

RECEIVED

OCT - 9 2024

Davidson County Chancery Court

COPY

IN THE CHANCERY COURT OF TENNESSEE
20th JUDICIAL DISTRICT, DAVIDSON COUNTY, NASHVILLE

STATE OF TENNESSEE
ex rel. JONATHAN SKRMETTI
Attorney General and Reporter,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC., a
corporation,

Defendant.

Case No. 24-1185-II

AGREED FINAL JUDGMENT

Plaintiff, the State of Tennessee, Office of the Attorney General and Reporter, as described in Paragraph 1 below (“Plaintiff”), and Defendant Marriott International, Inc., a corporation, appearing through its attorney, TaCara Harris of King & Spalding LLP, having stipulated to the entry of this Agreed Final Judgment (“Judgment”) by the Court without the taking of proof and without trial or adjudication of any fact or law, without this Judgment constituting evidence of or an admission by the Defendant, regarding any issue of law or fact alleged in the Complaint on file, and without the Defendant admitting any liability, and with all parties having waived their right to appeal, and the Court having considered the matter and good cause appearing:

IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

I. PARTIES AND JURISDICTION

1. The Plaintiff in this case is State of Tennessee, Office of the Attorney General and Reporter .

2. The Defendant in this case is Marriott International, Inc., a corporation incorporated under the law of the State of Delaware with its principal office located at 7750 Wisconsin Ave., Bethesda, Maryland 20814. “Marriott” shall mean Marriott International, Inc. and its U.S. subsidiaries and successors that collect, store, or process PERSONAL INFORMATION provided, however, for the avoidance of doubt, “Marriott” shall not include any MARRIOTT FRANCHISED HOTEL. “Starwood” shall mean Starwood Hotels & Resorts Worldwide, LLC, its subsidiaries and successors that collect, store, or process PERSONAL INFORMATION. “Marriott” shall include “Starwood” unless specifically stated otherwise.¹

3. Marriott agrees that the Court has jurisdiction over the subject matter of this action and jurisdiction over the parties to this action, and venue is proper in this Court solely for the purpose of entry as well as any subsequent modification or enforcement of this Judgment.

4. Marriott agrees that for the limited purpose of entry of this Judgment, at all relevant times, it has transacted business in the State of Tennessee, including, but not limited to, Davidson County.

¹ Prior to November 15, 2015, Starwood was a separate corporation with its principal office located at One Starpoint, Stamford, CT 06902.

5. The injunctive terms and other relief contained in this Judgment are being ordered pursuant to and subject to the CONSUMER PROTECTION LAW, DATA BREACH NOTIFICATION LAW, and PERSONAL INFORMATION PROTECTION LAW.

II. DEFINITIONS

6. “COMPENSATING CONTROL” or “COMPENSATING CONTROLS” shall mean one or more alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the Chief Information Security Officer (or his or her appropriate designee) to be impractical to implement at the present time due to legitimate technical or business constraints. Such alternative mechanisms must (a) meet the intent and rigor of the original stated requirement; (b) provide a similar level of security as the original stated requirement; (c) be up to date with current industry-accepted security protocols; and (d) be commensurate with the additional risk imposed by not adhering to the original stated requirement.

7. “CONSUMER” or “CONSUMERS” shall mean one or more natural persons who reside in or are a resident of the United States and who either (a) purchases or has purchased goods or services from Marriott or any MARRIOTT FRANCHISED HOTEL or (b) provides or has provided PERSONAL INFORMATION to Marriott in relation to the potential purchase or use of goods or services from Marriott or any MARRIOTT FRANCHISED HOTEL.

8. “CONSUMER PROTECTION LAW” shall mean the Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. § 47-18-101, et seq.

9. “CORPORATE LEVEL” shall mean MARRIOTT ASSETS in Marriott’s corporate network segment and other non-property network segments.

10. “COVERED CONDUCT” shall mean Marriott’s conduct related to the STARWOOD DATA BREACH and the UNAUTHORIZED ACCOUNT ACCESS INCIDENTS, including alleged failures to (a) protect PERSONAL INFORMATION; (b) maintain reasonable information technology safeguards or controls; (c) remediate deficient controls; (d) maintain adequate controls; and (e) determine risk. “COVERED CONDUCT” shall also include any alleged misrepresentations by Marriott as to the collection, maintenance, use, deletion, disclosure, security, privacy, availability, confidentiality, or integrity of PERSONAL INFORMATION related to the STARWOOD DATA BREACH and the UNAUTHORIZED ACCOUNT ACCESS INCIDENTS.

11. “COVERED DATABASES” shall mean the central reservation and loyalty databases that Marriott uses to operate guest reservation or loyalty program transactions that includes two or more of the following data elements: (a) reservation details; (b) hotel stay preferences; (c) LOYALTY REWARDS PROGRAM number; or (d) LOYALTY REWARDS PROGRAM points balance. As of the EFFECTIVE DATE, “COVERED DATABASES” shall mean Marriott’s Automated Reservation System for Hotel Accommodations (“MARSHA”) and Loyalty/Universal Guest Identification (“UGI”) systems. “COVERED DATABASES” shall include any equivalent successor databases.

12. “CRITICAL IT VENDOR” shall mean a third party that provides managed services that are a significant component of the Information Security Program

and has direct access to: (a) MARRIOTT ASSETS or (b) COVERED DATABASES, including those outsourced to a cloud computing service provider.

13. “DATA BREACH NOTIFICATION LAW” shall mean the Tennessee Identify Theft Deterrence Act of 1999, Tenn. Code Ann. § 47-18-2101, et seq.

14. “EFFECTIVE DATE” shall be November 8, 2024. All requirements contained in this Judgment shall be enforceable and in effect as of the EFFECTIVE DATE unless otherwise stated.

15. “ENCRYPT” or “ENCRYPTION” shall mean encoding data into ciphertext—at rest or in transit—rendering it unusable, unreadable, or indecipherable without converting the ciphertext to plaintext through the use of a confidential process and key leveraging a security technology, methodology, or encryption algorithm generally accepted in the field of information security, commensurate with the sensitivity of the data at issue.

16. “FULL IMPLEMENTATION DATE” shall mean the earlier of (a) one (1) year from the EFFECTIVE DATE or (b) certification by Marriott pursuant to Paragraph 80.

17. “FTC ORDER” shall mean the order entered to resolve Federal Trade Commission Decision and Order relating to File No. 1923022: *In the Matter of Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC*.

18. “LOYALTY REWARDS PROGRAM” shall mean the Marriott Bonvoy program (or such name as it may be known in the future) offered by Marriott that allows

CONSUMERS to earn and redeem points for certain goods or services according to and subject to the terms of such program. The term “LOYALTY REWARDS PROGRAM” shall not be construed as creating any property rights for enrolled CONSUMERS.

19. “MARRIOTT ASSETS” shall mean all electronic systems used to carry out business (including networking equipment, databases or data stores, applications, servers, devices, endpoints, and other systems) that: (a) are capable of using and sharing software, data, and hardware resources; (b) are owned or operated directly by Marriott; and (c) collect, maintain, process, store, or transmit PERSONAL INFORMATION. For the avoidance of doubt, electronic systems are not Marriott Assets if they are physically located outside of the United States, unless they support the operation of a property located in the United States that is owned or operated under a Marriott brand.

20. “MARRIOTT FRANCHISED HOTEL” shall mean any hotel that is owned by a third party and operated under a Marriott brand by a third party pursuant to a license or franchise agreement with Marriott.

21. “PERSONAL INFORMATION” shall mean the following data elements from or about an individual CONSUMER:

a. First name or first initial and last name in combination with one or more of the following data elements that relate to such CONSUMER: (i) Social Security number; (ii) state or federal issued identification number, including driver’s license number, passport number, or military identification number; (iii) financial account number or credit or debit card number in combination with any

required security code, access code, or password that would permit access to the CONSUMER's financial account; or

b. A username or e-mail address in combination with a password or security question and answer that would permit access to an individual's online account; or

c. Any other "Personal Information" as defined by the DATA BREACH NOTIFICATION LAWS as of the EFFECTIVE DATE.

d. Notwithstanding (c) above, a first name or first initial, and last name, in combination with an e-mail address alone shall not constitute PERSONAL INFORMATION.

22. "PERSONAL INFORMATION PROTECTION LAW" shall mean the Tennessee Information Protection Act, Tenn. Code Ann. § 3301, et seq.

23. "REPORTABLE INCIDENT" means a SECURITY EVENT that triggers a notification obligation under a DATA BREACH NOTIFICATION LAW.

24. "SECURITY EVENT" shall mean any compromise to the confidentiality, integrity, or availability of (a) PERSONAL INFORMATION held on or accessed through any of the MARRIOTT ASSETS or (b) any of the COVERED DATABASES, or any event that gives rise to a reasonable likelihood of such compromise.

25. "STARWOOD DATA BREACH" shall refer to the incident announced by Marriott on November 30, 2018 in which a person or persons gained unauthorized access

to Starwood's reservation database and subsequently exported data from certain tables, involving approximately one-hundred thirty-one million five-hundred thousand (131,500,000) guest records pertaining to customers associated with the United States, some of which included contact information, gender, dates of birth, payment card information, passport numbers, legacy Starwood Preferred Guest information, reservation information, and hotel stay preferences.

26. "UNAUTHORIZED ACCOUNT ACCESS INCIDENTS" shall refer to the incident(s) announced by Marriott on March 31, 2020 and in June 2020 in which a person or persons used the login credentials of certain Marriott franchise property employees to inappropriately access information regarding approximately five million five-hundred thousand (5,500,000) guest records, some of which included contact information, gender, dates of birth, loyalty account information, and hotel stay preferences.

III. INJUNCTIVE RELIEF

27. The duties, responsibilities, burdens, and obligations undertaken in connection with this Judgment shall apply to Marriott.

28. The terms contained in this Judgment are being entered pursuant to injunctive relief permitted by the CONSUMER PROTECTION LAW, the DATA BREACH NOTIFICATION LAW, and/or the PERSONAL INFORMATION PROTECTION LAW.

COMPLIANCE WITH LAW

29. Marriott shall not misrepresent or omit information in violation of the CONSUMER PROTECTION LAW regarding either (a) how Marriott collects, maintains, uses, deletes, or discloses PERSONAL INFORMATION or (b) the manner or extent to which Marriott protects the privacy, security, availability, confidentiality, or integrity of PERSONAL INFORMATION.

30. Marriott shall comply with the DATA BREACH NOTIFICATION LAW and the PERSONAL INFORMATION PROTECTION LAW.

INFORMATION GOVERNANCE

31. **Board Committee:** Marriott shall maintain a committee of the Board of Directors² (“Board Committee”) that shall assist the Board in providing oversight of Marriott’s information security program (“Information Security Program”). The Board Committee shall meet not less than four (4) times per year.

32. On or before December 31, 2024, and annually thereafter, the Board Committee shall acknowledge in its minutes that it has received the materials and presentations required by this Judgment and the minutes shall include a list or description of such materials and presentations.

33. **Chief Information Security Officer:** Marriott shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program (hereinafter referred to as the “Chief Information Security

² As of March 15, 2021, Marriott included such a committee in its charter, entitled the Technology and Information Security Oversight Committee.

Officer”). The Chief Information Security Officer shall have the education, qualifications, and experience appropriate to the level, size, and complexity of the role in implementing, maintaining, and monitoring the Information Security Program. This Chief Information Security Officer (or his or her appropriate designee) shall:

- a. Report to the Board Committee on Marriott’s risk assessment(s) and Information Security Program;
- b. Report to the Board of Directors regarding Marriott’s Information Security Program;
- c. Report to the Chief Executive Officer within forty-eight (48) hours of determining that a SECURITY EVENT both (i) involves the PERSONAL INFORMATION on MARRIOTT ASSETS of one thousand (1,000) or more CONSUMERS and (ii) there is reasonable likelihood that the PERSONAL INFORMATION has been accessed or acquired by an unauthorized third party. In the event that the Chief Executive Officer is not a member of the Board of Directors, any reports made pursuant to this subparagraph shall also be reported to a designated member of the Board Committee by the Chief Information Security Officer unless otherwise reported to the Board Committee or the Board of Directors by the General Counsel; and
- d. Inform the Board Committee at its regularly scheduled meeting time of all REPORTABLE INCIDENTS.

34. **Necessary Resources and Support:** Marriott shall ensure that the Information Security Program receives the resources and support reasonably necessary for the Information Security Program to be implemented and function as required by this Judgment.

35. **Training:** On at least an annual basis Marriott shall provide training on how to safeguard PERSONAL INFORMATION and data in the COVERED DATABASES to Marriott employees who have access to (i) PERSONAL INFORMATION on any of the MARRIOTT ASSETS or (ii) any of the COVERED DATABASES. The training shall be based on Marriott's determination of the highest risks to PERSONAL INFORMATION or data in any of the COVERED DATABASES typically experienced by the employee's role and function.

36. **Training – Information Security Personnel:** In addition to training required in Paragraph 35 above, Marriott shall provide and continue to provide training to employees who are responsible for implementing, maintaining, or monitoring the Information Security Program ("InfoSec Personnel") on how to safeguard and protect PERSONAL INFORMATION and COVERED DATABASES. Marriott shall provide the training required under this Paragraph: (a) to all current InfoSec Personnel within one-hundred eighty (180) days of the EFFECTIVE DATE, except for those InfoSec Personnel who already received such training within the prior twelve (12) months of the EFFECTIVE DATE, and (b) for any employee hired as, or transitioned into, an InfoSec Personnel role after the EFFECTIVE DATE such training shall be within ninety (90) days of hire or transition.

INFORMATION SECURITY PROGRAM

INFORMATION SECURITY PROGRAM: GENERAL

37. **Information Security Program:** Marriott shall develop, implement, and maintain through appropriate review and revision cycles, a written comprehensive Information Security Program, and Marriott shall continue to implement and maintain reasonable safeguards and controls to reduce security risks.

38. For a period of twenty (20) years from the EFFECTIVE DATE, the Information Security Program required by this Judgment shall include the specific requirements of Paragraphs 40 through 78 in this Judgment in accordance with Marriott's analysis of risk as set forth in Paragraph 46 of this Judgment provided, however, that the following provisions shall expire at a period of ten (10) years from the FULL IMPLEMENTATION DATE: Paragraphs 55, 56, 61, 62, 68, 69, 74, and 75.

39. Marriott's Information Security Program shall be documented and shall contain administrative, technical, and physical safeguards appropriate to:

- a. The size and complexity of Marriott's operations;
- b. The nature and scope of Marriott's activities; and
- c. The volume and sensitivity of (i) the PERSONAL INFORMATION collected, maintained, processed, stored, or transmitted by MARRIOTT ASSETS or (ii) data stored or maintained in the COVERED DATABASES.

40. Marriott shall enforce the policies and procedures required by this Judgment. Marriott shall monitor for non-compliance and undertake remedial measures for non-compliance as appropriate and without unreasonable delay.

41. **Incident Response Plan:** Marriott's Information Security Program shall include a written incident response plan. Where appropriate, Marriott shall revise and update this response plan to adapt to any changes to MARRIOTT ASSETS or the COVERED DATABASES. The plan shall conform to a nationally recognized standard and may be updated or revised.

42. Marriott shall conduct, at a minimum, incident response plan exercises ("table-top exercises") once per year.

INFORMATION SECURITY PROGRAM: RISK ASSESSMENT AND ANALYSIS

43. **Risk Assessment:** Marriott shall conduct an annual risk assessment (hereinafter, "Risk Assessment") which includes:

a. The identification of internal and external risks to the security, confidentiality, or integrity of PERSONAL INFORMATION on MARRIOTT ASSETS or the COVERED DATABASES that could result in the unauthorized disclosure, misuse, loss, or other compromise of such PERSONAL INFORMATION or data in any of the COVERED DATABASES;

b. An assessment of safeguards in place to control these risks;

- c. The evaluation and adjustment of the Information Security Program in light of the results of such testing and monitoring;
- d. The implementation of reasonable safeguards to control these risks; and
- e. Documentation of safeguards implemented in response to such annual Risk Assessments.

44. **Risk Assessment – Special:** Marriott shall include in any Risk Assessment performed pursuant to Paragraph 43 above appropriate additional risk analysis in relation to (a) MARRIOTT FRANCHISED HOTELS and (b) CRITICAL IT VENDORS.

45. **Risk Assessment Method:** Marriott shall develop a risk assessment method by utilizing method(s) published by a nationally recognized security body and shall include the risk assessment criterion of “harm to others” as a component of the magnitude of impact analysis as well as the likelihood of that impact (“Risk Assessment Method”). Marriott shall document the Risk Assessment Method including (i) the selection of method(s), (ii) criteria, and (iii) what Marriott has established as the acceptable risk threshold(s). Marriott, as it deems appropriate, may modify the Risk Assessment Method, but shall document the change and the rationale for the change.

46. **Risk Analysis – Applicability:** When analyzing risk to determine implementation, maintenance, and compliance with the specific requirements of the Information Security Program at Paragraphs 37 through 78 and Integration at Paragraphs

81 through 85, which incorporate the Definitions as set forth in Paragraphs 6 through 26 of this Judgment, Marriott shall perform such analysis consistent with a risk-based analysis performed in accordance with the applicable Risk Assessment Method selected at Paragraph 45.

47. **Risk Analysis – Compensating Controls:** Prior to approving a COMPENSATING CONTROL, Marriott shall perform a risk analysis to PERSONAL INFORMATION or data stored or maintained in the COVERED DATABASES consistent with the Risk Assessment Method. Such risk analysis shall be documented and indicate the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable, and that the Chief Information Security Officer (or his or her appropriate designee) agrees with both the risk analysis and the determination that the risk is acceptable.

48. **Additional Risk Analysis – Software, Hardware, and Systems:** Prior to approving any new software, hardware, or systems for use as MARRIOTT ASSETS, Marriott shall perform an analysis of risk to PERSONAL INFORMATION or data in any of the COVERED DATABASES.

INFORMATION SECURITY PROGRAM: VENDOR OVERSIGHT

49. **Vendor Management:** Marriott shall develop, implement, and maintain written, risk-based policies and procedures for overseeing a Marriott vendor that has access to (i) MARRIOTT ASSETS, (ii) PERSONAL INFORMATION provided by or obtained by the vendor on behalf of Marriott, or used at the direction of Marriott for the benefit of Marriott, or (iii) COVERED DATABASES (“relevant vendor”). These policies

and procedures shall include a process for including in contracts with a relevant vendor executed or amended after the EFFECTIVE DATE: (a) requirements appropriate to the service provided by the relevant vendor to implement and maintain security safeguards; (b) periodic evaluations of the relevant vendor's cybersecurity practices; (c) a requirement that a relevant vendor notifies Marriott promptly after discovering a SECURITY EVENT or REPORTABLE INCIDENT; and (d) a requirement that a relevant vendor notifies Marriott of a compromise of the relevant vendor's systems that compromise MARRIOTT ASSETS or COVERED DATABASES.

50. **Vendor Management – Critical IT Vendors:** In addition to the requirements for relevant vendors at Paragraph 49 above, Marriott shall develop, implement, and maintain enhanced controls for CRITICAL IT VENDORS. Said controls shall include, but are not limited to:

a. Contractual requirements that obligate CRITICAL IT VENDORS to monitor the security safeguards and procedures of their own third-party vendors whose actions or inactions may impact MARRIOTT ASSETS or COVERED DATABASES;

b. Monitoring performance of the CRITICAL IT VENDOR's assigned duties and compliance with the CRITICAL IT VENDOR's contract with Marriott. The frequency and type of monitoring shall be appropriate based on feasibility and the CRITICAL IT VENDOR's responsibilities and access;

c. Permitting access to, or collection, retention, transmission, use and storage of PERSONAL INFORMATION or any of the COVERED DATABASES

by the CRITICAL IT VENDOR only to provide the contractually agreed upon services; and

d. Logging and monitoring for all points of the CRITICAL IT VENDOR's connection to MARRIOTT ASSETS or COVERED DATABASES.

51. For any CRITICAL IT VENDOR with which Marriott has shared security responsibilities, the CRITICAL IT VENDOR's security responsibilities shall be clearly delineated in writing.

INFORMATION SECURITY PROGRAM: MARRIOTT FRANCHISED HOTELS

52. Marriott shall develop, implement, and maintain written policies and procedures that require MARRIOTT FRANCHISED HOTELS to implement and maintain appropriate safeguards to protect PERSONAL INFORMATION. Such requirements shall include that MARRIOTT FRANCHISED HOTELS notify Marriott (a) within twenty-four (24) hours of any compromise to the systems of the MARRIOTT FRANCHISED HOTEL that compromises MARRIOTT ASSETS or (b) within five (5) business days of the termination of any MARRIOTT FRANCHISED HOTEL employee or contractor who has access to MARRIOTT ASSETS.

53. Marriott also shall develop and implement an audit program with an industry-appropriate sample to review compliance of MARRIOTT FRANCHISED HOTELS with the obligations outlined in Paragraph 52 of this Judgment. Such industry-appropriate sample shall be designed to consider the sizes, geographical locations, and Marriott brands of MARRIOTT FRANCHISED HOTELS.

INFORMATION SECURITY PROGRAM: CHANGE CONTROL

54. **Change Control:** Marriott shall develop, implement, and maintain policies and procedures to manage and document changes that impact PERSONAL INFORMATION at the CORPORATE LEVEL in production environments. Marriott shall also develop, implement, and maintain policies and procedures to manage and document changes to COVERED DATABASES.

INFORMATION SECURITY PROGRAM: OTHER

55. **PCI Compliance:** Marriott shall validate compliance with the applicable version of the Payment Card Industry Data Security Standard (“PCI DSS”) according to the requirements of the applicable acquiring bank relationship and payment card network requirements.

56. **Zero Trust:** The principles of zero trust should be considered and, where reasonably feasible, utilized in the design of the Information Security Program. Such principles include, but are not limited to, continuous verification, minimizing the impact of any breach, and incorporating behavioral and contextual data into the Information Security Program.

INFORMATION SECURITY PROGRAM:

PERSONAL INFORMATION SAFEGUARDS AND CONTROLS

GENERAL

57. **Minimum Extent Necessary:** The Information Security Program shall include or incorporate written policies and procedures that are modified as appropriate to

require reasonable efforts to collect, use, share, and retain PERSONAL INFORMATION to the minimum extent necessary to satisfy legitimate business need or legal requirements.

58. **Secure Disposal:** Marriott shall develop, implement, and maintain policies and procedures governing its retention and secure disposal of PERSONAL INFORMATION.

59. **Retention Period:** Marriott shall develop, implement, and maintain a policy to retain PERSONAL INFORMATION or CONSUMER information in COVERED DATABASES for only as long as is reasonably necessary to fulfill the purpose for which the PERSONAL INFORMATION or CONSUMER information in COVERED DATABASES was collected unless a longer time period is required to satisfy a documented accounting, tax, or legal obligation. Marriott's policy may provide that PERSONAL INFORMATION need not be destroyed and may be retained for a documented legitimate business need except for marketing.

INFORMATION SECURITY PROGRAM: SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS

60. **Access Controls and Account Management - General:** Marriott shall develop, implement, and maintain risk-based access controls, where access is to MARRIOTT ASSETS or to COVERED DATABASES. Such controls will be role-based, including for individual accounts, administrator accounts, service accounts, or vendor accounts.

61. **Access Controls and Account Management – Specific:** For the access controls and account management required by Paragraph 60 above:

a. Marriott shall require multi-factor authentication or equivalent enhanced authentication measures for remote access to MARRIOTT ASSETS or COVERED DATABASES.

b. In the event passwords are used in conjunction with any other access control, Marriott shall implement and maintain a policy requiring appropriate password complexity and change intervals.

c. Marriott shall implement enhanced measures for administrator-level passwords, such as ENCRYPTION, using a password vault, privileged access management solution, or measures of similar efficacy.

d. Marriott shall have policies and procedures that require Marriott to remove access privileges of a Marriott employee as soon as practicable and within two (2) business days following that employee's last day of employment.

e. Marriott shall have policies and procedures that require Marriott, upon receiving a notice of termination of a non-Marriott employee who is no longer employed by a MARRIOTT FRANCHISED HOTEL or performing services for Marriott, to remove access privileges as soon as practicable and within two (2) business days of the later of (i) notice to Marriott or (ii) last day of employment.

f. Marriott shall use the principle of least privilege to limit employee access to PERSONAL INFORMATION on MARRIOTT ASSETS or to COVERED DATABASES to the minimum required to perform job-related responsibilities and business functions.

g. Marriott shall periodically inventory the users who have access to MARRIOTT ASSETS or to COVERED DATABASES to determine whether such access remains necessary or that the level of access is appropriate.

h. Marriott shall annually review a sampling of user accounts to ensure access privileges have been appropriately terminated or that the level of access is appropriate. In the event that such a sample demonstrates non-compliance with Marriott's policies and procedures, Marriott shall undertake remedial measures.

62. **Encryption:** Marriott shall ENCRYPT PERSONAL INFORMATION or otherwise employ COMPENSATING CONTROLS to protect PERSONAL INFORMATION from unauthorized access where the information is externally transmitted electronically from MARRIOTT ASSETS or is stored on MARRIOTT ASSETS. When Marriott uses ENCRYPTION, it shall meet or exceed encryption key management requirements and changes in accordance with an industry-recognized standard.

63. **Threat Management:** Marriott shall develop, implement, and maintain a threat management program that shall include the use of automated tools to continuously monitor MARRIOTT ASSETS and COVERED DATABASES for active threats. Marriott

shall use reasonable measures to develop the initial configuration of these tools, monitor for updates, and make configuration changes and updates. Marriott shall use information from these tools to support its security updates and patch management program and in conjunction with its incident response plan to address threats that pose an unreasonable risk to MARRIOTT ASSETS or COVERED DATABASES.

64. **Logging and Monitoring:** Marriott shall develop, implement, and maintain policies and procedures for logging and monitoring MARRIOTT ASSETS and COVERED DATABASES. Such policies and procedures shall include appropriate applications and services, such as a Security Information and Event Management solution and third-party monitoring services, to collect logs in near real-time of events occurring on MARRIOTT ASSETS or COVERED DATABASES. Marriott shall regularly and actively review logs within a twenty-four (24) hour period, and appropriately follow-up with respect to SECURITY EVENTS. Marriott shall appropriately configure and test logging and monitoring services to facilitate effective identification of a SECURITY EVENT and escalation according to Marriott's incident response plan.

65. **Unauthorized Applications:** Marriott shall develop, implement, and maintain controls or authentication measures designed to alert on, and to protect against the execution or installation of identified unauthorized applications on MARRIOTT ASSETS or COVERED DATABASES.

66. **Intrusion Detection and Prevention:** Marriott shall develop, implement, and maintain intrusion prevention and detection systems, endpoint protection systems,

threat monitoring systems, or similar technologies reasonably designed to detect and restrict unauthorized access to MARRIOTT ASSETS or COVERED DATABASES.

67. **Change Detection:** Marriott shall develop, implement and maintain reasonable controls designed to provide notification within a twenty-four (24) hour period of unauthorized modifications to critical system files at the CORPORATE LEVEL.

68. **Segmentation:** Marriott shall develop, implement, and maintain policies and procedures that are reasonably designed to create network segmentation of MARRIOTT ASSETS and COVERED DATABASES in a secure manner and to logically separate MARRIOTT ASSETS between production and non-production environments. Such policies shall include a process designed to detect the presence of PERSONAL INFORMATION in non-production environments.

69. **Non-Production Environments:** Marriott shall develop, implement, and maintain policies and procedures to prohibit the use of PERSONAL INFORMATION within non-production environments unless it is de-identified.

70. **Vulnerability Management:**

a. Marriott shall develop, implement, and maintain a vulnerability management program reasonably designed to continually identify and assess vulnerabilities of MARRIOTT ASSETS or COVERED DATABASES by: (i) discovering vulnerabilities identified by reputable outside sources; (ii) assigning risk rankings to new vulnerabilities; (iii) running internal and external network

vulnerability scans at least quarterly or after any significant change to MARRIOTT ASSETS or COVERED DATABASES; and (iv) performing re-scans to ensure that previously identified vulnerabilities have been properly remediated.

b. Marriott shall develop, implement, and maintain a risk-based testing program reasonably designed to identify and assess security vulnerabilities of MARRIOTT ASSETS or COVERED DATABASES. This program shall include an appropriate schedule of risk-based tests including internal and external penetration testing, segmentation testing, and web application penetration testing to be performed on MARRIOTT ASSETS or COVERED DATABASES that adequately takes into account security risk. Such testing shall not be less than annual and shall include retests where necessary to confirm appropriate remediation.

71. **Component Hardening:** Marriott shall develop configuration standards to harden operating systems and network devices at the CORPORATE LEVEL against known threats and vulnerabilities. These standards shall be consistent with industry-recognized system hardening standards. Following the development of configuration standards, Marriott shall implement such configuration standards for new operating systems and network devices that are MARRIOTT ASSETS according to a risk-based schedule. Marriott shall evaluate and implement such configuration standards for existing operating systems and network devices that are MARRIOTT ASSETS according to a risk-based analysis and schedule.

72. **Updates/Patch Management:** Marriott shall develop, implement, and maintain processes and procedures for patch management to maintain, keep updated, and support the software on MARRIOTT ASSETS or COVERED DATABASES, using measures that take into consideration the impact a software update will have on data security of MARRIOTT ASSETS or COVERED DATABASES, Marriott's ongoing business and network and operational needs, and the scope of the resources required to maintain, update, and support the software.

a. Such processes and procedures shall include a schedule to install security updates and security patches in a timely manner that considers (without limitation) the severity of the vulnerability for which the update or patch has been released to address, the severity of the issue in the context of MARRIOTT ASSETS or COVERED DATABASES, the impact on Marriott's ongoing business and network operations, and the risk ratings articulated by the relevant software and application vendors or disseminated by the Cybersecurity and Infrastructure Security Agency or equivalent successor Federal agency.

73. **Software:** If any software on any of the MARRIOTT ASSETS is reaching its end-of-life or end-of-support date, Marriott must either timely replace such software or, prior to the end-of-life or end-of-support date, implement COMPENSATING CONTROLS.

74. **Digital Certificates:** Marriott shall use a digital certificate management tool or service to inventory digital certificates. A digital certificate for the purposes of this

paragraph shall include a security token, biometric identifier, or a cryptographic key used to protect externally facing systems and applications.

75. **Data Loss Prevention:** Marriott shall develop, implement, and maintain a process designed to detect and restrict unauthorized or inadvertent transmission of PERSONAL INFORMATION from MARRIOTT ASSETS.

76. **Asset Inventory:** Marriott shall develop, implement, and maintain written policies and procedures to regularly inventory and classify MARRIOTT ASSETS and COVERED DATABASES, including, but not limited to, with the use of scanning or equivalent tools.

77. **Hardware Removal:** In the event that Marriott removes and does not intend to reinstate within a reasonable timeframe, any MARRIOTT ASSETS that store or contain PERSONAL INFORMATION, Marriott shall remove or ENCRYPT the PERSONAL INFORMATION contained on that asset or destroy the asset. In the event that Marriott discontinues use of any of the COVERED DATABASES, Marriott shall remove or ENCRYPT the CONSUMER information on that database or destroy the database.

78. **Shared Security Responsibilities:** For any electronic systems that: (a) are capable of using and sharing software, data, and hardware resources, (b) collect, maintain, process, store, or transmit PERSONAL INFORMATION, and (c) have shared security measures between Marriott and a third party, such electronic systems shall be MARRIOTT ASSETS to the extent Marriott has direct control of the security measures required by this Judgment at Information Security Program: Specific Technical

Safeguards and Controls, Paragraphs 60 to 77. For any central reservation and loyalty database that: (a) Marriott uses to operate guest reservation or loyalty program transactions that includes two or more of the following data elements: (i) reservation details, (ii) hotel stay preferences, (iii) LOYALTY REWARDS PROGRAM number; or (iv) LOYALTY REWARDS PROGRAM points balance, and (b) has shared security measures between Marriott and a third party, such database shall be a COVERED DATABASE to the extent Marriott has direct control of the security measures required by this Judgment at Information Security Program: Specific Technical Safeguards and Controls, Paragraphs 60 to 77. Nothing contained in this paragraph shall alter Marriott's obligations under any state, federal, or other local law, rule, or regulation.

FULL IMPLEMENTATION

79. **Full Implementation:** Not later than the FULL IMPLEMENTATION DATE, Marriott shall timely implement the following specific provisions of the Information Security Program: Access Control and Account Management – Specific at Paragraph 61; Segmentation at Paragraph 68; Vulnerability Management at Paragraph 70; Updates/Patch Management at Paragraph 72; and Data Loss Prevention at Paragraph 75 (“Listed Provisions”).

80. Not later than one (1) year from the EFFECTIVE DATE, Marriott shall certify to the Office of the Attorney General for the State of Connecticut, Privacy Section and the Consumer Protection Division of the Office of the Attorney General of Maryland

(hereinafter “Designated State Attorneys General”³) that Marriott has fully implemented the Listed Provisions.

INTEGRATION

81. **Post-Acquisition Compliance Assessment:** For a period of twenty (20) years from the EFFECTIVE DATE, Marriott shall employ the following process after the closing of an acquisition pursuant to which Marriott assumes control of any entity that owns, licenses, maintains, processes, or transmits PERSONAL INFORMATION (“Acquired Entity”): Marriott must assess whether the Acquired Entity’s information security program is in compliance with the mandated terms for the Information Security Program required by the Judgment (Paragraphs 37 through 78) (“Post-Acquisition Assessment”).

a. For purposes of this section, “control” shall mean (i) either (1) holding fifty (50) percent or more of the outstanding voting securities of an issuer or (2) in the case of an unincorporated entity, having the right to fifty (50) percent or more of the profits of the entity, or having the right in the event of dissolution to fifty (50) percent or more of the assets of the entity; or (ii) having the contractual power presently to designate fifty (50) percent or more of the directors of a for-profit or not-for-profit corporation, or fifty (50) percent or more of the trustees in the case of trusts that are irrevocable and/or in which the settlor does not retain a reversionary interest.

³ Marriott is simultaneously entering into settlements with the Connecticut Attorney General and the Maryland Attorney General, among other Attorneys General, that are similar to this Judgment.

b. For purposes of this section, “entity” shall mean any natural person, corporation, company, partnership, joint venture, association, joint-stock company, trust, estate of a deceased natural person, foundation, fund, institution, society, union, or club, whether incorporated or not, wherever located and of whatever citizenship, or any receiver, trustee in bankruptcy or similar official or any liquidating agent for any of the foregoing, in his or her capacity as such; or any joint venture or other corporation which has not been formed but the acquisition of the voting securities or other interest in which, if already formed, would require notification under the Hart-Scott-Rodino Act and its implementing regulations.

82. **Post-Acquisition Plan:** Marriott shall create a plan and timeline to address gaps and deficiencies identified by Marriott in the Post-Acquisition Assessment when comparing the Acquired Entity’s information security program with the Information Security Program. Where Marriott acquires assets that will become MARRIOTT ASSETS through a transaction that does not constitute an acquisition of an Acquired Entity pursuant to Paragraph 81, Marriott may create a plan to address gaps and deficiencies identified by Marriott in a risk analysis conducted consistent with Paragraph 46. The initial timeline for addressing such gaps and deficiencies in either the acquisition of an Acquired Entity or assets shall be no longer than eighteen (18) months following the closing of an acquisition.

83. Marriott may integrate or connect any asset or assets acquired in a transaction described in Paragraph 81 or 82 of this Judgment for use in a production

environment of any of the MARRIOTT ASSETS at such time that the applicable asset or assets comply with the Information Security Program.

84. In the event that Marriott is unable to complete the plan within the initial timeline, Marriott will report to the Board Committee regarding the implementation timeline progress and update the timeline accordingly.

85. **Documentation Requirements:** Marriott shall document its efforts to comply with the requirements set forth in Paragraphs 81 through 84 of this Judgment.

THIRD-PARTY INFORMATION SECURITY ASSESSMENTS

86. **Assessment:** Marriott shall engage an independent third party (the “Assessor”) on a biennial basis to assess Marriott’s information security practices, as well as its compliance with the terms of the Information Security Program, Full Implementation, and Integration required by this Judgment (Paragraphs 37 through 85) (“Third-Party Assessment”). The Assessor shall document the Third-Party Assessment in a written report (“Assessor’s Report”).

a. The Assessor must be highly qualified and well experienced. This shall mean that, at a minimum, the Assessor must be a Certified Information Systems Security Professional (“CISSP”) or a Certified Information Systems Auditor (“CISA”), or a similarly qualified person or organization, and have at least five (5) years of experience evaluating the effectiveness of computer system security or information system security. In the event that Marriott obtains approval to engage an Assessor from the Federal Trade Commission pursuant to

the FTC ORDER, Marriott shall be deemed to have satisfied this requirement. In the event that the Federal Trade Commission pursuant to the FTC ORDER rejects an Assessor, Marriott shall not engage such Assessor for this Judgment.

b. The first Third-Party Assessment shall cover a period commencing on sixty (60) days after the EFFECTIVE DATE and ending at three-hundred sixty-five (365) days later (“Initial Assessment Period”). If the issuance date of the FTC ORDER occurs no more than 90 days after the EFFECTIVE DATE, Marriott may provide written notice to the Connecticut Attorney General’s Office that Marriott is exercising its option to adjust the Initial Assessment Period to match the initial assessment period contained in the FTC ORDER and the Initial Assessment Period contained in this subparagraph shall be revised accordingly. Each subsequent Third-Party Assessment shall cover a continuous two-year period thereafter and be due each two-year period thereafter, for a total period of ten (10) years from the FULL IMPLEMENTATION DATE therefore resulting in a total of five (5) assessments.

c. The Third-Party Assessment shall:

- i. Determine whether Marriott has implemented and maintained the Information Security Program;
- ii. Assess the effectiveness of Marriott’s implementation and maintenance of the Information Security Program;

iii. Identify material gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program;

iv. Address the status of material gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessor's Report required by this Judgment; and

v. Identify specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (1) appropriate for assessing an enterprise of Marriott's size, complexity, and risk profile, and (2) sufficient to justify the Assessor's findings. No finding of the Assessor's Report shall rely primarily on assertions or attestations by Marriott's management.

d. The Assessor's Report must be completed within a reasonable period of time after each Third-Party Assessment ends and must be signed by the Assessor, stating that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Marriott's management.

e. Following the completion of the Third-Party Assessment and receipt of the Assessor's Report, the Chief Information Security Officer (or his or her designee) or General Counsel (or his or her designee) shall present the

Assessor's findings to the Board Committee at its next regularly scheduled meeting.

f. Marriott shall provide a copy of the Assessor's Report to the Designated State Attorneys General within fourteen (14) days after Marriott's receipt of the Assessor's Report. Upon request by either of the Designated State Attorneys General, Marriott shall provide the number of hours worked on the Assessment by each member of the assessment team.

g. Following the last reporting period covered by the Assessor's Report described in subparagraph 86.b and until the expiration of the FTC ORDER, Marriott shall provide copies of the Third-Party Assessments required by the FTC ORDER to the Designated State Attorneys General within three (3) business days after Marriott delivers each Third-Party Assessment to the Federal Trade Commission.

Reports

87. **Quarterly Reports:** Marriott shall provide to the Designated State Attorneys General the reports as set forth below ("Quarterly Reports"). Upon request by either of the Designated State Attorneys General, Marriott shall provide documentation to support the Quarterly Report.

a. On the first day of the fourth month following the EFFECTIVE DATE, Marriott shall provide a plan and schedule of (i) the development of the policies and procedures required by the Information Security Program and (ii) the implementation of the Listed Provisions.

b. On the first day of the seventh month following the EFFECTIVE DATE, Marriott shall provide a progress report (i) confirming the implementation of the policies and procedures required by the Information Security Program and (ii) providing the status of the implementation of the Listed Provisions. The progress report shall provide the status of Marriott's efforts to fully implement each provision of the Listed Provisions to include (i) whether or not the provision is fully implemented and, if not, the projected date of full implementation, (ii) whether or not all necessary underlying risk analyses have been performed and, if not, a schedule of performing the remaining risk analyses, and (iii) a high-level description of the changes made during the quarter in furtherance of achieving full implementation.

c. On the first day of the tenth month following the Effective Date, Marriott shall provide an additional Quarterly Report as described in subparagraph (b), for any Listed Provisions that were not reported as fully implemented in the prior Quarterly Report.

88. Either of the Designated State Attorneys General may provide a copy of any Assessor's Report or Quarterly Report received from Marriott to the Plaintiff upon request.

89. The Third-Party Assessments, the Assessor's Reports, the Quarterly Reports and all information contained therein shall be treated by the Plaintiff as confidential to the extent permitted by the laws of the State of Tennessee; shall not be shared or disclosed except as provided herein; and shall be treated by the Plaintiff as

exempt from disclosure as permitted under the relevant public records laws of the State of Tennessee. In the event that the Plaintiff receives any request from the public for the Third-Party Assessments, the Assessor's Reports, the Quarterly Reports or other confidential documents under this Judgment and believes that such information is subject to disclosure under the relevant public records laws, the Plaintiff agrees to provide Marriott with at least ten (10) days advance notice before producing the information, to the extent permitted by state law (and with any required lesser advance notice), so that Marriott may take appropriate action to defend against the disclosure of such information. The notice under this paragraph shall be provided consistent with the notice requirements contained in Paragraph 111. Nothing contained in this subparagraph shall alter or limit the obligations of the Plaintiff that may be imposed by the relevant public records laws of the State of Tennessee, or by order of any court, regarding the maintenance or disclosure of documents and information supplied to the Plaintiff.

CONSUMER-RELATED RELIEF

90. **Deletion Option:** Marriott shall provide a deletion option to CONSUMERS in accordance with this Paragraph. Marriott shall provide a method through Marriott's Privacy Center website, or by any other equivalent method it determines, by which a CONSUMER can request the deletion of the CONSUMER's information. Upon request by a CONSUMER to exercise the deletion option, Marriott shall provide confirmation of receipt of the CONSUMER's request and take reasonable steps to communicate the request to the MARRIOTT FRANCHISED HOTEL(s).

a. If Marriott identifies that the CONSUMER resides in a U.S. jurisdiction that provides the CONSUMER with deletion rights, Marriott shall process the CONSUMER's request in compliance with the law of that jurisdiction.

b. If Marriott identifies that the CONSUMER does not reside in a U.S. jurisdiction that provides the CONSUMER with deletion rights, Marriott shall process the CONSUMER's deletion request in accordance with this subparagraph. Once Marriott verifies that the CONSUMER is a CONSUMER for whom Marriott possesses information associated with the email address and/or LOYALTY REWARDS PROGRAM account number, within sixty (60) days, Marriott shall process the CONSUMER's deletion request and notify the CONSUMER that the request has been processed. Marriott shall have until one hundred eighty (180) days after the EFFECTIVE DATE to implement this subparagraph.

c. Nothing in subparagraph (b) shall abrogate Marriott's rights to: (i) avail itself of any and all rights, exceptions, and exemptions existing under any state or federal law or (ii) retain a subset of a CONSUMER's information to comply with its legal, regulatory, or other obligations. Marriott is not obligated to comply with the requirements under subparagraph (b) when the requirements conflict with Marriott's ability to comply with federal, state, or local laws or regulations; any civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local or other governmental authorities; or any transactional, tax, escheatment, corporate accountability, or other legitimate

business need compatible with the context in which the CONSUMER provided the information.

91. Loyalty Rewards Program Review:

Marriott shall:

a. Develop, implement, and maintain an easily accessible method by which a CONSUMER can request that Marriott review the requesting CONSUMER's LOYALTY REWARDS PROGRAM account for suspected unauthorized account activity that occurred within the preceding twelve (12) months. Upon receipt of such request and relevant substantiating information from the CONSUMER, Marriott shall timely undertake reasonable steps to determine if any such suspected unauthorized activity has occurred in the CONSUMER's LOYALTY REWARDS PROGRAM account; or

b. In the event of a SECURITY EVENT specifically involving the unauthorized use of authentication credentials for CONSUMER LOYALTY REWARDS PROGRAM account(s), timely undertake reasonable steps to determine if any suspicious or unauthorized activity has occurred in CONSUMER LOYALTY REWARDS PROGRAM account(s).

c. Following any review pursuant to subparagraph (91.a) or (91.b) above, in the event that Marriott determines that suspicious or unauthorized activity by a third party resulted in any reduction of points associated with a CONSUMER's LOYALTY REWARDS PROGRAM account, unless Marriott

determines that the CONSUMER violated the terms of use of the LOYALTY REWARDS PROGRAM, Marriott shall restore the reduced points in the relevant CONSUMER's LOYALTY REWARDS PROGRAM account.

92. **Loyalty Rewards Program Access:** Marriott shall offer a multi-factor authentication method or equivalent enhanced authentication measures to CONSUMERS to directly access any Marriott account, including a LOYALTY REWARDS PROGRAM account.

93. **Consumer Transparency:**

a. Marriott shall continue to provide for CONSUMERS a link to its consumer privacy policy on the U.S. homepage of its website and in its U.S. version of its mobile application. The policy shall continue to be provided in a manner that is: (i) in readily understandable language and syntax, and (ii) in a type size, font, color, appearance, and location sufficiently noticeable for a CONSUMER to read and comprehend it, and, at a minimum, in a print that contrasts with the background against which it appears.

b. Marriott's consumer privacy policy shall include the following:

i. The detailed categories of PERSONAL INFORMATION Marriott collects and maintains;

ii. How Marriott collects the PERSONAL INFORMATION;

iii. How Marriott uses the PERSONAL INFORMATION;

iv. Whether Marriott shares the PERSONAL INFORMATION with others and, if so, what PERSONAL INFORMATION is shared and the categories of persons or entities with whom the PERSONAL INFORMATION is shared; and

v. Whether CONSUMERS can request deletion of their PERSONAL INFORMATION and, if so, how to request such deletion.

c. Material changes to Marriott's public consumer privacy policy with respect to PERSONAL INFORMATION shall be updated in Marriott's online privacy notices as soon as reasonably practical before the change is implemented. Marriott shall also e-mail notices to CONSUMERS who have valid e-mail addresses on file with Marriott informing them of such changes.

94. **Consumer Complaints:** Marriott shall maintain a point of contact, such as a dedicated e-mail address, for the Plaintiff or any U.S. federal or state governmental agency charged with enforcement of a U.S. federal or state CONSUMER PROTECTION LAW, DATA BREACH NOTIFICATION LAW, or PERSONAL INFORMATION PROTECTION LAW ("Consumer Protection Agency") for the receipt of CONSUMER complaints. Marriott shall promptly review and respond to all CONSUMER complaints submitted by a Consumer Protection Agency.

IV. DOCUMENT RETENTION

95. After the EFFECTIVE DATE Marriott shall maintain the following records for a period of not less than five (5) years:

a. Personnel records showing, for each employee of Marriott providing services in relation to any aspect of the Judgment, that employee's name, addresses, telephone numbers, job title or position, dates of service, and (if applicable) the reason for termination;

b. Written complaints either received by Marriott's Global Privacy Office directly from CONSUMERS through the dedicated Marriott privacy email address published on Marriott's Group Global Privacy Statement (privacy@marriott.com) or received by Marriott indirectly from a Consumer Protection Agency pursuant to Paragraph 94, and any written response;

c. Reports, assessments, and documentation required by this Judgment in Paragraphs 39, 43, 45, 49, 54, 58, 68, 85, and 86.d;

d. A copy of each notice to CONSUMERS provided pursuant to Paragraph 93.c; and

e. Copies of all subpoenas and subpoena responses with law enforcement agencies located in the United States if such subpoenas relate to Marriott's compliance with this Judgment.

96. Marriott shall maintain all materials the Assessor relied upon to conduct the Third-Party Assessment to the extent identified by the Assessor in the Assessor's Report, that are in the possession of Marriott, whether prepared by or on behalf of Marriott, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Marriott's

compliance with related provisions of this Judgment for a period of five (5) years from the date of the delivery of the Assessor's Report pursuant to Paragraph 86.d.

V. MONETARY PAYMENT

97. No later than thirty (30) days after the EFFECTIVE DATE, Marriott shall pay Plaintiff the sum of Nine Hundred Nineteen Thousand, Forty Three Dollars (\$919,043.00).

a. Marriott's payment to the Plaintiff may be used for any purpose, including compensatory or remedial purposes, permitted by law, at the sole discretion of the Tennessee Attorney General.

b. For the avoidance of doubt, the monetary payment made to the Plaintiff pursuant to this paragraph does not include other costs incurred or expenditures made by Marriott to come into compliance with the requirements of the Information Security Program contained in this Judgment.

c. Costs or expenditures incurred by Marriott to implement the provisions of Section III and Section IV of this Judgment are costs to come into compliance with the laws alleged by Plaintiff to have been violated. For the avoidance of doubt, neither the Plaintiff nor Marriott makes any warranty or representation as to the tax consequences of such costs or expenditures incurred by Marriott to implement the provisions of Section III and Section IV of this Judgment. Additionally, Plaintiff does

not make any warranty or representation and has not agreed to the amount of costs or expenditures appropriate for Marriott to implement the provisions of Section III and Section IV.

98. Marriott shall pay all court costs associated with the filing of this Judgment.

99. Plaintiff and Marriott agree to waive any attorneys' fees as a prevailing party under any statute, regulation, or rule.

VI. RELEASE

100. Following full payment of the amounts due under this Judgment, the Plaintiff shall release and discharge Marriott from all civil claims that it could have brought under its CONSUMER PROTECTION LAW, DATA BREACH NOTIFICATION LAW and/or PERSONAL INFORMATION PROTECTION LAW arising out of the COVERED CONDUCT. Nothing contained in this paragraph shall be construed to limit the ability of the Plaintiff to enforce the obligations that Marriott has under this Judgment.

101. Notwithstanding any term of this Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 100 as to any entity or person, including Marriott:

a. Any criminal liability that any person or entity, including Marriott, has or may have to Plaintiff; and

b. Any civil or administrative liability that any person or entity, including Marriott, has or may have to Plaintiff under any statute, regulation or rule giving rise to, any and all of the following claims:

- i. State or federal antitrust violations;
- ii. State or federal securities violations; or
- iii. State or federal tax claims.

102. Nothing in this Judgment shall be construed to settle, release, or resolve any claim against Marriott or any other person or entity by a non-party involving any private causes of action, claims, or remedies or be construed to create, waive, or limit any private causes of action, claims, or remedies.

VII. NO ADMISSION OF LIABILITY

103. **No Violations of Law:** In stipulating to the entry of this Judgment, Marriott does not admit to any violation of or liability arising from any state, federal, or local law.

104. Nothing contained in this Judgment shall be construed as an admission or concession of liability by Marriott, nor to any express or implied allegations relating to current or historical information security policies and practices. Nothing contained in this Judgment shall be construed to create any third-party beneficiary rights or give rise to or support any right of action in favor of any CONSUMER or group of CONSUMERS or confer upon any person other than the Plaintiff and Marriott any rights or remedies. By

entering into this Judgment, Marriott does not intend to create any legal or voluntary standard of care and expressly denies that any practices, policies, or procedures inconsistent with those set forth in this Judgment violate any applicable legal standard. This Judgment is not intended to be and shall not be construed as, deemed to be, represented as, or relied upon in any manner by any party in any civil, criminal, or administrative proceeding before any court, administrative agency, arbitration, or other tribunal as an admission, concession, or evidence that Marriott has violated any federal, state, or local law, or that Marriott's current or prior practices related to whether its Information Security Program is or was not in accordance with any federal, state, or local law.

VIII. GENERAL PROVISIONS

105. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Judgment after the EFFECTIVE DATE or other date as applicable to the specific provision to compromise the authority of the Plaintiff to initiate a proceeding for any failure to comply with this Judgment, or to alter or modify any federal or state law as to the use or enforcement of this Judgment.

106. Nothing in this Judgment shall be construed to limit the authority or ability of the Plaintiff to protect the interests or the people of Tennessee. This Judgment shall not bar the Plaintiff or any other governmental entity from enforcing laws, regulations, or rules against Marriott for conduct subsequent to or otherwise not covered by this Judgment. Further, nothing in this Judgment shall be construed to limit the ability

of the Plaintiff to enforce the obligations that Marriott has under this Judgment, subject to the meet and confer requirements in Paragraph 113.

107. Nothing in this Judgment shall be construed as excusing or exempting Marriott from complying with any state, federal, or other jurisdiction's law, rule, or regulation, nor shall any provision of this Judgment be construed in a manner to prevent Marriott from complying with any such law, regulation, or rule where in conflict with this Judgment. Furthermore, no provisions of this Judgment shall be construed as authorizing, permitting, or requiring Marriott to engage in any acts or practices prohibited by any state, federal, or other jurisdiction's law, rule, or regulation.

108. Marriott shall deliver a copy of this Judgment to, and otherwise fully apprise, its Chief Executive Officer, Chief Information Security Officer, Chief Privacy Officer, General Counsel, and Board of Directors within ninety (90) days of the EFFECTIVE DATE. To the extent Marriott replaces any of the above listed officers or directors, Marriott shall deliver a copy of this Judgment to their replacements within ninety (90) days from the date on which such person assumes such position with Marriott unless such person has previously been provided a copy pursuant to this Judgment.

109. Marriott shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Judgment or for any other purpose that would otherwise circumvent any term of this Judgment. Marriott shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Judgment.

110. This Judgment shall not be construed to waive any claims of sovereign immunity that the State of Tennessee may have in any action or proceeding.

111. **Notice:** All notices or other documents to be provided under this Judgment shall be sent by electronic mail. Nothing herein prohibits the sending party from simultaneously providing notice by electronic mail and by United States mail or a nationally recognized courier service.

a. Whenever Marriott shall provide notice or documents to the Plaintiff under this Judgment, that requirement shall be satisfied by sending notice to:

Deputy of the Consumer Protection Division
Office of the Tennessee Attorney General
P.O. Box 20207
Nashville, TN 37202-0207
Email: Consumerdivision@ag.tn.gov

The Plaintiff may update its designee and contact information by sending written notice to Marriott informing it of the change.

b. Whenever the Plaintiff shall provide notice or documents to Marriott under this Judgment, that requirement shall be satisfied by sending notice to:

Primary Point of Contact:
Rena Hozore Reiss
Executive Vice President and General Counsel
7750 Wisconsin Avenue
Bethesda, MD 20814
OGC@marriott.com

Alternate Point of Contact:

Kimberly Shur
Senior Vice President and Global Privacy Officer
7750 Wisconsin Avenue,
Bethesda, MD 20814
GPO@marriott.com

Marriott may update its designee and contact information by sending written notice to the Plaintiff informing it of the change. In the event that Marriott does not have a valid designee on file, the Plaintiff may send notice to Marriott's registered agent or counsel of record in this Judgment to satisfy this requirement.

112. Solely for the purposes of entry of this Judgment, Marriott waives any defect associated with service of the Plaintiff's Complaint and does not require issuance or service of process of a summons. Further, Marriott waives any statutorily required notice associated with the commencement of this action, including any requirement to seek injunctive relief.

113. **Meet and Confer:** If the Plaintiff has reason to believe that Marriott has failed to comply with this Judgment, and if in the Plaintiff's sole discretion the failure to comply does not threaten the health or safety of citizens and/or does not create an emergency requiring immediate action, the Plaintiff will notify Marriott of such failure to comply and Marriott shall have thirty (30) days from receipt of such notice to provide a good faith written response, including either a statement that Marriott believes it is in full compliance or otherwise a statement explaining how the violation occurred how it has been addressed or when it will be addressed, and what Marriott will do to make sure the violation does not happen again. The Plaintiff may agree to provide Marriott more than thirty (30) days to respond.

114. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Judgment, or to compromise the authority of the Plaintiff to initiate a proceeding for any failure to comply with this Judgment after receiving the response from Marriott described in Paragraph 113 above, if the Plaintiff determines that an enforcement action is in the public interest.

115. **Severability:** If any clause, provision, or section of this Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Judgment and this Judgment shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or provision had not been contained herein.

116. Jurisdiction is retained by the Court for the purpose of enabling any party to the Judgment to apply to the Court at any time for such further orders and directions as may be necessary or appropriate for the construction or the carrying out of this Judgment, for the modification of any of the injunctive provisions hereof, for enforcement of compliance herewith, and for the punishment of violations hereof, if any.

The clerk is ordered to enter this Judgment forthwith.

ORDERED AND ADJUDGED at Nashville, Tennessee, this _____ day of _____,
2024.

CHANCELLOR

APPROVED FOR ENTRY:

ATTORNEY GENERAL, STATE OF TENNESSEE



JONATHAN SKRMETTI

Attorney General and Reporter

B.P.R. No. 031551

Office of the Tennessee Attorney General

P.O. Box 20207

Nashville, TN 37202-0207

Date: 10/9/24

APPROVED:

DEFENDANT MARRIOTT INTERNATIONAL, INC.

By: 

Date: 10-9-2024

Rena Hozore Reiss
Executive Vice President and General Counsel
Marriott International, Inc.
7750 Wisconsin Ave.,
Bethesda, Maryland 20814

COUNSEL FOR DEFENDANT, MARRIOTT INTERNATIONAL, INC.

By: TaCara H. Harris

Date: 10/9/2024

TaCara Harris
Local Counsel for Marriott International, Inc.
Tennessee Bar No. 32148
King & Spalding LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600

and

By: Phyllis B. Sumner

Date: 10-9-2024

Phyllis B. Sumner
Lead Counsel for Marriott International, Inc.
Stephen P. Cummings
Jillian Simons
King & Spalding LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140

COPY

**IN THE CHANCERY COURT OF DAVIDSON COUNTY, TENNESSEE
FOR THE TWENTIETH JUDICIAL DISTRICT AT NASHVILLE**

STATE OF TENNESSEE,)
ex rel. JONATHAN SKRMETTI,)
 Attorney General and Reporter,)
)
 Plaintiff,)
)
 v.)
)
 MARRIOTT INTERNATIONAL, INC.,)
 a corporation,)
)
 Defendant.)

Case No. 24-1185-TI

FILED
 2024 OCT -9 AM 10:12
 CLERK OF COURT
 DAVIDSON COUNTY, TENNESSEE

COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF

Plaintiff, the State of Tennessee, Office of the Attorney General and Reporter (the “Plaintiff” or the “State”), brings this action against defendant Marriott International, Inc., a corporation (“Marriott” or “Defendant”), for violations of the Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. § 47-18-101, et seq. (the “TCPA”), and states as follows:

THE PARTIES

1. Plaintiff, the State of Tennessee, is one of fifty sovereign states of the United States. Jonathan Skrmetti is the Attorney General and Reporter of the State of Tennessee and has been duly appointed to serve as Attorney General by the Tennessee Supreme Court. This proceeding is brought by the State of Tennessee in its sovereign capacity by and through the Attorney General.

2. The Attorney General is authorized under Tenn. Code Ann. § 47-18-108(a)(1) to bring an action in the name of the State against any person he has reason to believe has violated, is violating, or, based upon information received from another law enforcement agency, is about

to violate the TCPA, and to restrain such violation by temporary restraining order, preliminary, or permanent injunction.

3. The Attorney General has reason to believe that Defendant has engaged in acts or practices declared to be unlawful by the TCPA in conjunction with data privacy violations, among other things, and that this proceeding is in the public interest. *See* Tenn. Code Ann. § 47-18-108(a)(1).

4. Defendant Marriott International, Inc. (“Marriott”) is a Delaware corporation with its principal office or place of business at 7750 Wisconsin Ave., Bethesda, Maryland 20814.

JURISDICTION AND VENUE

5. At all times relevant to this Complaint, Marriott was engaged in trade and commerce affecting consumers in Tennessee. Marriott was also in possession of the personal information of Tennessee residents. In addition, at all times relevant to this Complaint, Marriott was engaged in offering for sale and selling hospitality services to consumers in Tennessee.

6. Venue for this action properly lies in Davidson County, Tennessee, pursuant to Tennessee Code Annotated § 47-18-108(a)(4).

7. This Court has subject matter jurisdiction under Tennessee Code Annotated § 47-18-108(a). The Chancery Court is authorized to hear this case as a court of general jurisdiction and under the TCPA.

8. This Court has personal jurisdiction over Defendant because, as more fully set forth in this Complaint, it conducts or transacts business in Tennessee. The violations of law alleged in this Complaint took place in or were directed into Tennessee by Defendant. In addition, many of the consumers impacted by Defendant’s violations reside in Tennessee. *See* Tenn. Code Ann. §§ 20-2-202, -222, -223, and -225.

9. The Defendant agrees to waive notice as required by Tenn. Code Ann. § 47-18-108(2).

BACKGROUND

10. 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.

11. On or about November 16, 2015, Marriott announced that it would acquire Starwood Hotels and Resorts Worldwide, LLC (“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.

12. 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 in December 2018.

Starwood Data Breach

13. 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. In fact, Marriott did not detect this breach until September 7, 2018, nearly two

years after the legal close of Marriott's acquisition of Starwood. The incident (hereinafter, the "Starwood Data Breach") was announced by Marriott on November 30, 2018.

14. 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 Starwood's internal network for a four-year period, until Marriott's system finally detected an attempt to export consumer data from the guest reservation database on September 7, 2018.

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

16. During this period spanning more than four years, 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.

17. Following the breach, a forensic examiner assessed Starwood's systems and identified failures, 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.

18. The Starwood Data Breach exposed the personal information of 339 million consumer records globally, including 131.5 million guest records pertaining to customers

associated with the United States, some of which included contact information, gender, dates of birth, payment card information, passport numbers, legacy Starwood Preferred Guest information, reservation information, and hotel stay preferences.

Unauthorized Account Access Incidents

19. The information security failures detailed in this Complaint are not limited to Starwood's computer networks, systems, and databases.

20. 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 "Unauthorized Account Access Incidents").

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

22. The intruders were able to access over 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.

23. 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 that could be used or redeemed, including for booking stays at hotel properties.

Defendants' Deceptive Information Security Statements

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

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

26. 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).

27. 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.

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

"Personal Information" is information that identifies you as an individual or relates to an identifiable individual. We may collect Personal Information such as:

Name[s] . . . home and work address[es], telephone number[s] and email address[es], your business title, date and place of birth, nationality, passport, visa or other government-issued identification information, guest stay information, including the hotels where you have stayed, date of arrival and departure, goods and services purchased, special requests made, information and observations about your service preferences (including room type, facilities, holiday preferences,

amenities requested, ages of children or any other aspects of the Services used); . . . credit and debit card number; Marriott [] Rewards information online user accounts details, profile or password details and any frequent flyer or travel partner program affiliation . . .

We seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization. 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).

Information Security Practices

29. Marriott and/or Marriott as successor to Starwood failed to provide reasonable or appropriate security for the personal information that they collected and maintained about consumers. Among other things, Marriott and/or Marriott as successor to Starwood:

- a. Failed to patch outdated software and systems in a timely manner, leaving Starwood’s network susceptible to attacks;
- b. 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 Marriott and/or Marriott as successor to Starwood from detecting intruders in its network and further prevented it from determining the information exfiltrated from its network;
- c. 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 were not created;

- d. Failed to implement appropriate firewall controls. This failure resulted in malicious actors making unauthorized connections from outside of the Starwood's network;
- e. Failed to implement appropriate network segmentation, which allowed intruders to move easily between Starwood hotel property systems and Starwood's corporate networks;
- f. Failed to apply adequate multifactor authentication to protect sensitive information. For example, Starwood failed to comply with contractual obligations and/or internal policies requiring multifactor authentication for remote access to sensitive environments, including environments containing payment card data;
- g. Failed to properly eradicate threats from the Starwood or Marriott environment after incidents, and failed to implement improvements based on lessons learned from previous incidents; and
- h. Failed to implement appropriate password controls. As a result of this failure, employees often used default, blank, or weak passwords.

30. As a direct result of the failures described in Paragraph 29 above, between 2014 and 2020, malicious actors were able to gain unauthorized access to the personal information of millions of consumers, including passport information, payment card numbers, Starwood loyalty numbers, along with name, gender, date of birth, address, email address, telephone number, username, and hotel stay and other travel information.

COUNT ONE

**VIOLATIONS OF TENNESSEE CONSUMER PROTECTION ACT OF 1977
TENN. CODE ANN. § 47-18-101, ET SEQ. – Deceptive and Unfair Acts and Practices**

31. Plaintiff realleges and incorporates Paragraphs 1 through 30 as if fully set forth herein.

32. Defendant has engaged in deceptive acts or practices affecting the conduct of trade or commerce, as set forth above, in violation of Tenn. Code Ann. § 47-18-104.

33. Defendant made false and misleading statements to consumers regarding its data protection practices which had the capacity, tendency, or effect of deceiving or misleading consumers in violation of Tenn. Code Ann. § 47-18-104.

34. Defendant's failure to adequately inform consumers regarding its data protection practices constitutes a failure to state material facts, the omission of which has deceived or tended to deceive consumers, as set forth above in violation of Tenn. Code Ann. § 47-18-104.

35. Defendant's failure to take reasonable steps to protect consumers' personal information and subsequent data breach caused substantial harm to consumers, that consumers could not reasonably avoid, and which did not benefit the marketplace or competition, making it an unfair trade practice in violation of Tenn. Code Ann. § 47-18-104.

REMEDIES

44. Pursuant to Tenn. Code Ann. § 47-18-108(a), Plaintiff is entitled to an order providing injunctive relief against Defendant.

45. Pursuant to Tenn. Code Ann. § 47-18-108(b), Plaintiff is entitled to an order to restore money or property, among other things, to any person who has suffered any ascertainable loss and require payment to the State of a civil penalty of not more than one thousand dollars (\$1,000) for each violation.

46. The Court may also order reimbursement to the State for the reasonable costs and expenses of investigation and prosecution of actions under the TCPA, including attorneys' fees. *See* Tenn. Code Ann. § 47-18-108(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests this Court enter judgment against Defendant Marriott and enter an Order:

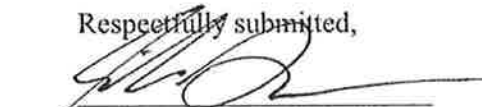
A. Finding that Defendant violated the TCPA, Tenn. Code Ann. § 47-18-101, et seq. by engaging in the unlawful acts and practices alleged herein, and permanently enjoining Defendant from continuing to engage in such unlawful acts and practices;

C. Requiring Defendant to pay up to \$1000 for each and every violation of the TCPA, as provided by Tenn. Code Ann. § 47-18-108(b);


D. Requiring Defendant to pay all costs for the prosecution and investigation of this action, as provided by Tenn. Code Ann. § 47-18-108(b); and

F. Providing any such other and further relief as the Court deems just, proper, and equitable under the circumstances.

Respectfully submitted,



JONATHAN SKRMETTI
Attorney General and Reporter



AC AGEE, B.P.C. No. 035024
Assistant Attorney General

OFFICE OF THE TENNESSEE ATTORNEY GENERAL
Public Protection Section
Consumer Protection Division
UBS Tower, 20th Floor

315 Deaderick Street
Nashville, Tennessee 37243
P: (615) 741-1671
F: (615) 532-2910
Jeff.Hill@ag.tn.gov
Matthew.Janssen@ag.tn.gov
AC.Agee@ag.tn.gov

Attorneys for Plaintiff, State of Tennessee

Dated: October 9, 2024