FOR IMMEDIATE RELEASE

Media Contacts:
press@oag.state.md.us
410-576-7009

Attorney General Anthony G. Brown Announces $52 Million Multistate Settlement with Marriott for Data Breach of Guest Reservation Database

BALTIMORE, MD (October 9, 2024) – Attorney General Anthony G. Brown announced today that his office, along with a coalition of 49 other attorneys generals' offices, 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. Along with a coalition of other states, Maryland co-led the investigation into the data breach. 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 the states. Maryland will receive $2,214,224 from the settlement.

"Marylanders should not have to choose between staying in a hotel and protecting their privacy. Consumers should be able to trust that companies will take reasonable steps to protect their personal information," **said Attorney General Brown**. "This settlement ensures that Marriott hotel guests can rest easy knowing that their personal data will be better protected moving forward."

Marriott acquired Starwood in 2016 and took control of its computer network. Over a four-year period, from July 2014 until September 2018, intruders went undetected in the Starwood, and later Marriott, system. 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. The attorneys general contend that Marriott misrepresented the nature and extent of the data security protections it maintained over the data it identified as consumer personal information.

Today's settlement resolves allegations that Marriott violated Maryland's Consumer Protection Act and Personal Information Protection Act by failing to implement reasonable data security and fix data security deficiencies, particularly when attempting to use and integrate Starwood

into its systems. The Federal Trade Commission, which has been coordinating closely with the attorneys general throughout this investigation, has also reached a parallel settlement with Marriott.

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

- Implementing 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 technical security requirements with respect to consumer data.
- Increased vendor and franchisee oversight and clearly outlined contracts with cloud providers.
- In the future, if Marriott acquires another entity, it must timely assess the acquired entity's information security program and develop plans to promptly address identified gaps or deficiencies in security as part of the integration into Marriott's network.
- An external third-party evaluation of Marriott's information security program every two years for a period of 20 years.

As part of the settlement, Marriott will give consumers specific protections, including a data deletion option. Marylanders will have the ability to ask Marriott to delete their data, which is a right they do not currently have under state law. Marriott must also 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.

Maryland, Connecticut, and Oregon as well as the District of Columbia, Illinois, Louisiana, Massachusetts, North Carolina, and Texas co-led the multistate investigation, assisted by the Executive Committee of Alabama, Arizona, Arkansas, Florida, Nebraska, New Jersey, New York, Ohio, Pennsylvania, and Vermont, and joined by Alaska, Colorado, Delaware, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Maine, Michigan, Minnesota, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Mexico, North Dakota, Oklahoma, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

###

https://www.marylandattorneygeneral.gov/press/2024/100924a.pdf