Transitions

PROTECTING YOUR PRIVACY IN A POST DATA BREACH WORLD

The recent hack into the Marriott/Starwood Hotels database impacted up to 500 million customers worldwide. To place this in perspective, the population in the United States is 325 million, so it is reasonable to assume a widespread impact on this data breach. We now all live in a post data breach world. So, a quick review of ways to protect your privacy seems the best way to start the New Year.

To illustrate the magnitude of breaches in the last few years, my personal information was hacked by the Chinese when they broke into a supposedly secure database of a U.S. Government Agency. Then my credit card background information was breeched in a database hack of a large retailer. To make matters worse, in response to a request from a news reporter, one of our securities regulators inadvertently released parts of their database containing my confidential personal information. Although we cannot prevent these types of breaches from occurring, there are simple steps one should take to better protect personal information.

Let's begin with recognizing that your data is being tracked everywhere and is being used. Large data aggregators like Amazon, Google, and Facebook use all the personal information everyone provides in the conduct of their business. Next time you log into these types of sites, look at your preferences and either block or remove information about yourself. For example, these companies really do not need to know your birthdate. If they require that information, this is the time to change your records and become either younger or older.

continued next page

Herb Diamant
PRESIDENT & SENIOR
PORTFOLIO MANAGER

DIAMANT
ASSET MANAGEMENT

170 Mason Street
Greenwich, CT 06830
(203) 661-6410

continued from page 1

2 When accessing web sites using public Wi-Fi, such as in any hotel, airport, or coffee shop, assume everything you are typing is being recorded by others. Although it is fine to conduct a basic search, this is not the place to open any important web site like your bank account. This may seem obvious to you, yet this type of breach happens all the time.

3 Review your monthly statements. When a credit card is compromised, the hackers typically try a small charge at a gas station before charging larger items. Although banks will remove fraudulent charges, this will only occur if you notify them in a timely manner. Best practice is to review each credit card and bank statement, on at least a monthly basis, to confirm the charges are valid.

4 The most important step is to change your passwords periodically, preferably several times a year. Every New Year's resolution should include changing important passwords. Begin by identifying the sites you visit and categorize them into either "important" or "low risk" sites. Strong passwords are needed for logging in to an important site like your email or bank account. By contrast, if someone hacks into a low risk site like your online newspaper, they only gain access to read the newspaper.

5 For passwords to your important websites, there are common best practices to follow. Never use your name or address in the password. And never use the same password for another website. Since longer passwords are more difficult to crack, I advocate using a complicated phrase, that is meaningful to you, and includes a capital letter and a special character. Two examples of phrased passwords are "thequickbrownfoxjumpedovertheLazydogin18" or "Hawaiihasgreatwaves%3". They may be harder to remember, but they are also much harder to hack. When the hackers try to use the information gained from other data breaches, your reoccurring password changes may prevent them from accessing your important web sites.

Large data aggregators like Amazon, Google, and Facebook use all the personal information everyone provides in the conduct of their business. Next time you log into these types of sites, look at your preferences and either block or remove information about yourself.

continued from page 2

6. Use multi-factor authentication. This is a very important step to secure your privacy. This simple process of confirming your identity requires two or more pieces of evidence to verify you are the one accessing your website. This should be used for any website containing important personal information. Either use their help desk or online instructions to go through the steps to set this up. The first place to start is to add multi-factor authentication to your email. When you forget or lose your password on a website you use, the website will often email you a link to confirm your identity and reset your password. This means if your email password is compromised and there is no second layer of authentication to confirm your identity, a hacker now has been given the ability to access all your website accounts that lack multi-factor authentication!

The most important step is to change your passwords periodically, preferably several times a year. Every New Year's resolution should include changing important passwords.

When I log into my personal Gmail account from someplace other than my home computer, after entering my password, the second step is Google sends me a text message code directly to my cell phone, which I promptly enter to complete the login process. This extra step prevents a hacker, who was able to learn my name and password, from gaining access to this information, because they will not receive the code being sent only to my cell phone.

These simple steps should keep you safer in this Post Data Breach World. Feel free to share this article with your friends and family. Should you want to talk further on this important topic, give us a call with any questions.

Written by: **Herb Diamant**, President and Senior Portfolio Manager
Please feel free to contact us with any questions or comments at **(203) 661-6410** or email Herb directly at **herb@portfolioadvisor.com**

CREATIVE SOLUTIONS TO WEALTH MANAGEMENT

Diamant Asset Management was built on a foundation of family and friendships with ethics and integrity as our guiding principles. As an independent Registered Investment Advisor, we take our fiduciary responsibility seriously and act as a guardian of your wealth.

Managing wealth through the transitions of life. It's what inspires us to do what we do every day.