BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

PRESS RELEASE

Attorney General Frosh Advises Consumers to Take Steps to Protect Personal Information Following Marriott Data Breach

Company Announces as Many as 500 Million Customers' Personal Information May Have Been Accessed

BALTIMORE, MD (November 30, 2018) – Bethesda-based Marriott has announced that the personal information of as many as 500 million customers may have been accessed via its Starwood guest reservation database on or before September 8, 2018. The company's investigation found that there had been unauthorized access to the Starwood database since 2014.

"The Marriott data breach is one of the largest and most alarming we've seen. My office will be taking a hard look at Marriott's actions to understand the circumstances that led to the breach," said Attorney General Frosh. "We will also be working with the company to make sure all customers who may have been impacted are notified and provided the resources to protect their personal information. We will be closely monitoring the company's response to ensure that consumers are protected while we continue to investigate the data breach. I strongly urge consumers to take active and necessary steps to prevent any misuse of their information."

Marriott believes that the breach compromised the personal information of up to approximately 500 million guests who made a reservation at a Starwood property. Information that may have been compromised includes name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (SPG) account information, date of birth, and gender. For some, the information also includes payment card numbers and payment card expiration dates.

Marriott has set up a website and call center to assist consumers who may have been impacted at info.starwoodhotels.com. The company will also notify via email affected consumers whose email was in the Starwood guest reservation database.

Attorney General Frosh advises consumers who may have been impacted to take the following steps:

- Check your credit reports from all three of the major credit reporting agencies: Equifax, Experian, and TransUnion. Reports can be obtained for FREE by visiting www.annualcreditreport.com. Unrecognizable accounts or activity could indicate identity theft.
- Place a credit freeze on your files. A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that credit freezes must be obtained from each of the credit reporting agencies. A credit freeze won't prevent a thief from making

charges to your existing accounts, such as debit and credit cards. Parents or guardians of minor children may also place a credit freeze on behalf of their child. For more information on how to obtain a credit freeze, please visit http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/freezing.aspx

- Monitor your existing credit card and bank accounts closely for changes you do not recognize.