

How to Protect Yourself from Identity Theft

Also how get a free credit report, and what to do if your identity has been compromised

CONTENTS

1. Introduction	2
1a. Test your identity quotient	2
2. Steps to Protection	3
2a. Step 1 - Contact the Credit Bureaus and set a fraud alert	3
3. Step 2 - Restrict Junk Mail	6
4. Step 3 - Block pre approved credit offers.....	7
5. How do thieves steal an identity?	8
6. Quiz - Test your knowledge about Restoring an Identity	9
6a. other quizzes Spyware, phishing	9
7. Link to Identity Theft Victim's Guide	9
8. Legal Stuff	10

1. Introduction

I am going to share with you for free, what I pay for on a monthly basis. I use a company called [LifeLock](#) (if you are interested in [LifeLock](#) just click on the word LifeLock in blue and underlined - you will be brought to their website.) LifeLock provides identity protection services for me. Because of time limitations the \$9.00 a month I pay for the service is a great investment. I am also a student and recently did research for a paper about avoiding Identity Theft; the result of my research is this e-book. I hope the time you spend browsing this book saves you from the horror of Id Theft or if your identity has already been compromised, I hope this e-book helps you on the road to recovery.

1a. Test your identity quotient

First, you may want to test your "Identity Quotient"
<http://www.privacyrights.org/ITquiz-interactive.htm>

Understanding Your Score:

- 100 + points - Recent surveys* indicate that 7-10 million people were victims of ID theft last year. You are at high risk. We recommend you purchase a paper shredder, become more security-aware in document handling, and start to question why people need your personal data.
- 50-100 points - Your odds of being victimized are about average. Higher if you have good credit.
- 0-50 points - Congratulations!. You have a high "IQ." Keep up the good work and don't let your guard down now.

2. Steps to Protection

Below is the basic process that [LifeLock](#) uses. Todd Davis, the president of LifeLock is so sure that his steps will protect from ID Theft, that he regularly gives out his social security number. The LifeLock system is guaranteed to work up to \$1 million. "My Social Security Number is 457-55-5462" says Todd Davis, co-Founder and Chief Executive Officer of [LifeLock](#)." LifeLock has been featured on many of the major networks, MSNBC, CNN, CNBC, and WSJ.com.

2a. Step 1 - Contact the Credit Bureaus and set a fraud alert

A fraud alert allows you to take control of who issues you credit and when. The alerts tell any company that uses your credit report, such as a bank or insurance company; they must contact you before the can:

- Issue credit
- Arrange loans
- Open accounts
- Increase credit lines
- Open new credit cards
- Otherwise influence your assets

If a company can't contact you directly at a number you designate of if you do not approve the transaction, the transaction stops.

The company I use to protect my credit for \$9.00 a month set alerts with Equifax, Experian, and TransUnion within the first hour, [Lifelock](#).

You can contact each of the bureaus individually, (they say they share the information but that is not a 100% guarantee)

TransUnion
Fraud Victim Assistance Department
Phone: 800-680-7289
Fax: 714-447-6034

P.O. Box 6790
Fullerton, CA 92634-6790

Equifax
Consumer Fraud Division
Phone: 800-525-6285 or: 404-885-8000
Fax: 770-375-2821

P.O. Box 740241
Atlanta, GA 30374-0241

Experian
Experian's National Consumer Assistance
Phone: 888-397-3742

P.O. Box 2104
Allen, TX 75013

Or you can set your fraud alert Online.

Learn more about Fraud alerts from Experian at their website.
http://www.experian.com/consumer/fraud_fags.html

An excellent resource for information about Identity Theft is a government website <http://onguardonline.gov/idtheft.html> . I want to quote a little from their site about fraud alerts.

“An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report with one nationwide consumer reporting company, you'll get information about ordering one **free credit report** from each of the companies. It's prudent to wait about a month after your information was stolen before you order your report. That's because suspicious activity may not show up right away. Once you get your reports, review them for suspicious activity, like inquiries from companies you didn't contact, accounts you didn't open, and debts on your accounts that you can't explain. Check that information — like your SSN, address (es), name or initials, and employers — are correct.”

Notice two things the site tells us about fraud alerts;

1. Fraud alerts are only good for 90 days – that means you have to remind yourself to reset the fraud alert every 90 days. (That's one of the reasons I pay [LifeLock](#) to reset my alerts every 90 days.)
2. Setting a fraud alert entitles you to a free credit report, without going to one of those online places that give you a free credit report so the can you're your personal information.

Free Credit Report – read the above paragraph starting with “An initial fraud alert..... It is very important that you set a fraud alert with the credit reporting agencies to protect your identity.

3. Step 2 - Restrict Junk Mail

One of the way to restrict the amount of junk mail in your mail box is to sign up with the Direct Marketing Association's mailing preference service.

<http://www.dmaconsumers.org/offmailinglist.html>

From their website:

"Some consumers would like to receive less advertising mail at home. The Mail Preference Service (MPS) is designed to assist those consumers in decreasing the amount of national non-profit or commercial mail they receive at home. This section will tell you how to use MPS.

The Mail Preference Service (MPS) is a consumer service sponsored by The Direct Marketing Association (The DMA). Established in 1917, The DMA is the oldest and largest national trade association serving the direct marketing field."

You visit their site and fill out their form. Note there is a \$1.00 charge to use their service.



[LifeLock](#)

4. Step 3 Block pre approved credit offers

You can opt out of prescreened credit offers by visiting.
<https://www.optoutprescreen.com/?rf=t>

At their website you will learn:

“Under the Fair Credit Reporting Act (FCRA), the Consumer Credit Reporting Companies are permitted to include your name on lists used by creditors or insurers to make firm offers of credit or insurance that are not initiated by you ("Firm Offers"). The FCRA also provides you the right to "Opt-Out", which prevents Consumer Credit Reporting Companies from providing your credit file information for Firm Offers. Through this website, you may request to:

Opt-Out from receiving Firm Offers for Five Years - (electronically through this website).

Opt-Out from receiving Firm Offers permanently - (mail Permanent

Opt-Out Election form available through this website).

Opt-In and be eligible to receive Firm Offers. This option is for consumers who have previously completed an Opt-Out request - (electronically through this website).”

By selecting the Opt-out link, you will have the option to opt out permanently by mail or by a website link that allows you to opt out for five years.

5. How do thieves steal an identity?

The Federal Trade Commission

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

Has a website that is a one-stop national resource to learn about the crime of identity theft.

It provides detailed information to help you deter, detect, and defend against identity theft. An example of what you'll find at the FTC site:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>

“How do thieves steal an identity?”

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.

Skilled identity thieves may use a variety of methods to get hold of your information, including:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
5. **Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
6. **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

6. Quiz - Test your knowledge about Restoring an Identity

Test your knowledge about Identity Theft and restoring your identity once it has been compromised. Visit the link below.

http://onguardonline.gov/quiz/idtheft_quiz.html

6a. Other quizzes on Spyware, phishing, and security using wireless hot spots

Other quizzes to test yourself about Spyware, phishing scams, and protecting yourself while using wireless hot spots.

<http://onguardonline.gov/quiz/index.html>

7. Link to Identity Theft Victim's Guide

Identity Theft Victim's Guide

If your Identity has been Stolen you can find an Identity Theft Victim's guide at <http://www.privacyrights.org/fs/fs17a.htm>

Identity Theft: What to Do if It Happens to You

Included in detail description at the website are the following topics and more:

1. Notify credit bureaus / fraud alerts

- 1a. Monitor your credit reports.**
 - 1b. Security freeze.**
 - 2. Law enforcement.** Report the crime to your local police or sheriff's department right away
 - 3. Federal Trade Commission.** Report the crime to the FTC.
 - 4. What to do with *new credit accounts opened by the imposter.***
 - 5. Handling problems with your existing credit or debit accounts.**
 - 6. Debt collectors.** If debt collectors try to get you to pay the unpaid bills on fraudulent accounts,
 - 7. Check and banking fraud.** *If you have had checks stolen or bank accounts set up fraudulently*
 - 8. ATM cards.** *If your ATM or debit card has been stolen or compromised ,*
 - 9. Brokerage accounts.** You do not have the same protections against loss with brokerage accounts as you do with credit and debit card or bank accounts.
- 10. Fraud involving U.S. mail.**

8. Legal Stuff

This document is for information purposes only. No representation or warranties of any kind exist with regards to completeness or accuracy of the information within the book. The author and publisher shall in no event be held liable for any loss or other damages caused by the use and misuse of or inability to use any or all of the information described in this book.

By using the information in this book, you agree to do so entirely at your own risk.



[LifeLock](https://www.lifelock.com)