Testimony of Arne Sorenson, President & CEO, Marriott International

Before the
Senate Committee on Homeland Security & Governmental Affairs
Permanent Subcommittee on Investigations
March 7, 2019

Chairman Portman, Ranking Member Carper, and Members of the Subcommittee, thank you for the opportunity to testify today.

The subject the Subcommittee is tackling – private sector cyber-attacks – is an increasingly urgent one that has hit Marriott International directly with the data security incident that we announced on November 30, 2018. We deeply regret this incident. We are committed to supporting our affected guests and enhancing security measures to protect against future attacks.

For 91 years, Marriott has been in the business of serving people. We began as a small family business in Washington, D.C., serving hamburgers and root beer as The Hot Shoppes. Today we are a global hospitality company, conducting operations in all 50 of the United States and 130 countries and territories. Throughout that time, we have built our reputation by putting people first and focusing on the care of our guests.

As a company that prides itself on taking care of people, we recognize the gravity of this criminal attack on the Starwood Guest Reservation Database and our responsibility for protecting our guests' data. To our guests, including our employees who have stayed at Starwood hotels, I sincerely apologize. We are working hard every day to rebuild your confidence.

I. Timeline of Events

In order to explain our current understanding of the incident, it is helpful to start with a chronology of events. Because this incident involved the Starwood Guest Reservation Database,

I will begin with the merger of Marriott and Starwood Hotels & Resorts Worldwide in September 2016.

A. Merger with Starwood

On November 15, 2015, Marriott signed a merger agreement with Starwood, which was announced publicly the following day. The transaction closed on September 23, 2016. During the intervening ten months, we obtained information about Starwood's technology and network and assessed how to integrate the two systems, although our inquiry was legally and practically limited by the fact that, until the merger closed, Starwood remained a direct competitor of Marriott.

Following this evaluation, we made the decision to retain Marriott's reservation system as the central system for the combined group of hotels and to retire Starwood's reservation system. Migrating all of Starwood's 1,270 hotels onto Marriott's reservation system while avoiding disruption of the reservation process for guests and hotels was a significant undertaking over a period of two years. After the close of the merger, we continued to operate the Starwood system and we invested in additional information security measures for that system. In November 2018, we accelerated the timeline to retire the system and, as of December 18, 2018, we are no longer using the Starwood Guest Reservation Database to conduct business operations.

B. Discovery and Investigation of the Incident

On September 8, 2018, Accenture, which managed the Starwood Guest Reservation Database, contacted Marriott's IT team with information about a Guardium alert generated on September 7. Guardium is an IBM security product used on the Starwood system to help secure databases. The Guardium alert was triggered by a query from an administrator's account to return the count of rows from a table in the database. Such a query would not return the content of these rows, only the total number of rows in the table.

As part of our investigation into the alert, we learned that the individual whose credentials were used had not actually made the query. We implemented containment and access control measures, and continued to do so throughout the investigation that followed.

We quickly engaged legal counsel and industry experts to investigate the scale and scope of the incident. On September 10, 2018, two days after Accenture elevated the alert, Marriott brought in third-party investigators to conduct a full investigation into the circumstances that led to the alert and to assist with containment measures. On September 17, 2018, the investigators uncovered a Remote Access Trojan ("RAT"), a form of malware that allows an attacker to covertly access, surveil, and even gain control over a computer. I was notified of the ongoing investigation that day, and our Board was notified the following day.

C. Investigation of the Incident

Uncovering the full scope of the attack took significant forensic work. We worked with and relied on experts in the field to conduct a thorough and careful investigation. In early October 2018, the investigators found on some systems evidence of malware, including MimiKatz, a tool that searches a device's memory for usernames and passwords. Through the first two weeks of November 2018, although there was evidence of an unauthorized party on the Starwood network since July of 2014, our investigators had found no evidence that the attacker had accessed guest data in the Starwood Guest Reservation Database.

On October 29, 2018, we contacted the FBI to provide them with information about the tools used by the attacker, the timeline of the intrusion, and forensic findings. Since that time, we have provided the FBI with several updates and ready access to forensic findings and information to support their investigation. At the same time, our investigative experts continued their

painstaking forensic work, rolling out endpoint detection technology on devices across the Starwood network.

On November 13, our investigators discovered evidence that two compressed, encrypted files had been deleted from a device that they were examining. The files were encrypted and the actual content was unknown. There was also evidence to suggest that those two files had potentially been removed from the Starwood network. Six days later, on November 19, 2018, investigators were able to decrypt the files, and found that one contained an export of a table from the Starwood Guest Reservation Database containing guest data, while the other contained an export of a table holding passport information.

On November 19, 2018, upon learning that the files the attacker compressed and encrypted contained personal information, we immediately began preparations to notify our guests and regulatory authorities. Recognizing that speed was of the essence, in the days that followed we worked to make sure that we could provide concrete and useful information to our guests. These efforts are described below. While these preparations were ongoing, we also began notifying regulatory authorities.

On November 25 and 26, we found that, in 2015 and 2016, prior to our acquisition of Starwood, the attacker had likely created a copy of two other tables, which the attacker later deleted. The file names correspond to two other tables in the Starwood Guest Reservation Database. We have been unable to recover those files and could not determine if they had been taken.

On November 29, 2018, we gave an update to the FBI and notified the four major payment card networks and their credit card processing vendors. We provided notice to regulators in over

twenty foreign countries and territories, as well as to state Attorneys General, the Federal Trade Commission, the Securities and Exchange Commission, and the three credit reporting agencies.

II. The Scope of the Incident

Our first public announcement about the incident on November 30, 2018 estimated that approximately 500 million guest records were involved, even though we knew that the numbers would likely decrease as our investigation continued and we de-duplicated the records. We issued a follow-up press release on January 4, 2019, adjusting the number of affected records downward to 383 million guest records as a result of our further investigative efforts and certain de-duplication efforts. To be clear, this does not mean that information concerning 383 million unique guests was involved; in many instances, there appear to be multiple records for the same guest, but because of the nature of the data, further de-duplication cannot easily be performed. We cannot confidently determine whether records with similar names, or even identical names with different addresses, represent one person or multiple people, but we have concluded with a fair degree of certainty that information for fewer than 383 million unique guests was involved.

According to our most recent investigative findings, the incident involved approximately 18.5 million encrypted passport numbers and approximately 5.25 million unencrypted passport numbers (approximately 663,000 of which have been associated with the United States). With respect to payment cards, the incident involved approximately 9.1 million encrypted payment card numbers, of which approximately 385,000 were unexpired as of September 2018. Based on our current information, we believe that the information accessed by an unauthorized third party could include several thousand unencrypted payment card numbers. To date, we have not found evidence that the master encryption keys needed to decrypt encrypted payment card and passport numbers were accessed, but we cannot rule out that possibility. Certain data analytics and

investigative work continues, including by a Payment Card Industry Forensic Investigator engaged on behalf of the payment card networks.

III. Marriott Is Dedicated to Providing Support to Guests

We deeply regret that this incident occurred and are focused on responding to our guests' needs and questions. We have therefore created several resources for guests who are concerned that their information may have been involved in the incident.

A. Notification of Guests

While our forensic work was ongoing, Marriott worked to create guest communication documents and coordinate with external vendors to build the logistical infrastructure required to facilitate guest notifications. We wanted to be transparent with our guests and also to be ready on day one to handle inquiries from guests across the world.

On November 30, we provided public notice of the incident via a press release and notification banners across Marriott's websites and the Marriott and Starwood Preferred Guest apps. After the November 30 press release, we also began providing email notifications to various guests who had valid email addresses in the affected tables. We sent email notifications on a rolling basis, and our emails to U.S.-based guests were completed on December 11, 2018.

B. Dedicated Website for Guests

We have created a dedicated website to provide information and updates about the incident and to assist anyone who was potentially affected. The website provides details regarding the incident, the information involved, the steps being taken to investigate, and answers to frequently asked questions (FAQs). The website also has information about how guests can monitor and protect their data and details on both call centers and web monitoring services. The dedicated

website is available in several languages, such as English, Spanish, French, German, Italian, and Portuguese. It can be found at https://info.starwoodhotels.com.

C. Call Centers to Answer Guests' Questions

In order to answer guests' questions about the incident, we set up dedicated call centers available in a number of languages, most of which operate seven days per week. We focused on creating call centers that were well staffed so that guests would face minimal wait times. Through February 28, 2019, the average wait time in the United States and Canada is nine seconds. If our call center staff is not able to answer specific questions that a guest may have, there is an escalation process in place to ensure that further efforts are made to respond to inquiries.

Through February 28, 2019, the call centers had received approximately 53,000 calls in total. Significantly, the number of total calls and escalations has been trending steadily downwards, with the exception of a brief increase following the January 4, 2019 press release.

D. Web Monitoring to Help Guests

We are also offering two free monitoring solutions for potentially-affected guests. U.S., U.K., and Canadian guests can enroll in a service called WebWatcher, which monitors the sites where personal information may be shared and alerts guests if evidence of their personal data is found. In the United States, enrollment in WebWatcher provides two additional benefits: fraud loss reimbursement coverage and unlimited fraud consultation services for one year. Through February 28, 2019, approximately 250,750 U.S. guests had activated WebWatcher. In certain other countries, we have engaged Experian to provide its IdentityWorks Global Internet Surveillance product to guests. Through February 28, 2019, approximately 36,000 guests had enrolled in the Experian product.

E. Claims Processing

We have created a process that enables guests or other customers to ask what information about them, if any, was involved in this incident. That process, and an expedited process for ascertaining whether a particular passport number was included in the set of unencrypted passport numbers involved in the incident, can be accessed through a publicly-available link on the dedicated website referenced above. So far, approximately 17,700 requests have been received through this website by guests wanting to know more about whether their information was involved.

Additionally, we have established a process for guests to submit individual claims of fraud related to this incident. We review any claims made by a guest with individual attention, diligence, and care.

F. No Evidence of Fraudulent Use of Information

Thus far, we have not received any substantiated claims of loss from fraud attributable to the incident. Moreover, none of the security firms we engaged to monitor the dark web have found evidence that information contained in the affected tables has been or is being offered for sale. We have not been notified by any banks or card networks that Starwood has been identified as a common point of purchase in any fraudulent transactions, which typically identifies the merchant location where cardholder data was stolen or where a data security breach may have occurred. We will continue to be vigilant for fraudulent use of guest information or attempts by anyone to profit from the incident.

With respect to passport numbers, the State Department has stated that a United States passport number, by itself, cannot be used to travel internationally or procure a new passport.

IV. Marriott Is Improving Security and Privacy Protections Going Forward

As noted above, the Marriott and the Starwood networks have always been separate. This incident affected only the Starwood network. As we combined the Marriott and Starwood organizations after the merger closing, we undertook a review of our systems and set in motion a plan to enhance the security of our systems to address the ever-increasing sophistication of cyber-attackers. As of December 18, 2018, we are no longer using the Starwood Guest Reservation Database for business operations. In the time between the discovery of this incident and the retirement of the Starwood database, we took additional steps to secure the Starwood network, including malware removal, deployment of endpoint protection tools to approximately 70,000 devices that were originally on the Starwood network, rebuilding impacted hosts, and IP whitelisting to control access to the Starwood database.

I want to emphasize that our work here is not limited to payment card industry (PCI) compliance. We had already increased our investment in enhancing our information security prior to the incident, and the incident has caused us to accelerate those efforts and to further increase our investment and speed up planned enhancements. Beyond the steps taken to secure the Starwood network and the retirement of the Starwood Guest Reservation Database, we have accelerated our roll-out of endpoint protection tools to over 200,000 devices. Those tools allow real-time discovery of suspicious behavior on both the Starwood and Marriott networks and have next-generation anti-virus features. We are focused on identity access management, which means a broader deployment of two-factor authentication across our systems, as well as network segmentation, which means isolating the most valuable data so that it becomes more difficult for attackers to access the systems and for malware to spread through the environment.

We are working to identify ways that we can be an industry leader on these issues. We know that this is a race that has no finish line. Cyber-attacks are a pervasive threat. At Marriott, we are committed to taking care of our guests and to proactively finding ways to protect against, detect, and respond to these evolving cyber threats.

*****

I thank the Subcommittee again for the opportunity to testify today.