gov/dmv/licensetheft/

North Dakota

- http://www.ag.state.nd.us/cpat/idtheft/idtheft.htm
- http://www.psc.nd.gov/public/consinfo/index.php
- http://www.ag.nd.gov/Brochures/FactSheet/IdentityTheft.pdf

Ohio

- http://www.ohioattorneygeneral.gov/IdentityTheft
- http://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/Identity-Theft
- http://www.pickocc.org/annualreports/2007/hotline.shtml
- http://www.sos.state.oh.us/Businesses/BusinessInformation/BusinessIdentityTheft.aspx

Oklahoma

- http://www.oag.ok.gov/oagweb.nsf/Consumer!OpenPage
- http://www.odl.state.ok.us/usinfo/pubs/idtheft.pdf
- http://oklahomamoneymatters.org/Consumers/ID_Theft.shtml

Oregon

- http://www.doj.state.or.us/consumer/Pages/id_theft.aspx
- http://www.oregon.gov/ODOT/DMV/driverid/idtheft.shtml
- https://www.oregonlegislature.gov/citizen_engagement/Reports/2004IF_Identity_Theft.pdf

Pennsylvania

- https://www.attorneygeneral.gov/Consumers/Bureau_of_Consumer_Protection/
- https://www.attorneygeneral.gov/Consumers/Identity_Theft/
- **[ES]**http://www.portal.state.pa.us/portal/server.pt/gateway/PTARGS_0_496447_0_0_18/identity_theft.pdf
- http://www.dmv.state.pa.us/forms/idTheftReportingForms.shtml

Puerto Rico

- **[ES]** http://www.justicia.gobierno.pr/rs_template/v2/DivEco

Rhode Island

- http://www.doit.ri.gov/documents/security/Brochure%20Fight%20back%20against%20identity%20theft.pdf
- http://www.doit.ri.gov/documents/security/IRS%20ID%20Theft%20Message.pdf
- http://www.risp.ri.gov/docs/Guide_Identity_Theft_RISP.pdf

South Carolina

- http://www.justice.gov/usao/sc/programs/resources.html
- http://www.scdmvonline.com/DMVNew/default.aspx?n=reporting_fraud

South Dakota

- http://atg.sd.gov/Consumers/IdentityTheft.aspx

Tennessee

- http://tennessee.gov/attorneygeneral/cpro/identitytheft.html
- http://tennessee.gov/safety/cididtheft.htm
- http://tennessee.gov/consumer/documents/IdentityTheftBrochurenew.pdf

Texas

- http://www.oag.state.tx.us/consumer/identity_theft.shtml
- **[ES]** http://www.oag.state.tx.us/consumer/idtheft_span.shtml
- http://www.oag.state.tx.us/newspubs/opeds/200302blues.shtml

Utah

- http://www.idtheft.utah.gov
- http://publicsafety.utah.gov/investigations/IDTheftlink.htm

Vermont

- http://www.justice.gov/usao/vt/fraud_idtheft.html
- http://www.justice.gov/usao/vt/vwdocs/VictimServicesDirectory.pdf

Virgin Islands

- http://www.idtheftcenter.org/States/virgin-islands.html

Virginia

- http://www.ag.virginia.gov/index.php/citizen-resources/identity-theft
- http://www.ag.virginia.gov/CCSWeb/Reports/IDTheftBook02.pdf
- http://www.dmv.virginia.gov/webdoc/citizen/drivers/identitytheft.asp

Washington

- http://www.atg.wa.gov/ConsumerIssues/ID-Privacy.aspx
- http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/Tips.aspx
- **[ES]**http://www.atg.wa.gov/uploadedFiles/Home/Safeguarding_Consumers/Consumer_Issues_A-Z/Identity_Theft_(Privacy)/IDTheft_Consumer07-07%20Spanish.pdf
- http://www.dol.wa.gov/driverslicense/identitycrimes.html

Washington, D.C.

- http://mpdc.dc.gov/page/identity-theft
- http://mpdc.dc.gov/node/206412

West Virginia

- http://www.ago.wv.gov/consumerprotection/Pages/default.aspx
- http://www.ago.wv.gov/consumerprotection/Documents/Identity%20Theft%20Brochure.pdf

Wisconsin

- http://datcp.wi.gov/Consumer/Office_of_Privacy_Protection/index.aspx
- http://cwagwisconsin.org/elder-law-center/wi-identity-theft-coalition/
- http://privacy.wi.gov/
- **[ES]** http://privacy.wi.gov/spanish/factsheets/FilingComplaintSPANISH.jsp
- http://www.doj.state.wi.us/sites/default/files/dls/consumer-protection/ID_theft_broc.pdf
- **[ES]** http://www.doj.state.wi.us/sites/default/files/dls/consumer-protection/ID_theft_broc-sp.pdf

Wyoming

- http://www.justice.gov/usao/wy/divisions/criminal/criminaldivision.html
- http://www.uwyo.edu/studentatty/civil_criminal/civil_law/consumercredit/identitytheft.html
- http://identitytheftnetwork.org/resource-map/wyoming

Additional Comments

Along with all of the different ways to protect your identity and make it harder for thieves to obtain personal information, one of the best practices is to stay up-to-date with new ways your personal information may be compromised. With the speed of technological advances, including new ways to pay for goods and services, the ways your identity and personal information can be stolen continues to rise. An effort to stay on top of these trends will only better protect you and your loved-ones.