1923022

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

In the Matter of **MARRIOTT INTERNATIONAL, INC.,** **a corporation** **and** **STARWOOD HOTELS & RESORTS WORLDWIDE, LLC,** **a limited liability company.**	**DOCKET NO.**

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that Marriott International, Inc., a corporation, and Starwood Hotels & Resorts Worldwide, LLC, a limited liability company (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act, 15 U.S.C. § 45, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Marriott International, Inc. ("Marriott") is a Delaware corporation with its principal office or place of business at 7750 Wisconsin Ave., Bethesda, Maryland 20814.

2. Respondent Starwood Hotels & Resorts Worldwide, LLC ("Starwood") is a Maryland limited liability company with its principal office or place of business at 7750 Wisconsin Ave., Bethesda, Maryland 20814. Starwood is a wholly-owned subsidiary of Marriott.

3. On or about September 23, 2016, acting alone or in concert with Starwood, Marriott formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint.

4. The acts or practices of Respondents, as alleged in this Complaint, have been in or

affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act and constitute unfair and/or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

Relevant Business Practices

5. Marriott is a multinational hospitality company that manages and franchises hotels and related lodging facilities, including 30 brands and more than 7,000 properties throughout the United States and across 131 countries and territories.

6. On or about November 16, 2015, Marriott announced that it would acquire Starwood for $12.2 billion. Marriott's acquisition of Starwood closed the following year, on or about September 23, 2016, and Starwood became a wholly-owned subsidiary of Marriott. With the acquisition of Starwood, Marriott became the largest hotel chain in the world at that time with over 1.1 million hotel rooms, accounting for one out of every fifteen hotel rooms worldwide.

7. After the legal close of Marriott's acquisition of Starwood, Marriott took control of Starwood's computer network and has been responsible for establishing, reviewing, and implementing the information security practices for both itself and Starwood. Additionally, following the legal close of the acquisition, Marriott commenced a two-year process to integrate some Starwood systems into the Marriott network. Marriott fully integrated those Starwood systems into its own network by December 2018.

First Breach (Starwood)

8. Approximately four days after Marriott's announcement of the Starwood acquisition, on or about November 20, 2015, Starwood notified consumers that it had experienced a 14-month long data breach of its computer network, involving payment card information, including name, payment card number, security code, and expiration date, for over 40,000 consumers (hereinafter, the "First Breach").

9. Specifically, beginning in June 2014 and continuing for 14 months, a malicious actor had exploited security vulnerabilities to gain remote access to Starwood's computer network. Once inside Starwood's computer network, the malicious actor further compromised unprotected administrative accounts and credentials to install malware at more than one hundred Starwood-owned or managed hotel properties. This malware allowed the malicious actors to gain access to consumers' payment card information, including full name, payment card number, expiration date, and security code. The forensic examination conducted by Starwood following the intrusion found that, among other things, inadequate firewalls and network segmentation, inadequate access controls, the use of outdated and unsupported software, and the lack of multifactor authentication contributed to the First Breach.

10. During the 10 months between the announcement of Marriott's acquisition of Starwood and its closing, Marriott reviewed and evaluated Starwood's information security program to understand the state of Starwood's computer networks, systems, and their vulnerabilities, including the information security failures that led to the First Breach.

Second Breach (Starwood)

11. Despite having responsibility for Starwood's information security practices and network following the acquisition, Marriott failed to identify an ongoing breach within the Starwood network (hereinafter, the "Second Breach"). In fact, Marriott did not detect the Second Breach until September 7, 2018, nearly two years after the legal close of Marriott's acquisition of Starwood.

12. Forensic examiners determined that, on or about July 28, 2014, malicious actors compromised Starwood's external-facing webserver, installing malware on its network. This malware allowed the intruders to perform network reconnaissance activities, harvest highly privileged Starwood administrative and user credentials, and use those credentials to move throughout the Starwood's internal network for a four-year period, when Marriott's system finally detected an attempt to export consumer data from the guest reservation database on September 7, 2018.

13. Even after discovery of the breach, on September 10, 2018, the intruders exported additional guest information from Starwood's systems.

14. During this over four-year period, from July 2014 to September 2018—including the two years following Marriott's acquisition of Starwood and its integration of certain Starwood systems—the intruders went undetected, installing key loggers, memory-scraping malware, and Remote Access Trojans in over 480 systems across 58 locations within the Starwood environment. Those locations included a combination of corporate, data center, customer contact center, and hotel property locations.

15. Following the Second Breach, Respondents' forensic examiner assessed Starwood's systems and identified similar failures that resulted in the First Breach, including inadequate firewall controls, unencrypted payment card information stored outside of the secure cardholder data environment, lack of multifactor authentication, and inadequate monitoring and logging practices.

16. Due to the Second Breach, the personal information of 339 million consumer records globally was compromised, including more than 5.25 million unencrypted passport numbers. Additional compromised information included names, gender, dates of birth, payment card numbers, addresses, email addresses, telephone numbers, usernames, Starwood loyalty numbers, partner loyalty program numbers, and hotel stays and other travel information, such as location of hotel stays, duration of stays, number of children and guests, and flight information.

Third Breach (Marriott)

17. The information security failures detailed in this Complaint are not limited to Starwood's computer networks, systems, and databases, nor are they limited to the First and Second Breaches that began during Starwood's control and operation of its information security program.

18. Marriott announced in March 2020 that malicious actors had compromised the credentials of employees at a Marriott-franchised property to gain access to Marriott's own network (hereinafter, the "Third Breach").

19. The intruders began accessing and exporting consumers' personal information without detection from September 2018—the same month that Marriott became aware of the Second Breach—to December 2018 and resumed in January 2020 and continued until they were ultimately discovered in February 2020.

20. The intruders were able to access more than 5.2 million guest records, including 1.8 million records related to U.S. consumers, that contained significant amounts of personal information, including names, mailing addresses, email addresses, phone numbers, affiliated companies, gender, month and day of birth, Marriott loyalty account information, partner loyalty program numbers, and hotel stay and room preferences.

21. Marriott's internal investigation confirmed that the malicious actors' main purpose for searching, accessing, and exporting guest records was to identify loyalty accounts with sufficient loyalty points to be either used or redeemed, including for booking stays at hotel properties.

Respondents' Deceptive Information Security Statements

22. Prior to its acquisition, Starwood controlled and operated its website, www.starwood.com, where consumers could make reservations for hotel rooms.

23. Following the acquisition, Marriott controlled and continued to operate the Starwood website until approximately May 2018 when Marriott merged Starwood's website into the Marriott website.

24. At all relevant times, the privacy policy posted on the Starwood website stated:

> **SECURITY SAFEGUARDS:** Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your personal data against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although "guaranteed security" does not exist either on or off the Internet, ***we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, "firewalls"*** and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit. (emphasis added).

25. In addition to the Starwood website, Marriott operates its own Marriott-branded website, www.marriott.com, where consumers can make reservations for Marriott-branded

hotels, as well as Starwood-branded hotels.

26. At all relevant times, the privacy policy posted on the Marriott website stated:

> ***We seek to use reasonable organizational, technical and administrative measures to protect Personal Data.*** Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section, below. (emphasis added).

Respondents' Information Security Practices

27. Respondents failed to provide reasonable or appropriate security for the personal information that they collected and maintained about consumers. Among other things, Respondents:

a. Failed to implement appropriate password controls. As a result of this failure, employees often used default, blank, or weak passwords;

b. Failed to patch outdated software and systems in a timely manner, leaving Starwood's network susceptible to attacks. Indeed, the forensic examiner for the First Breach noted that the Starwood cardholder data environment included unsupported operating systems for which patches were no longer available;

c. Failed to adequately monitor and log network environments, limiting the ability to detect malicious actors and distinguish between authorized and unauthorized activity. This failure prevented Respondents from detecting intruders in their networks—for several years during the Second Breach—and further prevented them from determining the information exfiltrated from their networks;

d. Failed to implement appropriate access controls. For example, on numerous occasions, the accounts of former employees were not terminated in a timely manner, and separate unique accounts for users' remote access on Respondents' networks were not created;

e. Failed to implement appropriate firewall controls. This failure resulted in malicious actors making unauthorized connections from outside of Respondents' networks;

f. Failed to implement appropriate network segmentation, which allowed intruders to move easily between Starwood hotel property systems and Starwood's corporate network during multiple breaches; and

g. Failed to apply adequate multifactor authentication to protect sensitive information. For example, Starwood failed to comply with contractual obligations and internal policies requiring multifactor authentication for remote access to sensitive environments, including environments containing payment card data.

Consumer Injury

28. As a direct result of the failures described in Paragraph 27 above, between 2014 and 2020, malicious actors were able to gain unauthorized access to Respondents' networks in at least three separate breaches as described above. In the First Breach and Second Breach, the malicious actors used similar techniques, such as exploiting unpatched security vulnerabilities, remote access failures, and gaps in network segmentation, to gain access to the personal information of millions of consumers, including passport information, payment card numbers, Starwood loyalty numbers, name, gender, date of birth, address, email address, telephone number, username, and hotel stay and other travel information. Such prolonged exposure of the highly detailed and individualized personal information in the records contained on Starwood's network has caused or is likely to cause substantial injury to consumers.

29. For example, in the Third Breach, the theft of loyalty account numbers enabled malicious actors to fraudulently make purchases by redeeming loyalty points. In addition, identity thieves are likely to use loyalty account information to gain access to consumers' loyalty accounts and modify login information so that they can redeem points in the future or transfer the loyalty points to another loyalty account controlled by the identity thief. Compared to payment cards, loyalty accounts are more susceptible to fraud due to the value of the loyalty account points, the static nature of account numbers, and the lack of routine monitoring by consumers. As a result, likely because obtaining access to loyalty accounts and redeeming loyalty points is easier than obtaining and using stolen payment card numbers, malicious actors are known to pay more for loyalty account information on the dark web than payment card information. And, in contrast to payment cards, consumers do not have the same legally protected recovery rights when identity thieves fraudulently redeem loyalty points.

30. Similarly, the exposure of more than 5.25 million unencrypted passport numbers in the Second Breach, when combined with the other types of personal information contained in the exposed 339 million records, has caused or is likely to cause substantial injury to consumers. Malicious actors can combine stolen passport information, along with other personally identifying information in the records of Starwood, to create highly successful, targeted phishing campaigns to commit identity theft or other types of financial fraud. Such information is highly valuable on the open market, and wrongdoers frequently seek to purchase passport numbers on the dark web.

31. Consumers have also suffered, and will continue to suffer, additional injuries due to the significant amount of highly detailed and individualized personal information exposed. These injuries include wasted time and money to obtain identity theft protection services, detect

and monitor financial and loyalty accounts for identity theft, replace passports, and cancel and replace compromised payment cards.

32. These harms were not reasonably avoidable by consumers, as consumers had no way to know about Respondents' information security failures described in Paragraph 27 above.

VIOLATIONS OF THE FTC ACT

Count I – Respondents' Deceptive Security Statements

33. Through the means described in Paragraphs 24 and 26, Respondents have represented, directly or indirectly, expressly or by implication, that they used appropriate safeguards to protect consumers' personal information.

34. In truth and in fact, as described in Paragraph 27, Respondents did not use appropriate safeguards to protect consumers' personal information. Therefore, the representations set forth in Paragraphs 24 and 26 is false or misleading.

Count II – Respondents' Unfair Information Security Practices

35. As alleged in Paragraphs 27 to 32, Respondents' failure to employ reasonable security measures to protect consumers' personal information caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice was, and is, an unfair act or practice.

Violation of Section 5

36. The acts and practices of Respondents, as alleged in this Complaint, constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this ____day of _____, 2024, has issued this complaint against Respondents.

By the Commission, Commissioner Holyoak recused.

April J. Tabor
Secretary

SEAL: