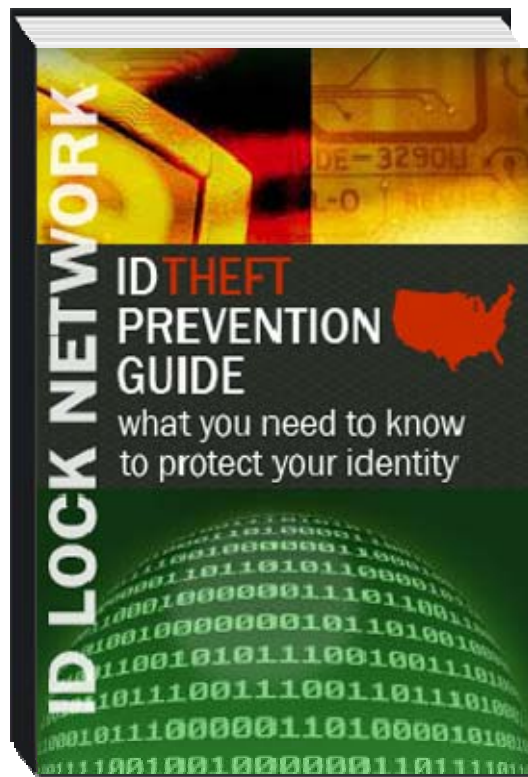


Identity Theft Prevention Guide

Things you should be doing now to protect your identity!



A distribution of IdLockNetwork.com
Copyright © www.idlocknetwork.com

Warning: Do not duplicate, sell, copy the material or redistribute this document under any circumstances

DISCLAIMER & TERMS OF USE

If you do not agree to the following Disclaimer & Terms of Use, please discontinue using this document immediately!

By downloading and becoming in possession of this document you signify your assent and agreement to these terms of use. If you do not agree please delete this file.

Restrictions on use of materials

The material presented in this document is copyrighted and all rights are reserved. Text, graphics, and other intellectual property are protected by US and International Copyright Laws, and may not be copied, reprinted, published, reengineered, translated, hosted, or otherwise distributed by any means without **explicit** permission. All of the trademarks on this site are trademarks of IdLockNetwork.com or of other owners used with their permission.

License and Use

IdLockNetwork.com warrants, and you accept, that IdLockNetwork.com is the owner of the copyright, Links to articles and resources available on this document and the IdLockNetwork.com home page. IdLockNetwork.com and its contributors reserve all rights and no intellectual property rights are conferred by this agreement.

IdLockNetwork.com grants you a non-exclusive, non-transferable license to use this document and this is subject to these Terms and Conditions. This document may be used only for viewing information or for extracting information to the extent described below.

You agree to use information obtained from IdLockNetwork.com databases only for your own private use or the internal purposes of your home or business, provided that is not the selling or brokering of information, and in no event cause or permit to be published, printed, downloaded, transmitted, distributed, reengineered, or reproduced in any form any part of the databases (whether directly or in condensed, selective or tabulated form) whether for resale, republishing, redistribution, viewing, or otherwise.

Nevertheless, you may on an occasional limited basis download or print out individual pages of information that have been individually selected, to meet a specific, identifiable need for information which is for your personal use only, or is for use in your business only internally, on a confidential basis. You may make such limited number of duplicates of any output, both in machine-readable or hard copy form, as may be reasonable for these purposes only. Nothing herein shall authorize you to create any database, directory or hard copy publication of or from the databases, whether for internal or external distribution or use.

Liability

The materials contained in this document are provided "as is" and without warranties of any kind either expressed or implied. **The information contained in this document is merely a guide of best practices, this is NOT a definitive guide or solution for identity theft, nor is there any guarantee that by following these steps you will be completely safe from identity theft.** IdLockNetwork.com disclaims all warranties, expressed or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. IdLockNetwork.com does not warrant that the functions contained in the materials will be uninterrupted or error-free, that defects will be corrected, or that this content or the server that makes it available are free of viruses or other harmful components. IdLockNetwork.com does not warrant or make any representations regarding the use or the results of the use of the material in this document in terms of their correctness, accuracy, reliability, or otherwise. You (and not IdLockNetwork.com) assume the entire cost of all necessary servicing, repair or correction. Applicable law may not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Under no circumstances, including, but not limited to, negligence, shall IdLockNetwork.com be liable for any special or consequential damages that result from the use of, or the inability to use, the materials in this document, even if IdLockNetwork.com or a IdLockNetwork.com authorized representative has been advised of the possibility of such damages. Applicable law may not allow the limitation or exclusion of liability or incidental or consequential damages, so the above limitation or exclusion may not apply to you. In no event shall IdLockNetwork.com's total liability to you for all damages, losses, and causes of action (whether in contract, tort, including but not limited to, negligence or otherwise) exceed the amount paid by you, if any, for accessing this document.

Facts and information at this website are believed to be accurate at the time they were placed on the website. Changes may be made at any time without prior notice. All data provided on this website is to be used for information purposes only. The information contained in this document and pages within, is not intended to provide specific legal, financial or tax advice, or any other advice, whatsoever, for any individual or company and should not be relied upon in that regard. The services described on these pages are only offered in jurisdictions where they may be legally offered. Information provided in our website is not all-inclusive, and is limited to information that is made available to IdLockNetwork.com and such information should not be relied upon as all-inclusive or accurate.

Other Legal Stuff

These Terms of Use will apply to all access to IdLockNetwork.com. IdLockNetwork.com reserves the right to issue revisions to these Terms of Use by publishing a revised version of this document on the home page: that version will then apply to all use by you following

TABLE OF CONTENTS

Introduction..... 1

The facts about identity theft 2

 What is identity theft? 2

 What are security breaches? 2

 Where does this leave you? 2

How identity theft happens 2

What identity thieves can do with your information 3

 Credit card fraud 3

 Phone and utilities fraud 3

 Bank fraud 3

 Personal ID and document fraud 3

 Social security and tax fraud 4

 Medical benefits fraud 4

 Wrongful incrimination 4

What you should do if your identity is stolen 4

How to protect you identity 5

 Computer security..... 5

 Stop carrying so much personal information in your wallet..... 5

 Protecting data at home..... 6

 Protecting your mail..... 6

 Get your name removed from mail and marketing lists 6

 Check your credit report often..... 7

 Setup fraud alerts with all three credit bureaus..... 7

 Secure your identity while on the internet..... 8

How to detect identity theft 9

Advanced methods for protecting your identity 9

How to compare identity theft protection services..... 10

ID protection services to consider..... 11

Other important identity theft resources 12

Conclusion 12

Identity Theft Prevention Guide

Introduction

You may not realize it but during your everyday activities you may be creating opportunities for an identity thief to have an easy payday. From ordering pizza with your credit card to writing checks at the market and even paying your bills online. We never really give these types of activities a second thought because they are in fact simple transactions.

Identity theft is one of the most dangerous crimes on the rise today because of the consequences it always brings to its victims. The process of resolution and recovery from this crime is still ages behind. The financial burdens, ruined credits and often permanently altered medical records are something the victims must resolve all on their own. Although several initiatives have taken place with the backing of the federal government, victims of identity theft are still facing a harsh and daunting task in which they're often held responsible for the consequences until they can prove otherwise.

It has been said by expert sources that the best protection against identity theft is a persistently proactive attitude towards personal information. Merchants and credit bureaus have given themselves the liberty of trading and sharing information that does not belong to them and even though there's no law that prohibits this practice, we as owners of the information being traded, have the right to put a stop to it.

Fighting back against identity theft begins with knowing that you're not safe if you have not taken the steps listed on this document to proactively begin securing your identity and personal financial information from those who are actively looking for it.

Pay close attention to the steps listed here and make it a habit to periodically learn more about how this crime may be evolving and what resolutions or new help is available for victims by visiting IdLockNetwork.com and the different sources listed in the "resources" section of this document.

Identity Theft Prevention Guide

The facts about identity theft

What is identity theft? Identity theft occurs when an individual deliberately appropriates the personal information of another for the purpose of utilizing it to obtain credit, loans, housing, jobs, medical care etc. Once in possession of someone else's identity a thief can run up a series of transactions, which they typically never intend to pay for, leaving the owner of the information responsible for the transactions and consequences caused therein.

What are security breaches? This occurs when a company or institution that handles personal data for a large number of clients or subscribers, is infiltrated by a hacker. They can also happen when one of their employees or computer systems fails to secure this data properly and ending up in the wrong hands. These events happen more than a few times a year. The current figures for these security breaches this year (2008) are 342. This is 69% higher than this time in 2007.

These security breaches happen at institutions like government agencies, health care and hospital facilities, educational institutions, businesses and corporate facilities and financial and banking institutions. It is also estimated that due to these security breaches as many as 22 million or more individual profiles containing very sensitive information have been exposed since 2007.

Where does this leave you? As the consumer or subscriber you are basically on your own to deal with any consequences that may occur due to your information being exposed. One thing consumers need to remember is that realistically there's no way to keep your information from reaching the wrong hands if it is mishandled by these organizations. You may be very well aware that you should never give your information over the phone or email or respond to phishing scams, but employees of these institutions and organizations may not be properly trained or clearly understand the risks of relating and distributing information to third parties, or know about the real dangers of identity theft. Most of that is out of your control.

How identity theft happens

There are many different ways that personal information can be obtained by an identity thief. It's important to point out as well that most identity thieves are more opportunistic than skilled, so often the methods used are opportunities unknowingly created by the information owners. Here's a short list of the most common ways identity thieves can steal your information:

1. They steal your mail by redirecting it to an alternate address by submitting a change of address card to the post office.
2. They may get personal information from you by posing as legitimate companies through email or phone calls. This is a method known as Phishing.
3. They may get your information from businesses or other institutions by stealing personnel records, bribing or conning a clerk who has access to your records, or hacking into computer systems at these institutions; known as security breaches.
4. Online hackers can hack their way into your computer system if your computer is not properly protected while you access the internet.
5. They access and gather information about you from public records, which are freely available to everyone at most local government offices and court houses.
6. They may steal your credit card information by using a data storage device in a process known as "skimming" they simply swipe your card on a device when you make a purchase or they may attach the device to an ATM machine.

Identity Theft Prevention Guide

7. They may steal or find your lost wallet or purse and move quickly to use the information in it before you report your cards lost.
8. They dig through trash to find any readable information you may not have taken the time to shred. This is known as dumpster diving.

Some identity theft victims also report that their identities were actually stolen by someone they know or are related to. It is not uncommon for family members to commit identity theft. Often children are the victims of identity theft by their own family members.

What identity thieves can do with your information

Once in possession of your information, the thief may go to work immediately, especially if it is your wallet or purse that they stole or found or if they purposely redirected your mail.

Credit card fraud:

1. A thief will open new credit card accounts if they have possession of your social security number. With the convenience of the internet, a thief can easily apply online and get a card within 7 working days. They will run up balances on that account under your name and leave you to deal with the bill, which will almost always go delinquent, because you won't know about it until collections come after you.
2. A thief can gain control of more than one account if they redirect your mail, then run up charges on all accounts, and because you are not receiving your bills it may be some time before you realize it.

Phones and utilities fraud:

1. A thief can open a phone and/or wireless phone account or run up charges on your existing account.
2. A thief can also use your name and social security number to turn on utilities such as electrical, gas, water and cable service. Again, they typically never intend to pay the bill so they'll continue using the services without paying ruining your credit with these utilities companies.

Bank Fraud:

1. Thieves can open new bank accounts under your name and SSN and write bad checks.
2. They can also authorize electronic transfers in your name in order to drain your checking or savings accounts.
3. They can also apply for and get loans under your name and leave you with the bill.

Personal ID and document fraud:

1. Identity thieves may even get a driver's license or official ID card using your identity and their picture. This is typical of undocumented foreign workers who enter the country illegally. Normally they keep up with making sure the identity remains in good standing so they can continue using it, but there's always the danger of being incriminated for criminal charges if your name is involved.

Social security and tax fraud:

1. Identity thieves can get employment under your social security number. This is highly typical of undocumented workers.
2. Because your social security number is used to gain employment you may be approached by the IRS for back taxes and be fined heavy fines for failing to properly report your

Identity Theft Prevention Guide

income. This can take time to sort out and normally you'd need legal representation to get the IRS off your back.

Medical benefits fraud:

1. If identity thieves can get employment under your name and social security number then they can also get medical treatment under your name. There is a long list of dangers associated with this medical identity theft but the most severe consequence is that of being given the wrong diagnosis.
2. The thieves may also be able to get Medicaid and Medicare benefits, which can cause a different set of problems if you are eligible for these programs.

Wrongful incrimination:

1. Your information may be involved in a police investigation if they have an ID with your name and driver's license or social security number. Since you don't know this is happening a warrant may be issued for your arrest if you fail to show up for court dates.
2. If someone is able to get a driver's license under your name something as simple as a traffic fine can ruin your perfect record forever.

What you should do if your identity is stolen

Repairing the damages caused to your credit and your financial life always takes time, money and lots of headaches. If you become a victim of identity theft, here's what you need to do:

1. Notify all your creditors, particularly the accounts that have been compromised, that you have been the victim of identity theft and put a freeze on your accounts so that no more charges occur. If new accounts were opened, close them.
2. File a police report immediately. Sometimes this is somewhat difficult since the police do not typically handle these types of cases, so you may be turned away or told to file online or over the phone. However, you must have an actual report that shows that the authorities acknowledge your case, this is important for creditors who require a police report to begin their own investigations. If you are denied filing the report, try another jurisdiction or ask to file a "Miscellaneous Incidents" report. You can also contact your state Attorney General to find out if the law in your state requires the police to file identity theft reports, if not then find out from them where and with whom you can file your report.
3. Complete the **identity theft affidavit**. In order to be sure that you will not be responsible for any debts created by the identity thief, you must properly fill out your identity theft affidavit. The FTC along with a group of credit grantors and attorneys created this affidavit to protect the victims. In the affidavit you must provide all information regarding the theft and yourself. You must also provide a fraudulent account statement. This is where you describe the fraudulent account opened in your name. You must provide a separate account statement for each company that you need to write to.
4. Contact the credit bureaus and notify them that you have been victimized by an identity thief and that you need to activate free identity fraud alerts. These alerts will automatically notify you via email if more changes occur to your credit report. Also these fraud alerts will flag any creditor running a credit check on your account to call and verify verbally with you before approving a new account.
 - Equifax 1-800-525-6285
 - Experian 1-888-397-3742
 - TransUnion 1-800-680-7289

Identity Theft Prevention Guide

5. Report your case to the FTC (Federal Trade Commission) – Your report will aid law enforcement officials across the country in their investigations.
 - Online: www.ftc.gov/idtheft
 - By Phone: 1-877-438-4338 / TTY 1-866-653-4261
 - By Mail: Identity theft Clearinghouse, FTC, Washington, DC 20580

How to protect your identity

Deter identity thieves by following these steps to safeguard your information:

1. Computer Security – one of the most common points of entry for an identity thief is to hack their way into your computer system. Most people often assume that having virus protection is the key to computer security. Virus protection is a must, but you have to consider that when you're on the internet your computer system becomes another node in a giant network of computers that are connected to your ISP's network, where hackers are constantly looking for points of entry into unsecured systems to gather any information left unguarded and anti-virus software alone is not designed to stop every kind of intrusion.

Firewall protection is necessary to make sure that your system is not penetrated and this is particularly true if you like 90% of internet users are running a windows platform like windows XP or windows Vista and have a high speed internet connection that is always on. Firewalls help make you invisible and block unauthorized communications to your system from outer sources. Without it, you basically leave your door open, since your computer's applications utilize network ports to communicate with the different online destinations that you access, this is an opportunity for a hacker to sniff your internet activity and attempt to break into your system.

Anti-Spyware software is also a good level of precaution, if your firewall is not able to block the unauthorized entry into your system, the anti-spyware and anti-virus software on your PC should do the job.

Viruses and spyware are similar but do differ. Viruses are more complex programs, they're able to reproduce themselves and contain the necessary code to cause serious disruption in the stability of a computer system. Spyware programs are typically hosted on websites and they are triggered when you visit these malicious sites, so they're not self contained like viruses and are not able to reproduce them selves. They're designed to collect information and then trigger the downloading of other programs to your system that can do some serious damage.

Having these security software programs installed is not good enough; they must be kept up to date. Software vendors continually release updates to these applications and these updates contain new "signatures", which are the new found spyware and viruses that are being used by hackers and software companies have figured out how to recognize and block them, so you must be sure these programs are updated often for them to be effective.

2. Stop carrying so much personal information in your wallet – Take a close look at your wallet or purse and get rid of the idea that you may need everything in it or that you should keep it full of your personal information just in case or because you never know. This is really the only reason why many people carry so many things in their wallets, including the contact numbers to their credit card and banking institutions, often pin numbers and passwords are also included on written pieces of paper.

Identity Theft Prevention Guide

One thing you should never carry in your wallet is your social security number, this is where the most damage can occur if you lose it and a thief gets a hold of it. SSNs are the most sought after pieces of information because of the potential gains a thief can get from it. So it's best to keep it in a safe at home along with any other piece of id that contains this number. SSNs are typically not needed on day to day activities; very few places would ask for your SSN card as a form of ID, so only carry it when you know you will need it.

Ideally you should only carry in your wallet your driver's license, your debit card for every day spending and one credit card that can get you out of emergencies like having to tow your car or posting a bail if you end up in any kind of trouble. Your health Insurance card is also a necessity, however if it contains your social security number you should also not carry the actual card, instead make a photo copy of it and cut out the last four digits of your SSN. Everything else like market discount membership cards and library cards should be fine as long as your SSN is not listed on them.

3. Protecting data at home – Most of us assume that because our documents are under our roof they're safe from strangers. Well that's partly true, you may not be suspicious about the people you hire to do contract work for you at home, your cleaners or even friends and family. Always file your bills, utility receipts, and anything else that contains your personal information. There's no need for anyone to see this information so keep it locked up in a file cabinet.

Get a shredder and destroy all documents that contain your name, address, account numbers etc. Never throw this information in your trash can, instead it should be shredded. As mentioned above, an approach that thieves use to gather your identity is known as **dumpster diving**, where they willingly dig through your trash to get a hold of any information that's still readable and use it anyway they can. So leaving this information whole only creates an opportunity for someone who's actively looking for this information. Paper shredders are relatively inexpensive and serve a world of good and every home should have one.

4. Protecting your mail – If your mail box is not a lock box, you should seriously consider getting a P.O box address. Directing all your mail to a place where it is secured will minimize the chances of your identity ending up in the wrong hands. Junk mail lists are proof that your name gets traded and sold to companies that intend to market their products and services to you. These companies are not at all interested in protecting your identity. These include credit card offers, pre-approval offers, card dealer discount letters, coupon books etc.

When you order new checks from your bank ask that they deliver the checks to the bank's branch office and not your home. Especially if your mail box is not a lock box, this is a very easy way to lose hundreds and even thousands of dollars from your account. If you're expecting a new credit card, ask the credit card issuer to either send it directly to your door in a certified letter that requires a signature upon receipt. Or if this is not something they're able to provide then get a clear estimate for when your card will arrive and be on the look out for the card in the mail by the estimated time of delivery. Should the card not arrive when promised, call and check on the status before it gets lost or delivered to the wrong place.

5. Get your name removed from mail and marketing lists – As mentioned above your consumer information is traded and passed around without your permission, and there is no law that can stop this. You can, however, take back control of your information by opting out of junk mail lists and pre-approved lists and this will significantly reduce the amount of junk mail you receive and the risk of your information landing in the wrong hands.

Identity Theft Prevention Guide

In order to opt out of these lists, here's what you need to do:

To opt out of pre-approved offers, which are some of the most dangerous pieces of mail floating around with your information, call **(888) 5OPTOUT (888-567-8688)** to opt out of Innovis and the three major credit bureaus, Equifax, Experian and Transunion. The three credit bureaus sell your information to credit companies. Innovis provides credit information to the real estate industry and to marketers about your real estate transactions, they also offer employment screening.

To get your name and address removed from the national mailing lists, you can register with DMACHOICE.org, this option is quicker than doing it by mail.

To get your name and phone number removed from telemarketing databases, visit the [National Do Not Call registry](#).

6. Check your credit report often – Credit card fraud is one of the most common instances of identity theft. You can get your free credit report once a year, but a lot can happen in a year and you need to detect changes on your credit report quickly, because if these changes are due to the actions of an identity thief you can begin taking action and be more effective by catching these activities early on and you can only catch these activities if you have access to your credit report at all times.

There are several ways of doing this. You can get a free credit report once a year with your credit score from all three credit bureaus by visiting AnnualCreditReport.com. This website is a centralized service for consumers to request free annual credit reports. It was created by the three nationwide consumer credit reporting companies - Equifax, Experian and TransUnion. Again you can only do this free once a year.

Ideally you should check your credit once a month or once every quarter and make sure your current accounts are intact and no new records have been entered that were not started by you. Another option is to make use of free fraud alerts, which must be renewed every 90 days. However, fraud alerts will complicate you getting approved for credit and loans that you originate for yourself as well; since this forces your creditors to get a verbal verification from you before they can approve a new account, but if you can live with that, fraud alerts are a great layer of protection and they're free.

You can set up fraud alerts yourself by contacting each of the three credit bureaus and requesting that these fraud alerts be placed and you should renew them yourself every 90 days.

7. Set up fraud alerts with all three credit bureaus – This is fairly easy and one of the most common steps towards identity theft protection, all you have to do is contact the credit bureaus individually and ask them to set free fraud alerts on your behalf. What fraud alerts do is make sure that the any creditor who receives an application for credit under your name, which requires a credit check, will be required to get a personal verification from you that you have in fact submitted an application for credit. Otherwise the application will be denied.

These fraud alerts normally expire in 90 days, but can be renewed if you request again at the end of the 90 days for the alerts to be renewed. Normally if you have been a victim of identity theft the fraud alerts can remain active for up to 7 years without having to renew.

Identity Theft Prevention Guide

8. **Secure your identity while on the internet** – The internet is one of the most dangerous places in terms of the safety of your identity. Because there are so many distractions and popular destinations that almost never emphasize security your identity can easily be taken. Here is a separate list of things you need to be doing and have in place while connected to the internet:
- a. **Don't give out personal information** – many online destinations deliberately ask for personal information in order to give you membership or access to specific information. If anything other than your email is required, you need to consider carefully if trading your information for theirs is worth the risk.
 - b. **Use a secure browser** – No browser is 100% safe, but some are in fact better than others. No one should be going online with Internet Explorer 6.0 or prior to that version. Internet Explorer has undergone a major overhaul with more emphasis on security but even now it is still prone to hacks. Other browsers to consider installing are Firefox and Opera, both offer a high level of security and have strong communities of developers who constantly contribute updates, security and usability features.
 - c. **Ignore email requests for personal information** – email scams and phishing scams via email are still very prevalent because they are in fact still effective. By now more people are aware that financial institutions never request that you verify your personal information via email or phone. These unsolicited email requests come from identity thieves who collect information from unsuspecting victims and often trade this information on identity and financial black markets. Never open these emails if the subject line reads something to the effect that *your account has been compromised* or that *your information must be verified to avoid suspending your account*.
 - d. **Install antivirus, spyware and firewall software** – your computer systems should have all three installed for ultimate protection. You must also make sure that each of these applications are updated frequently to get the latest signatures on new exploits and vulnerabilities. Viruses, spyware software and online intrusions are very common particularly when computer systems are unprotected. Spyware is the type of software that comes into your system uninvited and often runs silently as a background process to disguise its presence; among the most dangerous are keyloggers, which are programs that record your every key stroke particularly when you're online. The purpose of programs like this is to collect your account logins and passwords to any online destination that requires authentication.
 - e. **Use complex passwords** – For online memberships, online banking, your computer user account, and anything else that requires a password you should always practice the habit of creating complex passwords that are not easy to crack. Hackers run password cracking programs, and the more different characters you use in your passwords and the more complex your password is the harder it will be to crack. Use special characters, numbers and capital letters when you create your passwords. Also avoid using obvious things like your birthday or last name or names of your kids as passwords.
 - f. **Create an alias while online** - do not use your real name or provide real information about you on websites that you access for fun and amusement. Create aliases or user accounts that do not give away your true identity. With the popularity of social media, a lot of internet users are finding that networking online through social media is an effective and fun way to get in touch with people who share the same interests. Identity thieves are also present in these social media groups and are always on the lookout for someone they can target easily. Limit the amount of information you enter when you sign up for membership on these social sites.

Identity Theft Prevention Guide

How to detect identity theft

Always be on the alert for signs that your information has been compromised. Some of the most obvious and typical signs are:

- Mail or bills that may have stopped coming to your mail box
- Unexpected credit cards or account statements show up in your mail box
- Denial of credit for no apparent reason
- Call or letters about purchases you did not make
- Charges you did not make appear on your credit card statement or your debit account
- You see new accounts appear on your utility bills when you pay it online
- You get a thank you letter from a financial institution or creditor for opening a new account
- Your savings accounts balance dissipates or gradually decreases
- You get IRS letters for back taxes or failure to report additional income
- You get letters from social security or Medicaid about a claim recently submitted or benefit you're supposedly receiving
- You get denied employment for no particular reason at more than one employer
- You get contacted by the police about an alleged incident in which your identity happens to be involved.
- Your online banking or online credit account logins stop working for no reason

Advanced methods for protecting your identity

You may not be able to keep your information completely safe, but you can certainly make sure that if it does end up in the wrong hands, they'll have a very tough time doing anything with it. Because the numbers of cases of identity theft progressively increase every year, a new industry has emerged to extend the much needed service of centralizing and managing identity theft prevention for everyone.

These services are very effective and all of them use similar methods covering not only all of the prevention steps listed above but much more. But because no single method or service can guarantee 100% that your identity will remain intact, all of these services include an insurance policy, in which the service provider will spend thousands of their own money to restore your identity and your name if you should become a victim of identity theft while you're their subscriber.

The costs are still relatively low for the number of features offered. Features such as:

- **24/7 credit monitoring** – this includes setting up fraud alerts and automatically renewing them every 90 days for you.
- **Monitoring of your personal information on financial black markets** – Thousands of social security numbers are traded on online financial black markets daily, there's nothing you can really do on your own to monitor this yourself. Sophisticated technology is used to scan the hundreds of different suspicious and illegal information trading web sites.
- **Permanent removal of your name from junk lists** – Again this is something you can certainly accomplish yourself, but it helps to automate the process for faster results.
- **Lost or stolen wallet assistance** – losing your wallet can easily turn into the worse day of your life depending on how much of your information you were carrying in it. You can contact all your credit card and bank institutions with one call by having your identity theft prevention service contact them all for you.
- **Identity theft recovery assistance** – should you become a victim of identity theft you will have all the backing necessary to help you get through the process of recovering your

Identity Theft Prevention Guide

identity and restoring your good credit. Doing this on your own would be a daunting task, one that will also cost you plenty of money if you were not covered.

- **Up to a \$1,000,000 insurance/guarantee** – Depending on which service provider you sign up with, you can get anywhere from \$20,000 to \$1,000,000 of identity theft protection insurance should the worst happen.
- **Protect and insure your entire family** – monitoring your own credit may be a manageable task, but monitoring your family's information as well is less than practical and it should be outsourced.
- **Monitoring of utility accounts and wireless service accounts** – Not all providers offer this feature. It's important to know if your name is being used by someone to start utility services with gas, electric and water companies. Even though these people often do pay for these utilities that's your name being used and you could potentially inherit some liabilities.
- **Monitoring of Health Insurance Benefits** – This type of identity theft creates a lot of problems for the victims, so it's important that your health benefits are looked after 24/7 to keep your medical record intact. Currently not every one offers this service, if this is a serious concern to you, you might want to consider [Trusted ID](#) as your identity theft prevention provider.

The features vary per service provider so consider each one carefully since some of these will be more important to you than others. For a complete breakdown of the features including full reviews of some of the top providers, visit our [IdLockNetwork's](#) comparison page.

How to compare identity theft protection services

It's important that you don't get sold on features alone. First assess your own risk and if you have a family, then consider using a service that provides for family coverage. Do not overlook the fact that children are also vulnerable to identity theft. More cases today are involving the information of children and sadly it is often family members who are the thieves.

When comparing identity theft protection services, the costs are relatively economic across all service providers, for the number of features you get. So costs should not be a factor in your decision. Instead consider how much protection you feel you need as an individual. Is medical identity theft a big concern to you? Are you also concerned with internet security? Not all providers carry the same features, whether you compare them on this site or other sites.

Identity Theft Prevention Guide

ID Protection Services to Consider:

TRUSTED ID

Service Benefits:

- ✓ Fraud Flag Placement
- ✓ Credit Card Number Scanning
- ✓ Social Security Number Scanning
- ✓ Lost Wallet Protection
- ✓ Medical Benefits Protection
- ✓ Junk Mail Reduction
- ✓ Anti Spyware Protection
- ✓ Social Security Statement Review
- ✓ Free Annual Credit Reports
- ✓ \$1,000,000 Service Warranty

[ORDER TRUSTED ID](#) – Save 15%

IDENTITY TRUTH

Service Benefits:

- ✓ 24x7 monitoring of malicious sites
- ✓ Advanced notifications of fraud and potential fraud
- ✓ Personal information breach alerts
- ✓ Free fraud alerts from all three credit bureaus
- ✓ Stop pre-approved offers
- ✓ Immediate resolution in case of identity fraud
- ✓ Identity theft insurance and expert guidance
- ✓ Get an Identity Health Score

[ORDER IDENTITY TRUTH](#)

LIFE LOCK

Service Benefits:

- ✓ Fraud alerts from all three credit bureaus
- ✓ Removal from pre-approval offers
- ✓ Removal from junk mail lists
- ✓ Free credit report once a year
- ✓ Lost/Stolen wallet assistance
- ✓ Monitoring of personal data online with eRecon
- ✓ Monitoring of address changes with True-Address
- ✓ \$1,000,000 Service Guarantee

[ORDER LIFE LOCK](#)

Identity Theft Prevention Guide

Other Important Identity Theft Resources

The Federal Trade Commission (FTC) – www.ftc.gov/idtheft

A very thorough guide with plenty of information on how to protect and take action against identity theft on your own. You can file a complaint with the FTC if you have been victimized and you can also find the identity theft affidavit here to help you in the process of disputing fraud.

Identity Theft Resource Center (ITRC) - <http://www.idtheftcenter.org>

A non-profit organization dedicated exclusively to the study and prevention of identity theft. The ITRC provides support for victims as well as education.

Anti-Phishing Working Group (APWG) - <http://www.antiphishing.org>

A volunteer organization committed to the fight against fraud and identity theft by promoting best practices and education to consumers.

On Guard Online - <http://www.onguardonline.gov>

On-Guard Online provides practical solutions to and tips to the general public focusing on internet fraud and personal computer security.

The President's Task Force - <http://www.idtheft.gov>

The task force deployed a new front line in the fight against fraud and identity theft, established in 2006, this initiative calls for a coordinated effort between government and commercial entities to establish a strategic plan to more accurately fight this crime and aid its victims.

The US Department of Justice - <http://www.usdoj.gov/criminal/fraud/press/>

The department of justice has a press room archive and several articles to educate consumers and the major types of schemes used today by savvy thieves. From internet to telemarketing and foreign scams, this archive is a complete guide on how to prevent fraud.

Privacy Rights Clearinghouse - <http://www.privacyrights.org>

The PRC is also a non profit organization based in San Diego, CA. dedicated to providing information to consumers, raising awareness about technology and the many risks it can create and much more.

Conclusion

We sincerely hope that this has been an educational and practical guide for you to take action and begin protecting yourself from this crime. The threat of identity theft is real and it has claimed many victims already. Again, the key to making sure your identity remains intact is to take consistent and proactive action with your personal information.

Please check back with www.idlocknetwork.com periodically to check for updates to this document and other resources we may find useful to communicate to our readers. Good luck!