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 tfirst
cquisition of Starwood. This
f-sale systems and gain access to
f 14 months.

, and involved a breach of a
etected for four years—during which
rity practices and network following
September 2018, identified similar
te firewall controls, unencrypted
older data environment, lack of
ogging practices. As a result of the
tion of 339 million Starwood guest
ldwide. Additional compromised
ncluded: names, dates of birth,
e numbers, usernames, Starwood

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;

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 in4 T (e)-2 (d O)-3 ()2 (TJ-34.74 -1.24 Td[ei(e)-1 ((ont)3 Be)]me02 Tc 01 (iTd[(t)3 Bni(ch)1ie)]r d O)-c)