Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of Marriott International, Inc.*, File No. 1923022**

The Federal Trade Commission (the "Commission") has accepted, subject to final approval, an agreement containing consent order from Marriott International, Inc. ("Marriott") and Starwood Hotels & Resorts Worldwide, LLC ("Starwood" or collectively, "Respondents").

The proposed consent order ("Proposed Order") has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement, along with any comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the Proposed Order.

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. On or about November 16, 2015, Marriott announced that it would acquire Starwood, and on or about September 23, 2016, 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 more than 1.1 million hotel rooms, accounting for one out of every fifteen hotel rooms worldwide.

After 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 Marriott and Starwood. Additionally, Marriott commenced a two-year process to integrate some Starwood systems into the Marriott network. Marriott fully integrated those Starwood systems into its own network by December 2018.

According to the FTC's Complaint, Respondents suffered at least three (3) distinct data security breaches over the course of several years. Starwood informed customers of the first breach just four days after the announcement of Marriott's acquisition of Starwood. This breach allowed intruders to compromise Starwood's point-of-sale systems and gain access to more than 40,000 customer payment cards over the course of 14 months.

The second breach began on or around July 28, 2014, and involved a breach of a Starwood guest reservation database. This breach went undetected for four years—during which Marriott had responsibility for Starwood's information security practices and network following the acquisition. Forensic examiners, retained by Marriott in September 2018, identified similar failures that resulted in the first breach, including: inadequate firewall controls, unencrypted payment card information stored outside of the secure cardholder data environment, lack of multifactor authentication, and inadequate monitoring and logging practices. As a result of the second breach, intruders compromised the personal information of 339 million Starwood guest records and 5.25 million unencrypted passport numbers worldwide. Additional compromised information from the Starwood guest reservation database included: names, dates of birth, payment card numbers, addresses, email addresses, telephone numbers, usernames, Starwood loyalty numbers, and partner loyalty program numbers.

As to the third breach, 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 The intruders began accessing and exporting consumers' personal information without detection from September 2018—the same month that Marriott became aware of the second breach—to December 2018 and resumed in January 2020 and continued until they were ultimately discovered in February 2020. The intruders were able to access more than 5.2 million guest records, including 1.8 million records related to U.S. consumers, that contained significant amounts of personal information, including: names, mailing addresses, email addresses, phone numbers, affiliated companies, gender, month and day of birth, Marriott loyalty account information, partner loyalty program numbers, and hotel stay and room preferences. Marriott's internal investigation confirmed that the malicious actors' main purpose for searching, accessing, and exporting guest records was to identify loyalty accounts with sufficient loyalty points to be either used or redeemed, including for booking stays at hotel properties.

The Commission's proposed two-count complaint alleges that Respondents violated Section 5(a) of the FTC Act by: (1) deceiving customers by representing in each of their privacy policies that they used reasonable and appropriate safeguards to protect consumers' personal and financial information; and (2) failing to employ reasonable security measures to protect consumers' personal information. With respect to these counts, the proposed complaint alleges that Respondents:

- failed to implement appropriate password controls, which resulted in employees often using default, blank or weak passwords;
- failed to patch outdated software and systems in a timely manner;
- failed to adequately monitor and log network environments, limiting the ability to detect malicious actors and distinguish between authorized and unauthorized activity;
- failed to implement appropriate access controls;
- failed to implement appropriate firewall controls;
- failed to implement appropriate network segmentation to prevent attackers from moving freely across its networks and databases; and
- failed to apply adequate multifactor authentication to protect sensitive information.

The proposed complaint alleges, with respect to the second count above, that Respondents' failure to employ reasonable security measures to protect consumers' personal information caused, or is likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by

consumers themselves. Such practices constitute unfair acts or practices under Section 5 of the FTC Act.

Summary of the Proposed Order with Respondents

The Proposed Order contains injunctive relief designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

Part I prohibits Respondents from misrepresenting in any manner, expressly or by implication: (1) Respondents' collection, maintenance, use, deletion, or disclose consumers' personal information; and (2) the extent to which Respondents protect the privacy, security, availability, confidentiality, or integrity of consumers' personal information.

Part II requires that Respondents establish, implement, and document a comprehensive information security program. The program must include specific safeguards tailored to Respondents' previous data security shortcomings.

Parts III-VI require Respondents to obtain initial and biennial information security assessments by an independent, third-party professional for 20 years (Part III), cooperate with the independent assessor (Part IV), provide the Commission with a certification of compliance with the Order from Respondents' CEO (Part V), and submit reports to the Commission if they suffer additional data incidents (Part VI).

Part VII requires Respondents to provide a Clear and Conspicuous method by which U.S. consumers can request that Respondents review the deletion of personal information associated with an email address and/or Loyalty Rewards Program account number.

Part VIII requires Respondents to provide a link on their website and mobile app where all U.S. consumers may request deletion of Personal Information associated with an email address and/or Loyalty Rewards Program account number.

Parts IX-XII are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance.

Part XIII states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the Proposed Order, and it is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify the Proposed Order's terms in any way.