UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

In the Matter of **MARRIOTT INTERNATIONAL, INC., a corporation,** **and** **STARWOOD HOTELS & RESORTS WORLDWIDE, LLC, a limited liability company.**	**FILE NO. 1923022** **AGREEMENT CONTAINING CONSENT ORDER**

The Federal Trade Commission ("Commission") has conducted an investigation of certain acts and practices of Marriott International, Inc., and Starwood Hotels & Resorts Worldwide, LLC (collectively "Proposed Respondents"). The Commission's Bureau of Consumer Protection ("BCP") has prepared a draft of an administrative Complaint ("draft Complaint"). BCP and Proposed Respondents, individually or through their duly authorized officers, enter into this Agreement Containing Consent Order ("Consent Agreement") to resolve the allegations in the attached draft Complaint through a proposed Decision and Order to present to the Commission, which is also attached and made a part of this Consent Agreement.

IT IS HEREBY AGREED by and between Proposed Respondents and BCP, that:

1. The Proposed Respondents are:

   a. Proposed Respondent Marriott International, Inc., a Delaware corporation with its principal office or place of business at 7750 Wisconsin Avenue, Bethesda, Maryland 20814.

   b. Proposed Respondent Starwood Hotels & Resorts Worldwide, LLC, a Maryland limited liability company with its principal office or place of business at 7750 Wisconsin Avenue, Bethesda, Maryland 20814. Starwood is now a wholly-owned subsidiary of Marriott International, Inc

2. Proposed Respondents neither admit nor deny any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Proposed Respondents admit the facts necessary to establish jurisdiction.

3. Proposed Respondents waive:

   a. Any further procedural steps;

b. The requirement that the Commission's Decision contain a statement of findings of fact and conclusions of law; and

c. All rights to seek judicial review or otherwise to challenge or contest the validity of the Decision and Order issued pursuant to this Consent Agreement.

4. This Consent Agreement will not become part of the public record of the proceeding unless and until it is accepted by the Commission. If the Commission accepts this Consent Agreement, it, together with the draft Complaint, will be placed on the public record for 30 days and information about them publicly released. Acceptance does not constitute final approval, but it serves as the basis for further actions leading to final disposition of the matter. Thereafter, the Commission may either withdraw its acceptance of this Consent Agreement and so notify each Proposed Respondent, in which event the Commission will take such action as it may consider appropriate, or issue and serve its Complaint (in such form as the circumstances may require) and decision in disposition of the proceeding, which may include an Order. *See* Section 2.34 of the Commission's Rules, 16 C.F.R. § 2.34 ("Rule 2.34").

5. If this agreement is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to Rule 2.34, the Commission may, without further notice to Proposed Respondents: (1) issue its Complaint corresponding in form and substance with the attached draft Complaint and its Decision and Order; and (2) make information about them public. Proposed Respondents agree that service of the Order may be effected by its publication on the Commission's website (ftc.gov), at which time the Order will become final. *See* Rule 2.32(d). Proposed Respondents waive any rights they may have to any other manner of service. *See* Rule 4.4.

6. When final, the Decision and Order will have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other Commission orders.

7. The Complaint may be used in construing the terms of the Decision and Order. No agreement, understanding, representation, or interpretation not contained in the Decision and Order or in this Consent Agreement may be used to vary or contradict the terms of the Decision and Order.

8. Each Proposed Respondent agrees to comply with the terms of the proposed Decision and Order from the date that Proposed Respondent signs this Consent Agreement. Proposed Respondents understand that they may be liable for civil penalties and other relief for each violation of the Decision and Order after it becomes final.

MARRIOTT INTERNATIONAL, INC.

By:_____
Rena Hozore Reiss
Executive Vice President and
General Counsel

Date:_____

FEDERAL TRADE COMMISSION

By:_____
Katherine E. McCarron
Attorney, Bureau of Consumer Protection

By:_____
Kamay M. Lafalaise
Attorney, Bureau of Consumer Protection

STARWOOD HOTELS &
RESORTS WORLDWIDE, LLC

By:_____

Rena Hozore Reiss
Executive Vice President and
General Counsel

Date:_____

APPROVED:

By:_____

Tiffany George
Assistant Director
Division of Privacy and Identity Protection

By:_____
Samuel Levine
Director
Bureau of Consumer Protection

Date:_____

By:_____
Phyllis B. Sumner
King and Spalding LLP
Attorney for Proposed Respondents

Date:_____

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.**	**DECISION AND ORDER** **DOCKET NO.**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:

   a. Marriott International, Inc., a Delaware corporation with its principal office or place of business at 7750 Wisconsin Avenue, Bethesda, Maryland 20814.

   b. Starwood Hotels & Resorts Worldwide, LLC, a Maryland limited liability company with its principal office or place of business at 7750 Wisconsin Avenue, Bethesda, Maryland 20814. Starwood is now a wholly-owned subsidiary of Marriott International, Inc.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

1. "Clear and Conspicuous" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

   a. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made through only one means.

   b. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

   c. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

   d. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

e. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

f. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

g. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

h. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

2. "Covered Incident" means a Security Event that Marriott is legally required to notify a United States federal, state, or local governmental entity that information of or about an individual was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

3. "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.

4. "Loyalty Rewards Program" means the Marriott Bonvoy program (or such name as it may be known in the future) offered by Respondents that allows consumers to redeem points for certain goods or services according to the terms of such program offered by Respondents.

5. "Marriott" shall mean Marriott International, Inc., and its subsidiaries, successors, and assigns that collect, store, or process Personal Information; *provided*, *however*, that in no event shall "Marriott" include the "Marriott Franchised Hotels" or any subsidiary of Marriott that is incorporated and operates outside of the United States. "Marriott" shall include "Starwood" unless specifically stated otherwise.

6. "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 any Respondent.

7. "Personal Information" means individually identifiable information from or about an individual consumer, including: (a) a first and last name; (b) a home or other physical address; (c) an email address; (d) financial account information, such as

payment card number; (e) government-issued identifiers, such as driver's license or passport numbers; or (f) account information, such as username and password or Loyalty Rewards Program numbers.

8. "Respondents" means (a) Marriott and its subsidiaries, and any successors and assigns; and (b) Starwood and its subsidiaries, and any successors and assigns, individually, collectively, or in any combination.

9. "Security Event" shall mean any compromise to the confidentiality, integrity, or availability of Personal Information held on or accessed through any Marriott information technology ("IT") asset, or any event that gives rise to a reasonable likelihood of such compromise.

10. "Starwood" shall mean Starwood Hotels & Resorts Worldwide, LLC, its subsidiaries, successors, and assigns that collect, store, or process Personal Information; *provided*, *however*, that in no event shall "Starwood" include any subsidiary of Starwood that is incorporated and operates outside of the United States.

Provisions

I. Prohibition Against Misrepresentations About Privacy and Security

IT IS ORDERED that Respondents, Respondents' officers, agents, and employees, and all other persons in active concert or participation with any of them who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication:

A. Respondents' collection, maintenance, use, deletion, or disclosure of Personal Information; and

B. The extent to which Respondents protect the privacy, security, availability, confidentiality, or integrity of Personal Information.

II. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondents, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Personal Information, must, within 180 days of the effective date of this Order, establish, implement and maintain a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, Respondents must, at a minimum:

A. Document in writing the content, establishment, implementation, and maintenance of the Information Security Program;

B. Provide the written program and any evaluations thereof or updates thereto to Respondents' Board of Directors or governing body or, if no such board or

equivalent governing body exists, to a senior officer of Respondents responsible for Respondents' Information Security Program at least annually. Marriott shall also provide to that governing structure outlined above a Covered Incident report promptly (not to exceed 120 days) after a Covered Incident;

C. Designate a qualified employee to coordinate and be responsible for the Information Security Program;

D. Assess and document, at least annually and promptly (not to exceed 120 days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information ("Risk Assessment") that could result in the (1) unauthorized collection, maintenance, alteration, destruction, use, or disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, or other compromise of such Personal Information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondents identify based on the Risk Assessment described in sub-Provision II.D or risk-based analysis. Each safeguard must take into account the volume and sensitivity of the Personal Information that is being assessed, and the likelihood of unauthorized disclosure, misuse, loss, or other compromise of such Personal Information. Such safeguards must also include:

1. Providing role-appropriate training for Respondents' employees who either are responsible for the Information Security Program or have access to Personal Information on any Marriott IT asset, at least annually, on how to safeguard Personal Information on such Marriott IT asset. Respondents shall have policies and procedures that require Marriott Franchised Hotels to provide role-appropriate training for their employees who have access to Personal Information on any Marriott IT asset, at least annually, on how to safeguard Personal Information on such Marriott IT asset;

2. Documenting in writing the content, establishment, implementation, and maintenance of an incident response plan designed to ensure the identification of, investigation of, and response to the unauthorized access to Personal Information on Marriott IT assets. Where appropriate, Respondents shall revise and update this incident response plan to adapt to any changes to any Marriott IT asset;

3. Establishing, implementing, and maintaining policies and procedures for logging and monitoring Marriott IT assets. 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 of events occurring on Marriott IT assets. Such policies and procedures shall also require Marriott to use such technical measures to regularly and actively review logs for anomalous activity and active threats within a twenty-four (24) hour period, and appropriately follow up with respect to Security Events. Such measures shall require

Respondents to identify and respond to anomalous events and unauthorized attempts to access or exfiltrate Personal Information. 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;

4. Establishing, implementing, and maintaining data access controls for Marriott employees and vendors to Marriott IT assets (including databases) storing Personal Information and policies, procedures, and technical measures to minimize or prevent online attacks resulting from the misuse of valid credentials, including: (a) restricting inbound and outbound connections; (b) requiring and enforcing strong passwords; (c) preventing the reuse of credentials known to Marriott to be compromised to access Personal Information; (d) implementing password resets for credentials known to Marriott to be compromised; and (e) using the principle of least privilege to limit employee access to Personal Information to the minimum required to perform that employee's job;

5. Establishing, implementing, and maintaining multi-factor authentication or equivalent enhanced authentication measures for remote access by Marriott employees and vendors to Marriott IT assets (including databases) storing Personal Information. Respondents need only provide multi-factor authentication or enhanced authentication measure as an option for U.S. consumers for any account that collects Personal Information and authenticates U.S. consumers. Any information collected solely for multi-factor authentication may only be used for authentication purposes and no other purpose;

6. Developing configuration standards to harden operating systems and network devices in Marriott's corporate network segment and other non-property network segments against known threats and vulnerabilities. New operating systems and network devices introduced to such segments shall not be approved for use as Marriott IT assets until they meet Respondents' configuration standards;

7. Identifying instances where Respondents shall Encrypt, tokenize, or use other security measures to protect Personal Information on Marriott IT assets;

8. Establishing, implementing, and maintaining scanning or equivalent tools to regularly inventory and classify Marriott IT assets containing Personal Information that includes hardware, software, and location of any such Marriott IT assets. In the event that Marriott removes any Marriott IT asset containing Personal Information and does not intend to reinstate that asset, Marriott shall remove or Encrypt the Personal Information contained on the asset, or destroy that asset;

9. Establishing, implementing and maintaining vulnerability and patch management policies and procedures to maintain, keep updated, and support the software on Marriott IT assets containing Personal Information, using measures that take into consideration the impact a software update will have on such Marriott IT assets' data security, Marriott's ongoing business, network, and operational needs, and the scope of the resources required to maintain, update, and support the software. Marriott shall implement and maintain processes and procedures to schedule and install updates and security patches on that software in a timely manner, that require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed, and that include timelines for addressing vulnerabilities that account for the severity and exploitability of the risk implicated; and

10. Enforcing policies and procedures to ensure the timely investigation of Security Events and the timely remediation of critical and high-risk security vulnerabilities;

F. Assess, at least annually and promptly (not to exceed 120) days following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results;

G. Following the closing of an acquisition pursuant to which any Respondent assumes control of any entity that owns, licenses, maintains, processes, or transmits Personal Information ("Acquired Entity"), Respondents must assess whether the Acquired Entity's information security program is in compliance with the mandated terms for the Information Security Program required by Provision II of this Order ("Post-Acquisition Assessment"). Respondents shall design, implement, and maintain a plan and timeline to address gaps and deficiencies identified in the Post-Acquisition Assessment. The plan shall address such gaps and deficiencies that relate to any Acquired Entity's IT asset prior to Respondents' use as a Marriott IT asset in the production environment;

H. Test and monitor the effectiveness of the safeguards at least annually and promptly (not to exceed 120 days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include a vulnerability management program reasonably designed to continually identify and assess vulnerabilities within Marriott IT assets containing Personal Information by (1) discovering vulnerabilities identified by reputable outside sources; (2) assigning risk rankings to new vulnerabilities; (3) running internal and external network vulnerability scans at least quarterly or after any significant change to such Marriott IT assets, and promptly (not to exceed 120 days) after a Covered Incident; and (4) performing re-scans to ensure that previously identified vulnerabilities have been properly remediated. Such testing and monitoring must also include a risk-based testing program reasonably designed to identify and assess security vulnerabilities within such Marriott IT

assets. 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 such Marriott IT assets that adequately takes into account security risk. Such testing shall not be less than annual, and promptly (not to exceed 120 days) after a Covered Incident, and shall include retests where necessary to confirm appropriate remediation;

I. Select and retain vendors capable of safeguarding Personal Information they access through or receive from Respondents, and contractually require vendors to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Personal Information;

J. Evaluate and adjust the Information Security Program as appropriate in light of any changes to Respondents' operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision II.D of this Order, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, Respondents must evaluate the Information Security Program at least once annually and modify the Information Security Program based on the results; and

K. Require the Marriott Franchised Hotels by contract to implement and maintain appropriate safeguards to protect Personal Information. Marriott also shall develop and implement a risk-based audit program to review compliance of Marriott Franchised Hotels with the obligations imposed by Marriott. Marriott shall retain appropriate contractual rights to enforce a Marriott Franchised Hotel's compliance with such requirements.

III. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Information Security Program, Respondents must obtain initial and biennial assessments ("Third-Party Assessments"):

A. The Third-Party Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession, (2) conducts an independent review of the Information Security Program, (3) retains all documents relevant to each Third-Party Assessment for 5 years after completion of such Third-Party Assessment, and (4) will provide such documents to the Commission within 10 days of receipt of a written request from a representative of the Commission. The Assessor may not withhold any documents from the Commission on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.

B. For each Third-Party Assessment, Respondents must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion.

C. The reporting period for the Third-Party Assessments must cover: (1) the first 365 days after the issuance date of the Order for the initial Third-Party Assessment; and (2) each 2 year period thereafter for twenty (20) years after issuance of the Order for the biennial Third-Party Assessments.

D. Each Third-Party Assessment must, for the entire assessment period: (1) determine whether Respondents have implemented and maintained the Information Security Program required by Provision II; (2) assess the effectiveness of Respondents' implementation and maintenance of sub-Provisions II.A-K; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Third-Party Assessment required by this Order; and (5) 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 (a) appropriate for assessing an enterprise of Respondents' size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Third-Party Assessment shall rely primarily on assertions or attestations by Respondents' management. The Third-Party Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondents' management, and state the number of hours that each member of the assessment team worked on the Third-Party Assessment. To the extent that Respondents revise, update, or add one or more safeguards required under Provision II of this Order during an assessment period, the Third-Party Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Third-Party Assessment must be completed within 60 days after the end of the reporting period to which the Third-Party Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondents must submit the initial Third-Party Assessment to the Commission within 10 days after Respondents' receipt of the Third-Party Assessment. The submission must be made via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Marriott International, Inc., FTC File No. 1923022." All subsequent biennial Third-Party Assessments must be retained

by Respondents until the Order is terminated and provided to the Associate Director for Enforcement within 10 days of request.

IV. Cooperation with Third-Party Information Security Assessor

IT IS FURTHER ORDERED that Respondents, whether acting directly or indirectly, in connection with any Third-Party Assessment required by Provision III of this Order titled Information Security Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Third-Party Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Marriott IT assets so that the Assessor can determine the scope of the Third-Party Assessment, and visibility to those Marriott IT assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondents have implemented and maintained the Information Security Program required by Provision II; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A-K; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

V. Annual Certification

IT IS FURTHER ORDERED that Respondents must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from the Chief Executive Officer ("CEO") that: (1) Respondents have established, implemented, and maintained the requirements of this Order; and (2) Respondents are not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of the CEO or subject matter experts upon whom the CEO reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Marriott International, Inc., FTC File No. 1923022."

VI. Covered Incident Reports

IT IS FURTHER ORDERED that, within 10 days of any notification to a United States federal, state, or local government entity of a Covered Incident, Respondents must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that triggered any notification to the U.S. federal, state, or local government entity;

D. The number of consumers whose information was affected by the Covered Incident;

E. The acts that Respondents have taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of any materially different notice sent by Respondents to U.S. consumers or to any U.S. federal, state, or local government entity regarding the Covered Incident.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Marriott International, Inc., FTC File No. 1923022."

VII. Loyalty Rewards Program Accounts Review

IT IS FURTHER ORDERED that Respondents shall:

A. Establish, implement, and provide a Clear and Conspicuous method by which a U.S. consumer can request that Respondents review the requesting consumer's Loyalty Rewards Program account for suspected unauthorized account activity that occurred within the preceding 12 months. Upon receipt of such request and relevant substantiating information from the consumer, Respondents 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 U.S. consumer Loyalty Rewards Program

account(s), timely undertake reasonable steps to determine if any suspicious or unauthorized activity has occurred in such consumer Loyalty Rewards Program account(s). Following any review, pursuant to sub-Provision (A) or (B), in the event that Respondents determine that suspicious or unauthorized activity by a third party resulted in any reduction of points associated with a U.S. consumer's Loyalty Rewards Program account, unless Respondents determine that the consumer violated the terms of use of the Loyalty Program, Respondents shall restore the reduced points in the relevant consumer's Loyalty Rewards Program account.

VIII. Data Handling

IT IS FURTHER ORDERED that:

A. Within 180 days after issuance of this Order, Respondents shall provide a Clear and Conspicuous link on Marriott's website and on their mobile applications directing U.S. consumers to an online process through which they can request the deletion of their Personal Information that is associated with the email address and/or Loyalty Rewards Program account number identified in the consumer's request. Respondents must verify receipt of each such request and explain the process of deletion within 60 days of the request. Nothing in this Provision shall abrogate Respondents' right to avail itself of any and all rights, exceptions, and exemptions existing under any state or federal law.

B. Respondents shall maintain a policy designed to retain Personal Information for only as long as is reasonably necessary to fulfill the purpose for which the Personal Information was collected, and shall disclose the purpose for which the Personal Information is collected and the specific business need for retaining Personal Information in its terms of use or privacy policy. *Provided*, *however*, that such Personal Information need not be destroyed, and may be disclosed, if requested by a government agency; if required by law, regulation, or court order or other legal obligation; or for other documented legitimate business needs except for marketing.

IX. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

A. Respondents, within 10 days after the Effective Date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. Respondents must deliver a copy of this Order to: (1) Respondents' principals, officers, directors, and LLC managers and members; (2) Respondents' employees having managerial responsibilities for Respondents' Information Security Program and Respondents' agents and representatives who participate in

Respondents' Information Security Program; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within 10 days after the Effective Date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondents deliver a copy of this Order, Respondents must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

X. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

A. One year after the issuance date of this Order, Respondents must submit a compliance report, sworn under penalty of perjury, in which Respondents must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondents; (b) identify all of Respondents' businesses by all of their names, primary telephone numbers, and primary physical, postal, email, and Internet addresses; (c) describe the activities of each of Respondents' businesses; (d) describe in detail whether and how Respondents are in compliance with each Provision of this Order, including a discussion of all of the changes Respondents made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondents must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of any Respondent or any entity that any Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: In re Marriott International, Inc., FTC File No. 1923022.

XI. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years. Specifically, Respondents must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all U.S. consumer complaints related to Respondents' collection, maintenance, use, deletion, or disclosure of Personal Information received through Respondents' customer privacy channels, and any response, except to the extent that deletion of such records has been requested by a consumer;

D. A copy of each widely disseminated representation by Respondents that describes the extent to which Respondents maintain or protect the privacy, security or confidentiality of any Personal Information, including any representation concerning a change in any website or other service controlled by Respondents that relates to the privacy, security, or confidentiality of Personal Information;

E. For five (5) years after the date of preparation of each Third-Party Assessment required by this Order, all materials the Assessor relied upon to prepare the Third-Party Assessment, whether prepared by or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondents' compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

F. For five (5) years from the date received, copies of all subpoenas and other communications to and from law enforcement, and subpoena responses, if such communications relate to Respondents' compliance with this Order;

G. For five (5) years from the date created or received, all records, whether prepared by or on behalf of Respondents, that demonstrate non-compliance by Respondents with this Order; and

H. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

XII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents' compliance with this Order:

A. Within 10 days of receipt of a written request from a representative of the Commission, Respondents must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondents. Respondents must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that any Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such

complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Holyoak recused.

April J. Tabor
Secretary

SEAL:
ISSUED: