White Lighthouse
Investment Management

Protecting Your Credit And Financial Information After The Equifax Data Breach

(For Americans and Non-Americans with a US Social Security Number)

Jonathan Lachowitz, CFP® | Financial Planner | Investment Advisor

LinkedIn

Sept 30, 2017

John Wanvig, CFP® | Financial Planner | Investment Advisor

LinkedIn

Marina Hernandez, CFP®

On September 7th, Equifax, one of the three major Credit Reporting Agencies in the United States (TransUnion and Experian are the other two) announced that private information from over 143 million Americans (and presumably non-Americans with US Social Security Numbers, such as Green Card Holders) consumers had been stolen by cyber criminals. This is shocking but it is not surprising that another large Financial Institution has had a large harmful data breach. In this case, apparently the user name and password combination was “admin” & “admin” for this business-critical database. Equifax’s cybersecurity practices need updating and auditing!

The type of information that was stolen includes: Social Security Numbers, birthdates, names, addresses, credit card numbers, and more. Essentially, most of the primary information needed to steal someone’s identity who is a US Taxpayer. This latest data breach confirms what perhaps we should all have assumed before; our personal data is not safe and we should start acting as though

much of our private information is available for a very low cost on the internet. The rest of this note will provide you with information and recommendations on how you can protect yourself, your credit, and your identity from financial fraud.

First, you should assume that most of your privately identifiable information is relatively easily available on the internet for free or a very small fee and that it will stay there indefinitely. True privacy and anonymity doesn't exist for most people and your information is worth a lot more to you than it is to any criminal.

Two-thirds of cases of ID theft involve stolen credit cards, not stolen identities. US federal regulations limit your liability, usually to $50 per account, and that is often waived by card issuers. Identity theft that involves opening accounts in your name, can be much costlier and time consuming to repair.

Given these facts and the Equifax Data Breach, we recommend that you take protective action and remain aware and vigilant in order to avoid becoming a more serious victim of cybercrime. Below you will find some important information and our recommendations on the actions you should take to protect yourself.

Important information:

A. At this link, you will be able to find out if Equifax will confirm that your data was compromised. https://www.equifaxsecurity2017.com/potential-impact/
B. All US Consumers, whether their data was part of this breach or not, will be eligible for one free year of credit monitoring using Equifax's product Trusted ID Premier. You can read more about the data breach on their site here: https://www.equifaxsecurity2017.com/
C. The Federal Trade Commission has put out an article here with several suggestions that we also believe you should consider: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

Our Recommendations:

1st Level of Security (like an alarm system on your house): HIGHLY RECOMMENDED

Set yourself up with a Credit Monitoring Service. Choose one that monitors all three credit agencies. This link highlights most of the major credit monitoring services: https://aaacreditguide.com/credit-monitoring-services/

Unfortunately, like a lock on your front door, this is a service you will need forever. We now live in a cybercrime world.

a) **Their services:** These products alert you when someone uses your data to open an account in your name and spend your money, (open a credit card, mobile phone account, bank loan, store credit, even a mortgage). Most services also offer

insurance, up to $1mill, to clear up any credit problems or cyber-theft. It can take a considerable amount of time and effort to fix the mess and the best of these services provide you with professionals that can help you through the process of clean-up.

Our Favorites

a) **AAA Credit Monitoring** from the American Automobile Association. Jonathan uses this service and has had a good experience. Allows coverage of your children.

b) **Lifelock Credit Monitoring**: Highly rated and well-designed service that provides the coverage and services you need. It also has a well-developed mobile application.

c) **Identity Force**: Very good, complete service that is highly rated and reasonably priced as well.

d) **Identity Guard**: Most comprehensive service. Well rated.

2nd Level of Security (like a good alarm system and video monitoring): NOT ESSENTIAL BUT BETTER PROTECTION IF YOU FEEL AT RISK

1. **Put a Credit Freeze on your credit file.** This will prevent new issuers of credit from accessing your credit report and therefore new credit accounts will not be opened. If you don't need a new credit account (credit card, mortgage, etc) this is a good way to protect yourself. There will be a fee to un-freeze the account if you need a new credit line.

2. **Put a Fraud Alert on your credit file.** This will alert creditors to take extra caution before opening an account in your name. This link tells you the difference between a Credit Freeze and a Fraud Alert: you can implement either by contacting one of the 3 main agencies. https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#difference

Other HIGHLY RECOMMENDED ACTIONS:

1. Every year, request a FREE copy of your Credit Report at this site: https://www.annualcreditreport.com/index.action

2. Monitor carefully and regularly your Bank, Brokerage and Credit accounts looking for suspicious activity.

3. Use a Brokerage firm that provides a solid guarantee against fraud: This is one reason we are a big fan of using Charles Schwab and company: http://www.schwab.com/public/schwab/nn/legal_compliance/schwabsafe/security_guarantee.html

This article compares the policies of the top 5 brokerage firms in the US: http://www.marketwatch.com/story/hacked-this-is-what-the-top-5-brokers-will-do-for-you-2015-10-27

4. If possible, set up your credit cards to alert you by text message or email when making a significant purchase. This can help you respond rapidly to fraud. John has this feature on his Capital One credit card.

5. File your tax return as early as possible to prevent cybercriminals from filing fraudulent tax returns in your name and stealing your tax refund; this has been another common way criminals with your data can try and steal from you.

6. Beware of phishing emails used by cybercriminals to install spyware or ransomware on your personal devices. Phishing emails can look legitimate, may appear to come from financial institutions where you hold accounts or from the IRS, and they will have a link that you are asked to click on to verify information. When you click on the link, a virus is downloaded onto your device that can lock you out of it or be used to steal your detailed personal information. Whenever you receive emails with links, do not click on them and instead visit the webpage of the purported sending organization to follow up on the request safely.

7. Here are many recommendations not specifically related to this data breach:

    a. Don't send documents with your signature by email and when stored electronically, ensure they are in a system that is as secure as possible.

    b. Don't store secondary information online, or give it over to individuals or businesses where the data is not critical for them to have.

    c. Use two-factor authentication whenever possible to add a second level of protection and make it harder for hackers to login to your accounts. Email, social media accounts, financial institutions, the White Lighthouse Client Portal, and other website containing sensitive information will generally offer the liability to use a mobile device to receive a unique code that needs to be entered to verify login attempts to your account from a new device.

    d. Close any unnecessary accounts.

    e. Consider only using credit cards that guarantee 100% against fraudulent use.

    f. Ask yourself the question: Would you do anything different if you assumed that over 90% of your "private" data was in the public domain?

Additional Information and Resources

Contact Information for the 3 main Credit Reporting Agencies

Equifax – www.equifax.com – PO Box 740241, Atlanta, GA 30374-0241. 1-800-685-1111.

Experian – www.experian.com – PO Box 2104, Allen, TX 75013-0949. 1-888-EXPERIAN (397-3742)

TransUnion – www.transunion.com – PO Box 1000, Chester, PA 19022. 1-800-916-8800

Credit Reports and the Overseas American:

We have researched some of the challenges facing overseas Americans who want to get a copy of their credit report. Experian was the only agency that seemed to recognize this on their website as a challenge and they have a solution. You can still request a copy of your report by mail. See the link and instructions below:

http://www.experian.com/blogs/ask-experian/credit-education/faqs/credit-report-faqs/

How do I request my credit report if I live outside the United States? If you are an American citizen living abroad and would like to order a copy of your credit report, send all the following information to Experian, PO Box 2002, Allen, TX 75013.

- Your full name, including middle initial and generation information
- Your date of birth
- Your social security number
- Two proofs of your current mailing address (such as a copy of your driver's license, utility bill, insurance statement, bank statement, or telephone bill that shows your name at your current mailing address)
- Your previous US address
- Copy of a government-issued ID card

We hope you have found this article useful and that you will take some concrete steps to better protect yourself. Just like burglars prefer a home with no alarm system, hackers prefer to steal from easy targets. By following some of our recommendations, you will reduce the odds that you face a time consuming and costly Identity Cyber-Crime.

If after reading this article you still have questions or are uncertain as to what steps you should take in your situation, then please contact us for a discussion.