Marriott Provides Update on Starwood Database Security Incident

Jan 4, 2019

Update as of April 17, 2024:

Following an investigation with several leading data security experts, Marriott initially determined that the payment card numbers and certain passport numbers in the database tables involved in the Starwood database security incident that Marriott reported on November 30, 2018 were protected using Advanced Encryption Standard 128 encryption (AES-128). Marriott has now determined that the payment card numbers and some of the passport numbers in those tables were instead protected with a different cryptographic method known as Secure Hash Algorithm 1 (SHA-1).

BETHESDA, Md., Jan. 4, 2019 /PRNewswire/ -- Marriott today is providing an update on the number of guests whose passport numbers and payment card numbers were involved in the Starwood reservations database security incident announced by the company on November 30, 2018.

Working closely with its internal and external forensics and analytics investigation team, Marriott determined that the total number of guest records involved in this incident is less than the initial disclosure. Also, the number of payment cards and passport numbers involved is a relatively small percentage of the overall total records involved.

"We want to provide our customers and partners with updates based on our ongoing work to address this incident as we try to understand as much as we possibly can about what happened," said Arne Sorenson, Marriott's President and Chief Executive Officer. "As we near the end of the cyber forensics and data analytics work, we will continue to work hard to address our customers' concerns and meet the standard of excellence our customers deserve and expect from Marriott."

Marriott is updating its press release of November 30, 2018, which announced that the company determined on November 19, 2018 that there was unauthorized access to a Starwood guest reservations database. In that release, the company said that it believed the incident involved information about up to approximately 500 million guests who made a reservation at a Starwood property* on or before September 10, 2018, although at that point the company had not completed the analytics work to identify duplicative information.

Update on the Number of Guests Involved

Marriott now believes that the number of potentially involved guests is lower than the 500 million the company had originally estimated. Marriott has identified approximately 383 million records as the upper limit for the total number of guest records that were involved in the incident. This does not, however, mean that information about 383 million unique guests was involved, as in many instances, there appear to be multiple records for the same guest. The company has concluded with a fair degree of certainty that information for fewer than 383 million unique guests was involved, although the company is not able to quantify that lower number because of the nature of the data in the database.

Passport Information Update

Marriott now believes that approximately 5.25 million unencrypted passport numbers were included in the information accessed by an unauthorized third party. The information accessed also includes approximately 20.3 million encrypted passport numbers. There is no evidence that the unauthorized third party accessed the master encryption key needed to decrypt the encrypted passport numbers.

Marriott is putting in place a mechanism to enable its designated call center representatives to refer guests to the appropriate resources to enable a look up of individual passport numbers to see if they were included in this set of unencrypted passport numbers. Marriott will update its designated website for this incident (https://info.starwoodhotels.com) when it has this capability in place. The website lists phone numbers to reach the company's dedicated call center and includes information about the process to be followed if guests believe that they have experienced fraud as a result of their passport numbers being involved in this incident.

Payment Card Information Update

Marriott now believes that approximately 8.6 million encrypted payment cards were involved in the incident. Of that number, approximately 354,000 payment cards were unexpired as of September 2018. There is no evidence that the unauthorized third party accessed either of the components needed to decrypt the encrypted payment card numbers.

While the payment card field in the data involved was encrypted, Marriott is undertaking additional analysis to see if payment card data was inadvertently entered into other fields and was therefore not encrypted. Marriott believes that there may be a small number (fewer than 2,000) of 15-digit and 16-digit numbers in other fields in the data involved that might be unencrypted payment card numbers. The company is continuing to analyze these numbers to better understand if they are payment card numbers and, if they are payment card numbers, the process it will put in place to assist guests. Further updates will be made to the dedicated website: https://info.starwoodhotels.com.

Guests who have questions related to their payment cards should visit https://info.starwoodhotels.com for more information, including toll-free phone numbers to reach the company's dedicated call center.

Starwood Reservations Database Discontinued

The company has completed the phase out of the operation of the Starwood reservations database, effective the end of 2018. With the completion of the reservation systems conversion undertaken as part of the company's post-merger integration work, all reservations are now running through the Marriott system.

Guest Support

Marriott continues to offer the following services to help guests monitor and protect their information:

Dedicated Website and Call Center

- Marriott has established a dedicated website (https://info.starwoodhotels.com) and call center to answer questions guests may have about this incident. The frequently asked questions on https://info.starwoodhotels.comhave been updated and may be further supplemented from time to time. The call center is open seven days a week and is available in multiple languages.

Free Web Monitoring

- Guests from countries and regions listed on the site have the opportunity to enroll in web monitoring services free of charge for one year. Please visit https://info.starwoodhotels.com and click on Free Identity Monitoring to learn more.

*** Starwood brands include:** W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels. Starwood branded timeshare properties (Sheraton Vacation Club, Westin Vacation Club, The Luxury Collection Residence Club, St. Regis Residence Club, and Vistana) are also included.

Marriott International, Inc. (NASDAQ: MAR) is based in Bethesda, Maryland, USA, and encompasses a portfolio of more than 6,700 properties in 30 leading hotel brands spanning 129 countries and territories. Marriott operates and franchises hotels and licenses vacation ownership resorts all around the world. The company also operates award-winning loyalty programs: Marriott Rewards®, which includes The Ritz-Carlton Rewards®, and Starwood Preferred Guest®. For more information, please visit our website at www.marriott.com, and for the latest company news, visit www.marriottnewscenter.com. In addition, connect with us on Facebook and @MarriottIntl on Twitter and Instagram.

IRPR#1

View original content:http://www.prnewswire.com/news-releases/marriott-provides-update-on-starwood-database-security-incident-300772768.html

SOURCE Marriott International, Inc.

Connie Kim, 301-380-4028, NewsRoom@marriott.com