



Washington Regional Threat Analysis Center

Intelligence Brief

November 30, 2018

Product Number: 2018-11-043

Marriott Data Breach Impacts up to 500 Million Guests

Today, hospitality company Marriott International reported a data breach of its Starwood reservations database that exposed the personal information and booking details of up to 500 million guests.

- According to Marriott officials, the affected database contained guest information associated with reservations made at Starwood properties on or before September 10, 2018. The ongoing investigation suggests that an unauthorized party had access to the database since 2014.
- The compromised data of approximately 327 million guests include a combination of names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, genders, reservation information, and guest communication preferences. Encrypted payment card data of some guests was also stolen in the breach, but it is currently unknown whether the unauthorized party can decrypt and view that information. For the remaining guests, the compromised information was limited to their names, mailing addresses, email addresses, or other information.
- Marriott International released an official [statement](#) about the breach on their website and will be notifying impacted guests via email beginning today. The company also established a dedicated [website](#) and call center to handle inquiries and will be providing guests with the opportunity to enroll in a credit monitoring service for one year at no cost.

The WRTAC recommends affected Marriott International guests take the following measures to protect themselves against fraud and identity theft that could result from this breach:

- Monitor payment card accounts for unauthorized activity and report any fraudulent charges immediately to the associated financial institution.
- Enroll in the free credit monitoring service provided by Marriott International.
- Contact the three major credit bureaus—Equifax, TransUnion, and Experian—and place a security freeze on personal credit files to reduce the risk of identity theft. As of September 21, 2018, placing a freeze on credit files is free for consumers. More information is available on the US Federal Trade Commission's [website](#).
- Be wary of scammers attempting to use the news of this data breach to further victimize Marriott guests via phishing emails and fraudulent telephone calls. Never click on links or open attachments from unexpected emails and never reveal sensitive personal or financial information via email or over the phone during an unsolicited call.