



One Hundred Fifteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

December 3, 2018

Mr. Arne Sorenson
President and Chief Executive Officer
Marriott International
10400 Fernwood Road
Bethesda, MD 20817

Dear Mr. Sorenson:

I write because I am troubled by the massive data breach Marriott International (Marriott) announced on Friday, November 30, 2018 – the second largest of all time.¹ As incoming Chairman of the Committee on Homeland Security in the U.S. House of Representatives, I am disturbed by the evolving scale and scope of data breaches affecting Americans, the types of actors who may be interested in the data, and the nefarious purposes for which bad actors might use stolen data. Toward that end, I would like to meet with you to discuss how Marriott is responding to this breach and hardening its networks to prevent data breaches in the future.

On Friday, Marriott announced that hackers may have accessed the data of 500 million customers who stayed at its Starwood properties since 2014.² About 327 million customers may have had some combination of their arrival and departure dates, email address, mailing address, phone number, passport number, gender, and date of birth compromised.³ Additionally, hackers may have accessed the information necessary to decrypt stolen credit card information.⁴ Although it does not appear that any of the information accessed has appeared on the dark web, the breadth of the data would be attractive to both criminals and state actors.⁵

¹ Press Release, “Marriott Announces Starwood Guest Reservation Database Security Incident,” Marriott International (Nov. 30, 2018), <http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/> (last accessed Dec. 1, 2018); Uri Berliner, “Marriott Acknowledges Data Breach at Starwood Hotels,” *NPR* (Nov. 30, 2018), available at <https://www.npr.org/2018/11/30/672168736/marriott-acknowledges-data-breach-at-starwood-hotels>.

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ Nicole Periroth, et al., “Marriott Hacking Exposes Data of Up to 500 Million Guests,” *The New York Times* (Nov. 30, 2018), available at <https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html>.

We have entered an era where the data collected and stored to carry out and expedite routine business transactions can be weaponized against us. The data Marriott stores about its customers is a treasure trove for cyber criminals looking to make money and state actors hoping to gain intelligence about government officials. Breaches have the potential to undermine our economic and national security interests, and, to date, we have struggled to discourage hackers from investing time and resources into gaining unauthorized access to sensitive data. We must do better.

I would like to discuss the actions Marriott has taken in the wake of the breach, and how Marriott is thinking of security differently following a breach of this magnitude. For example, the breach of Starwood's reservation systems began four years before it was detected and before Starwood was acquired by Marriott. I am concerned about what that says about Starwood's ability to detect and remove the malware on its systems and about the type of cybersecurity review Marriott performs upon acquiring a company. I want to learn how Marriott plans to improve its capability in these areas. Moreover, I would like to discuss the value of threat information shared through the Travel ISAC, Hospitality Technology Next Generation, or by the Department of Homeland Security directly, and how it informs Marriott's investments to secure its networks and manage risk.

Thank you for your attention to my request. I look forward to meeting with you. If you have any questions or require additional information, please contact Alison Northrop, Chief Director for Oversight, at (202) 226-2616.

Sincerely,



BENNIE G. THOMPSON
Ranking Member