MARRIOTT INTERNATIONAL, INC.

By:_____
Rena Hozore Reiss
Executive Vice President and

FEDERAL TRADE COMMISSION

By:_____
Katherine E. McCarron

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 A0017 ft RondenCompvisas63.02 Tnt A00rguson 005 Twi005 Twr If5.9

Findings

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,

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

95 -1.15 TD0 Tc.0013 sks Respondeott shrevpromess upd(dinthisirume)Tj42.14 0 TD.0002 Tc220015(inc Incidens resabplana3

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

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

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.

ronsumer Protection

2 714-544 -1.

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.NrP Potatl

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 Aven

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.

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&RPPLVRQHUROXRDNUHFMG.

April -Tabor
Secretary

SEAL:
ISSUED: