Winningham
Becker
& Company, LLP

21031 Ventura Blvd
Suite 1000
Woodland Hills, CA
91364-2227
Tel (818) 598-6525
Fax (818) 598-6535
www.wbac.com

Equifax Hack – Now What

The dust has started to settle on the roller coaster of what to do now that Equifax has been hacked.

Here is what we have learned over the past month since the breach was announced.

On September 7, 2017 it was announced by Equifax that they had a data breach or unauthorized access to their networks from May 2017 – July 2017. Immediately following the breach there were many reports of what happened and possible outcomes of this breach.

The outcomes are as follows:

- 145.5 million identities of US consumers are at risk and information accessed includes Social Security numbers, birthdates, addresses and potentially driver's license numbers.
- 209,000 US consumers credit card numbers were accessed
- 182,000 US consumers certain dispute documents with personally identifiable information was accessed.

Time will tell what impact the breach has on your individual identity, credit, and future financial data. The main takeaway is that now is the time to watch your credit regularly. Even though your information might have been accessed it does not mean you are a victim of identity theft.

Our goal in sending you this letter is to alert you on how to protect yourself from a potential identity theft.

If you are one of the 145.5 million individuals whose information was accessed you can check by going to a website setup by Equifax.

Here is the website: https://www.equifaxsecurity2017.com/

If your information was accessed or not accessed, with cyber security getting harder every day, now is the time to take steps to protect your financial security.
Here are two ways to immediately protect your credit:

1. **Freeze your credit** - This will limit fraud on any new accounts. The cost of this differs state by state. If you are a CA resident here are the fees **per agency** and **per person**:
    a. Permanent Freeze –
        i. Not a victim of ID theft - $10
        ii. 65 or older and not a victim of ID theft – No fee
        iii. Victim of identity theft – No fee

    b. Temporary or permanent credit freeze lift -
        i. Not a victim of ID theft - $10
        ii. 65 or older and not a victim of ID theft– $5
        iii. Victim of identity theft – No fee

A credit freeze is the only way to protect identity theft by limiting the ability of someone to open a new account with your identity. This will not protect you from fraud on your current active accounts. If you freeze your credit, you may not lock your credit.

2. Lock **your credit** – This will allow you to instantaneously lock your credit with the respective credit monitoring agencies that you sign up with. You must sign-up for the respective agencies that offer the credit lock. The fees associated with this are $20 **per month** for both Transunion and Equifax and $20 **per month** for Experian, for a total cost of roughly $40 **per month**. This is an evolving way to protect your credit and will change as Equifax is coming out with a new service in January. If you lock your credit, you may not freeze your credit.

In addition to the two main ways to protect your credit here are some additional immediate ways to consider:

1. Sign-up with a credit monitoring service which could be included with the cost of locking your credit. Equifax is currently offering a year of credit monitoring with TrustID Premier (owned by Equifax) if your information was accessed. There are many credit monitoring services and we can discuss others with you.

2. Request copies of your credit report from the main credit reporting agencies – Equifax, Experian, TransUnion, and the lesser known Innovis – and examine them for any unexplained accounts opened in your name. You are entitled to order a free copy of your credit report from each of the major credit reporting agencies every 12 months through AnnualCreditReport.com .

3. Place a fraud alert on your credit file through the main credit reporting agencies. This is a warning to creditors that you may be a victim of identity theft. They should take additional precautions to verify that anyone seeking credit in your name really is you.

4. Ask your financial institutions about additional security measures for your accounts. For example, fraud alerts or code words can be placed on some of your bank accounts and credit cards for additional protection. In many cases, you can also enable text and email alerts – especially for debit and credit cards – that will potentially notify you of any suspicious activity.

Here are some long-term steps to take in protecting your credit:

1. Examine your account statements monthly and check for any unexplained activity. Frequently change your passwords.

2. File your taxes early. Sometimes identity thieves use Social Security numbers to get a tax refund or obtain a job. File as soon as you have all the information you need – before an identity thief has an opportunity to file in your name – and be sure to respond to any letters from the IRS.

3. Be aware of potential phishing emails, phone and mail scams, and be especially wary of emails that appear to come from the source of the breach. Criminals often take advantage of breaches and craft sophisticated phishing emails encouraging consumers to provide personal information. Be cautious with links embedded in emails and if you are not sure type in the web address of the link you received manually.

Here are some additional resources:

http://www.idtheftcenter.org/

https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

Should you have any questions please let us know.

Our goal is to alert you on the ways to protect your credit and financial security.

Sincerely,

Winningham Becker & Company, LLP