The Navigator

A Financial Planning Resource from
Pekin Singer Strauss Asset Management



September 2017

Special Issue

The Equifax Data Breach: What Do I Do?

by Matthew Blume, CFA
and Bill Pekin, CFA

By now, we expect that nearly all of our clients are aware of the recently-announced data breach at Equifax, in which the sensitive personal information of 143 million Americans was stolen by hackers. The data breach of a major credit bureau has been covered extensively in recent days by the news media, so we will not waste time rehashing the details of the breach. Instead, as your financial advisor, we want to focus our attention on providing you with tangible recommendations that you can implement immediately to try to minimize the negative potential impacts of this breach. Below are some steps that clients can take in an effort to protect themselves from the fallout of the Equifax data breach.

- ***Assume you are a victim of the breach.***

  This breach has affected more than one-half of the adult population of the United States, so there is a reasonably good probability that your personal information was, in fact, exposed in this breach. Equifax has provided a website where potential victims can verify whether or not they were impacted by the breach. However, a number of reports have indicated that the Equifax website may not be working properly and should not be relied upon. Therefore, the most prudent course of action is that you should assume that you were impacted and should take appropriate precautionary steps.

- ***Closely monitor your credit accounts.***

  The information that was accessed by hackers in this breach included not only the personal information of millions of Americans, such as birthdate and Social Security number, but also credit card information. This means that the hackers may be able to open new credit accounts on behalf of victims while also attempting to use existing credit accounts. You should closely monitor all of your credit accounts for abnormal activity, and not just in the near term. Thieves will often wait for months before using stolen credit information in order to lull victims into the false security that their information was not jeopardized. For this reason, you should continue to monitor your credit accounts indefinitely and diligently in order to spot any fraud attempts.

- ***Consider enrolling in a credit monitoring service.***

  As part of its response to the data breach, Equifax is offering one year of free credit monitoring through its TrustedID Premiere service, which monitors credit requests at Equifax and the two other major credit bureaus (Experian and TransUnion). People who were affected by the breach can enroll in the TrustedID Premiere service on the Equifax website after they have verified that their information was affected. However, it is important to note that Equifax is not enrolling customers immediately. Instead, individuals who want to enroll in the service are given a date to return to the site to complete their enrollment. Equifax is not sending out reminders to complete enrollment.

  While Equifax is offering its service for free to victims of the data breach, we encourage clients to consider enrolling in credit monitoring from a company other than Equifax. The fact that the company is not enrolling customers immediately exposes victims to greater risk by giving the hackers time to use the stolen information. In addition, the company's security measures and processes have clearly been called into question and should

Pekin Singer Strauss Asset Management

161 North Clark Street, Suite 2200, Chicago, IL 60601 | www.pekinsinger.com
312.554.7525 | 800.648.6361 | matt@pekinsinger.com

be viewed with skepticism. Clients can sign up for credit monitoring from other trusted services, such as LifeLock, TransUnion, or Experian.

- ***Obtain a free copy of your credit report.***

  All Americans are entitled to one free credit report from each of the three primary credit bureaus (Experian, Equifax, and TransUnion) each year. Clients should visit AnnualCreditReport.com to access their free credit report and check for new credit accounts opened in their names. We recommend that clients pull one report from one of the credit bureaus immediately and then pull reports from the other two bureaus at three to four month intervals going forward.

- ***Consider putting a freeze on your credit.***

  Probably the most effective way to protect yourself from the potential negative impacts of the Equifax data breach is to put a freeze on your credit. A credit freeze places tight restrictions on who can view your credit. Credit card companies, landlords, mortgage lenders, and many other entities pull credit reports when vetting applications for products or services. Placing a freeze on your credit will make it impossible for these entities to view your credit report, thereby making it impossible for thieves and fraudsters to open new credit accounts in your name. However, there is a cost associated with freezing your credit (typically $5 to $10 per credit bureau), and doing so can create additional steps for you if you decide to open a new credit line in the future. Once your credit has been frozen, it must be unfrozen in order to open a new credit line. This requires contacting each credit bureau, and it may involve a small fee. When you enact a credit freeze, you will be provided with a PIN that you will need in order to lift the freeze when you contact the credit bureaus.

  If you would like to put a freeze on your credit, contact the three credit bureaus:
  Experian (1-888-397-3742),
  Equifax (1-800-349-9960), and
  TransUnion (1-888-909-8872).

We strongly urge clients to address this issue immediately. The more time that passes before steps are taken to protect one's credit after a data breach, the greater the risk of a fraud event. Enacting the recommendations above in a timely manner can materially reduce the risks created by the Equifax data breach.

Data breaches, identity theft, and fraud are an unfortunate part of modern life, and there is no way to eliminate these risks entirely. However, addressing issues immediately when they arise can help to minimize the repercussions from such events. In addition, there are actions that clients can take before a breach occurs that may further reduce the risk of being a victim of identity theft or fraud. We encourage clients to review the Navigator that we wrote about the risks related to identity theft and measures that can be taken to minimize and mitigate these risks. And of course, if you have additional questions or concerns about this data breach or identity theft more broadly, please do not hesitate to reach out to us.
