computer dimensions
520.743.7554
info@computerdimensions.net
www.computerdimensions.net

The Marriott Breach And What You Need To Know

As you may have heard, Marriot has reported that their Starwood reservation database was hacked, potentially compromising upwards of 500 million records. Marriott is one of the largest hotel chains in the world. Anyone who made a reservation for a Starwood property on or prior to September 18, 2018 is at risk. Breached information includes names, credit card numbers, birth dates, arrival and check out dates, and passport numbers.

Large database breaches such as this are a big problem. If a credit card gets compromised, while certainly inconvenient, the card can be changed. Personal information such as passport numbers, birth dates, and names are NOT easily changed. Major incidents such as this are likely to continue so let's take this opportunity to practice smart security responses and behaviors.

First, understand that we live in the age of big data where vast amounts of information are stored about people. Through no fault of your own, this data can be occasionally hacked and it is important to understand what you should do if you are affected. You should always visit the official website of the breached entity or call them directly to get the facts and their recommended steps of action. Marriott has created a website - https://answers.kroll.com where people can educate themselves about the incident. One of the options they offer is people can register a free account at WebWatcher. This is a service that will notify people if their data has been hacked and is being targeted by cybercriminals. Services such as this are helpful, but there are other steps you should take when you are a victim of a breach.

- **Monitor Your Financial Accounts**: Watch your credit carefully. Most credit card companies have a service where they will notify you if a charge is over a certain amount or can send you daily reports of your financial activity. This is a great service to activate. You will minimize the chances of unauthorized transactions in the coming weeks.

- **Starwood Accounts**. If you have a Starwood (Marriott) account, change your password. Regardless of whether your account has been reported as breached, error on the side of caution. This is always a standard practice if a service you use has been compromised.

- **Activate A Security Freeze**: A Security Freeze is one of the most effective steps you can take to protect yourself from a cybercriminal who is seeking to use your information for identify fraud. Unfortunately, few people are aware of it. A security freeze locks your credit score, so no one can access them. This means that while your credit score is frozen no financial organization can check what your credit score is, meaning no one will give you (or a malicious actor) a loan or credit card. The pain is that you must manually set up a security freeze with each of the four credit bureaus. In

addition, if you want to apply for a new loan or credit card you will need to manually unlock your credit service. But really, how often do you apply for a new loan or credit card?

- **Beware Social Engineering Scams**: In the coming weeks following a breach, bad actors will take advantage of the incident and launch countless phishing emails, phone calls or text messages in an attempt to fool people. Remember, Marriott or any legitimate business will never ask you to provide your password by phone or email.

In the event you do fall victim to Identity Fraud, the FTC has created a great site to help you recover - https://www.identitytheft.gov. Regardless of the situation, always practice smart security behaviors and if you have security concerns reach out to Computer Dimensions anytime.