**Josh Kaul**
**Wisconsin Attorney General**

**P.O. Box 7857**
**Madison, WI 53707-7857**

**NEWS FOR IMMEDIATE RELEASE**

October 11, 2024

# AG Kaul Announces $52 Million Multistate Settlement with Marriott for Data Breach of Starwood Guest Reservation Database

MADISON, Wis. – Attorney General Josh Kaul announced today that a coalition of 50 Attorneys General has reached a settlement with Marriott International, Inc. as the result of an investigation into a large multi-year data breach of one of its guest reservation databases. The Federal Trade Commission, which has been coordinating closely with the states throughout this investigation, has reached a parallel settlement with Marriott. Under the settlement with the Attorneys General, Marriott has agreed to strengthen its data security practices using a dynamic risk-based approach, provide certain consumer protections, and make a $52 million payment to states. Wisconsin will receive $833,045 under the settlement.

"Data breaches like this one can result in harm to consumers," said Attorney General Josh Kaul. "Companies that have confidential consumer information must keep it safe."

Marriott acquired Starwood in 2016 and took control of the Starwood computer network in 2016. However, from July 2014 until September 2018, intruders in the system went undetected. This led to the breach of 131.5 million guest records pertaining to customers in the United States. The impacted records included contact information, gender, dates of birth, legacy Starwood Preferred Guest information, reservation information, and hotel stay preferences, as well as a limited number of unencrypted passport numbers and unexpired payment card information.

Shortly after the breach of the Starwood database was announced, a coalition of 50 Attorneys General launched a multi-state investigation into the breach. Today's



DOJ Communications Office DOJCommunications@doj.state.wi.us (608) 266-1220

settlement resolves allegations by the Attorneys General that Marriott violated state consumer protection laws, personal information protection laws, and, where applicable, breach notification laws by failing to implement reasonable data security and remediate data security deficiencies, particularly when attempting to use and integrate Starwood into its systems.

Under the terms of the settlement, Marriott has agreed to strengthen and continually improve its cybersecurity practices. Some of the specific measures include:

- Implementation of a comprehensive Information Security Program. This includes new overarching security program mandates, such as incorporating zero-trust principles, regular security reporting to the highest levels within the company, including the Chief Executive Officer, and enhanced employee training on data handling and security.
- Data minimization and disposal requirements, which will lead to less consumer data being collected and retained.
- Specific security requirements with respect to consumer data, including component hardening, conducting an asset inventory, encryption, segmentation to limit an intruder's ability to move across a system, patch management to ensure that critical security patches are applied in a timely manner, intrusion detection, user access controls, and logging and monitoring to keep track of movement of files and users within the network.
- Increased vendor and franchisee oversight, with a special emphasis on risk assessments for "Critical IT Vendors," and clearly outlined contracts with cloud providers.
- In the future, if Marriott acquires another entity, it must timely further assess the acquired entity's information security program and develop plans to address identified gaps or deficiencies in security as part of the integration into Marriott's network.
- An independent third-party assessment of Marriott's information security program every two years for a period of 20 years for additional security oversight.

These settlement terms are grounded in a well-developed risk-based approach in which Marriott not only needs to conduct an annual enterprise level risk assessment, but it must also perform risk analyses throughout the year for changes to security controls. Those ongoing risk assessments must address the criteria of "harm to others" – which would include potential harm to consumers.

As part of the settlement, Marriott will give consumers specific protections, including a data deletion option, even if consumers do not currently have that right under state



DOJ Communications Office DOJCommunications@doj.state.wi.us (608) 266-1220

law. Marriott must offer multi-factor authentication to consumers for their loyalty rewards accounts, such as Marriott Bonvoy, as well as reviews of those accounts if there is suspicious activity.

Joining Wisconsin in this multistate settlement are Alabama, Arizona, Arkansas, Florida, Nebraska, New Jersey, New York, Ohio, Pennsylvania, Vermont, Alaska, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Mexico, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wyoming and the District of Columbia.



DOJ Communications Office DOJCommunications@doj.state.wi.us (608) 266-1220