



## ParentPapers: Protecting Your Identity

*Last Updated: 03 June, 2007*

<http://www.secureparents.com>

Welcome to SecureParents, a free website dedicated to you, the busy parent. We are dedicated to helping you at no cost secure you and your family in today's information age. We understand the tremendous pressures and time limits that parents have. Our resources are designed by experts to be simple yet provide the critical information you need. ParentPapers are a series of papers designed to give you this information in less than 15 minutes.

### PAPER TOPIC:

In this paper we discuss how to protect one of your most personal and important assets, your identity.

*This paper is copyright "SecureParents". You are free and encouraged to distribute this paper to whomever you like. The only limitation is this paper cannot be modified nor sold for commercial purposes. This paper is distributed under the Creative Commons license, Attribution-NonCommercial-NoDerivs 3.0 Unported. In no event will SecureParents be liable for any damages, including loss of data, lost profits, cost of cover, or other special, incidental, consequential, direct or indirect damages arising from this documentation or the use thereof, however caused and on any theory of liability. This limitation will apply even if SecureParents has been advised of the possibility of such damage. You acknowledge that this is a reasonable allocation of risk.*

## Your Identity

The United States Federal Trade Commission (FTC), as the nations consumer protection agency, is one of the leading government organizations fighting identity theft. They define identity theft as

*"Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes."*

There are a variety of different types of information that help make up your identity. For example, your identity includes your name and home address, social security number, drivers license number, credit card account, bank account or even your frequent flier number. Basically, any information that helps identify you. The more information a criminal collects about you, the more he can do with it and the more value it has. There are a tremendous number of ways criminals can use your information. Examples include using your stolen identity to open a new credit card, cloning your ATM card, creating counterfeit checks, getting government benefits, rent a house, or commit crimes using your name. The end result is the criminal benefits but you pay for it. Lets learn about some steps we can take about protecting our identity.

## Protecting Your Identity

In today's digital age your information is collected and stored on computers around the world. Its stored in databases at your old school, at the stores you shop at, at large data collection brokers or even your local library and city hall. In many ways you cannot protect your information simply because you do not control it. However, there are some steps you can take to protect yourself.

1. Securing your own computer so criminals cannot compromise nor steal information from your systems while you are online. Refer to our ParentsPaper: [Ten Steps to Securing Your Home Computers](#) for more information.
2. Do not give your information away. Only give it to organizations or individuals you trust and only when you initiate the communication. If someone calls you or emails you asking for your information, you do not give it unless you contacted that individual or organization first. When in doubt, ask the person for their name and phone number and tell them you will call them back.
3. Shred any identifiable printed information before throwing it out.
4. Do not email your private information (such as your Social Security Number). If a trusted organization has a legitimate need for your information, give it over the phone. Email is insecure. Not only could someone intercept the communication but your data then resides on that person's or organization's computer, potentially for years.
5. If you do not want to receive pre-approved credit offers, call 1-888-5-OPT-OUT (1-888-567-8688) to be removed from the lists of major credit bureau lists.

### **Detecting Identity Theft**

Since in many ways you do not control your own information, the best way to protect yourself against identity theft is to detect it as soon as possible. If you detect identity theft right after it happens, you have a much better chance of mitigating the damage. However, if you detect identity theft months after it happens, the damage will be much greater and will require far more work and cost to recover from. Below are six common ways to detect if your identity has been stolen. This list is based on the FTC's website.

1. Seeing charges on your credit card bills or withdrawals or wire transfers in your checking account you can't explain. The easiest way to detect this activity is to check your financial and credit card statements every month.
2. Fraudulent or inaccurate information on your credit reports, including accounts and personal information, like your Social Security number, address(es), name or initials, and employers. The easiest way to detect this is with credit report monitoring. For more information about credit reports, refer to the ParentPaper: [Protecting Your Credit Rating](#).
3. Failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
4. Receiving credit cards that you didn't apply for.
5. Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason. If this happens your credit score may have been negatively impacted and you will want to check your credit score. For more information about credit scores, refer to the PaperPaper: [Protecting Your Credit Rating](#).
6. Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

### **Responding to Identity Theft**

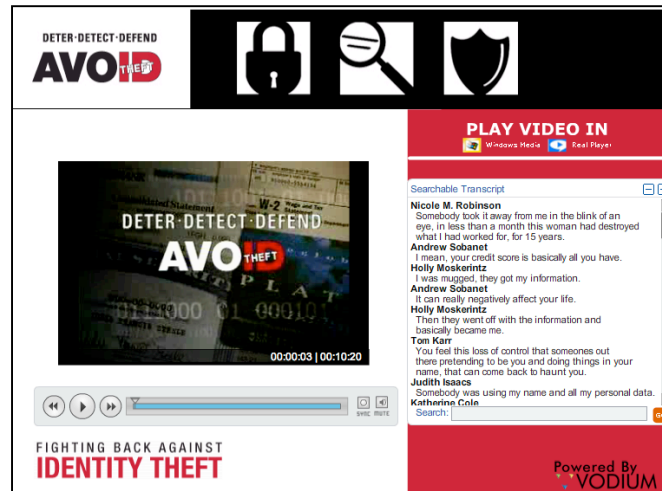
Okay, you believe you may have been a victim of identity theft, now what? Below are five steps you can take. This list is based on the FTC's website.

1. Place a fraud alert on your credit, which we explain in greater detail below.
2. Monitor and review your credit reports. We explain more about that in the PaperPaper: [Protecting Your Credit Rating](#).
3. Close the accounts you think have been impacted. If you think you are a victim of financial identity theft, for example if you lost your checkbook, credit card or ATM card or had them stolen, contact your local financial institution. Tell them to cancel your old card or checks, issue a new one, and flag your account so they are aware of the situation. This is helpful in the future for any follow-up. If a government issued identification has been lost, such as your license, contact the government agency that issued it. Ask them to cancel your old one, issue a new one, then flag your account so no one else can get a document in your name.
4. The next step is to file an online Complaint form with the FTC at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html>

5. Finally, create an Identity Theft Report. This report will be critical to proving to a variety of organizations (such as your bank) that you are a victim of identity theft. To do this, file a report with law enforcement. You may want to try your local law enforcement first, depending on the type of identity theft, and if that does not work file a police report with the federal law enforcement.

When responding to identity theft, be sure to keep a log recording every conversation you have with law enforcement, government officials, financial representatives or anyone else helping to resolve your case. Include the time and date you had the conversation, what was discussed, and whom you talked to. This information could be important when attempting to resolve issues or track down answers.

For more information on protecting, detecting and responding to identity theft, we highly recommend the FTC's website. In addition to extensive amounts of information, they offer a 10 minute video on identity theft. See Figure 1 for more information.



**Figure 1: FTC's video on identity theft. Find this video and learn more online at the FTC website, <http://www.ftc.gov/bcp/edu/microsites/idtheft/>**

### Fraud Alert

A fraud alert is an alert you issue with the three credit agencies. In the United States there are three nationwide consumer credit reporting companies (also known as credit bureau's) responsible for your credit rating; Equifax, Experian, and TransUnion. These three companies collect extensive amounts of information about you, such as when you open bank accounts, credit card payments, take loans, or miss payments on your electric bill. These organizations are defined by and must follow the rules laid down by the government, including the Fair Credit Reporting Act (FCRA, 15 U.S.C. 1681 et seq.) and Fair Debt Collection Practices Act (or FDCPA). These companies then take your information, run it through a variety of advanced algorithms and determine your credit score. For more information on the credit card agencies, refer to the ParentPaper: [Protecting Your Credit Rating](#).

A fraud alert notifies all three credit agencies that you believe you may be an identity victim. Whenever a merchant or organization does a credit inquiry on your credit score, the credit agency notifies the inquirer that you have a fraud alert. This forces them to go through additional steps before they can get your credit score. For example, let's say you have a credit fraud alert and you apply for a home equity loan from your bank. Normally your bank would simply do a credit check, find out what your score is, and determine your home equity loan based on the information. However, if you have a fraud alert on your credit score the bank will have to take additional steps. For example, they most likely will have to contact you at a later time (such as the next day over the phone) confirming that it was you who wanted the home equity loan and if they can proceed with the credit check. Additional steps like this help protect you if your identity may be compromised.

There are two types of fraud alerts, *initial fraud alert* and *extended fraud alert*. An initial fraud alert is very simple to apply for, you simply call one of the three credit agencies and ask to apply the alert. However, the initial fraud alert only applies for 90 days. The extended fraud alert is when you have a more serious situation and have actually applied for an Identity Theft Report with law enforcement. An extended fraud alert lasts for seven years. You can learn more about fraud alerts and how to apply for one at

<https://www.annualcreditreport.com/cra/helpfaq#fraudalert>

### Summary

Protecting your identity is a difficult challenge. One of the biggest problems you face is that you are not in control of most of your information. As a result, the best way for you to protect your identity is to monitor your identity, especially financial and credit activities, and to react immediately if something suspicious happens.

### Websites

In this paper we mentioned several important websites to protecting your identity. Here you can find them all listed. Whenever you are in doubt about the validity of a website, start first with the FTC's website which ends in '.gov'.

Federal Trade Commission	<a href="http://www.ftc.gov/bcp/edu/microsites/idtheft/">www.ftc.gov/bcp/edu/microsites/idtheft/</a>
AnnualCreditReport	<a href="http://www.annualcreditreport.com">www.annualcreditreport.com</a>
Experian (credit agency)	<a href="http://www.experian.com">www.experian.com</a>
TransUnion (credit agency)	<a href="http://www.transunion.com">www.transunion.com</a>
Equifax (credit agency)	<a href="http://www.equifax.com">www.equifax.com</a>
ParentPapers:	
Protecting Your Credit Rating	<a href="http://www.secureparents.com/papers">www.secureparents.com/papers</a>
Ten Steps to Securing Your Home Computers	<a href="http://www.secureparents.com/papers">www.secureparents.com/papers</a>

### About Us

Concerned about protecting your online finances and your credit rating? Wondering who is collecting information on your children? Confused on how to best secure your computers at home? SecureParents is designed for you - the busy, working parent. It's your one stop for all the steps you need to take to secure yourself and your family in today's rapidly changing information age. The website is free, supported by and for parents. If you have any comments or suggestions about this paper, our website, or you have a story you would like to share with us we would love to hear from you! Please send all feedback or questions to [info@secureparents.com](mailto:info@secureparents.com).