

<p>DISTRICT COURT, CITY AND COUNTY OF DENVER, COLORADO 1437 Bannock Street Denver, CO 80202</p> <hr/> <p>STATE OF COLORADO, <i>ex rel</i> PHILIP J. WEISER, ATTORNEY GENERAL, Plaintiff</p> <p>v.</p> <p>MARRIOTT INTERNATIONAL, INC., a corporation, Defendants</p>	<p style="text-align: center;">^ COURT USE ONLY ^</p>
<p>PHILIP J. WEISER, Attorney General LAUREN DICKEY, First Assistant Attorney General JILL M. SZEWCZYK, Assistant Attorney General Ralph L. Carr Colorado Judicial Center 1300 Broadway, Floor Denver, CO 80203 Telephone: 720-508-6217 E-Mail: Jill.Szewczyk@coag.gov</p>	<p>Case No.</p>
<p>STIPULATED CONSENT JUDGMENT</p>	

1 Plaintiff, the State of Colorado as more particularly described in Paragraph 1
2 below (“Plaintiff”), appearing through its attorney, Philip J. Weiser, Attorney
3 General of the State of Colorado,¹ and Defendant Marriott International, Inc., a

¹ Defendant is simultaneously entering into similar agreements with the Attorneys General or appropriate representatives of the States of Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New

1 corporation, appearing through its attorney, Phyllis Sumner of King & Spalding
2 LLP, having stipulated to the entry of this Final Judgment on Stipulation and
3 Order (“Judgment”) by the Court without the taking of proof and without trial or
4 adjudication of any fact or law, without this Judgment constituting evidence of or
5 an admission by the Defendant, regarding any issue of law or fact alleged in the
6 Complaint on file, and without the Defendant admitting any liability, and with all
7 parties having waived their right to appeal, and the Court having considered the
8 matter and good cause appearing:

9 IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

I. PARTIES AND JURISDICTION

- 10 1. The Plaintiff in this case is The State of Colorado.
- 11 2. The Defendant in this case is Marriott International, Inc., a
12 corporation incorporated under the law of the State of Delaware with its
13 principal office located at 7750 Wisconsin Ave., Bethesda, Maryland 20814.
14 “Marriott” shall mean Marriott International, Inc. and its U.S. subsidiaries
15 and successors that collect, store, or process PERSONAL INFORMATION
16 provided, however, for the avoidance of doubt, “Marriott” shall not include
17 any MARRIOTT FRANCHISED HOTEL. “Starwood” shall mean Starwood

Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming and the District of Columbia.

1 Hotels & Resorts Worldwide, LLC, its subsidiaries and successors that
2 collect, store, or process PERSONAL INFORMATION. “Marriott” shall
3 include “Starwood” unless specifically stated otherwise.²

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

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

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

15 II. DEFINITIONS

16 6. “COMPENSATING CONTROL” or “COMPENSATING
CONTROLS” shall mean one or more alternative mechanisms that are put in

² Prior to November 15, 2015, Starwood was a separate corporation with its principal office located at One Starpoint, Stamford, CT 06902.

1 place to satisfy the requirement for a security measure that is determined by
2 the Chief Information Security Officer (or his or her appropriate designee) to
3 be impractical to implement at the present time due to legitimate technical or
4 business constraints. Such alternative mechanisms must (a) meet the intent
5 and rigor of the original stated requirement; (b) provide a similar level of
6 security as the original stated requirement; (c) be up to date with current
7 industry-accepted security protocols; and (d) be commensurate with the
8 additional risk imposed by not adhering to the original stated requirement.

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

16 8. “CONSUMER PROTECTION LAW” shall mean the citation for
17 the State of Colorado set forth in Appendix A attached hereto.

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

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

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

1 12. “CRITICAL IT VENDOR” shall mean a third party that
2 provides managed services that are a significant component of the
3 Information Security Program and has direct access to: (a) MARRIOTT
4 ASSETS or (b) COVERED DATABASES, including those outsourced to a
5 cloud computing service provider.

6 13. “DATA BREACH NOTIFICATION LAW” shall mean the
7 citation for the State of Colorado set forth in Appendix A attached hereto.

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

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

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

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

5 18. “LOYALTY REWARDS PROGRAM” shall mean the Marriott
6 Bonvoy program (or such name as it may be known in the future) offered by
7 Marriott that allows CONSUMERS to earn and redeem points for certain
8 goods or services according to and subject to the terms of such program. The
9 term “LOYALTY REWARDS PROGRAM” shall not be construed as creating
10 any property rights for enrolled CONSUMERS.

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

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

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

6 a. First name or first initial and last name in combination
7 with one or more of the following data elements that relate to such
8 CONSUMER: (i) Social Security number; (ii) state or federal issued
9 identification number, including driver’s license number, passport
10 number, or military identification number; (iii) financial account
11 number or credit or debit card number in combination with any
12 required security code, access code, or password that would permit
13 access to the CONSUMER’s financial account; or

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

17 c. Any other “Personal Information” as defined by the DATA
18 BREACH NOTIFICATION LAWS as of the EFFECTIVE DATE.

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

4 22. “PERSONAL INFORMATION PROTECTION LAW” shall
5 mean the citation for the State of Colorado set forth in Appendix A attached
6 hereto.

7 23. “REPORTABLE INCIDENT” means a SECURITY EVENT
8 that triggers a notification obligation under a DATA BREACH
9 NOTIFICATION LAW.

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

15 25. “STARWOOD DATA BREACH” shall refer to the incident
16 announced by Marriott on November 30, 2018 in which a person or persons
17 gained unauthorized access to Starwood’s reservation database and
18 subsequently exported data from certain tables, involving approximately one-
19 hundred thirty-one million five-hundred thousand (131,500,000) guest
20 records pertaining to customers associated with the United States, some of

1 which included contact information, gender, dates of birth, payment card
2 information, passport numbers, legacy Starwood Preferred Guest
3 information, reservation information, and hotel stay preferences.

4 26. “UNAUTHORIZED ACCOUNT ACCESS INCIDENTS” shall
5 refer to the incident(s) announced by Marriott on March 31, 2020 and in June
6 2020 in which a person or persons used the login credentials of certain
7 Marriott franchise property employees to inappropriately access information
8 regarding approximately five million five-hundred thousand (5,500,000) guest
9 records, some of which included contact information, gender, dates of birth,
10 loyalty account information, and hotel stay preferences.

III. INJUNCTIVE RELIEF

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

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

1 COMPLIANCE WITH LAW

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

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

10 INFORMATION GOVERNANCE

11 31. **Board Committee:** Marriott shall maintain a committee of
12 the Board of Directors³ (“Board Committee”) that shall assist the Board in
13 providing oversight of Marriott’s information security program (“Information
14 Security Program”). The Board Committee shall meet not less than four (4)
15 times per year.

16 32. On or before December 31, 2024, and annually thereafter, the
17 Board Committee shall acknowledge in its minutes that it has received the

³ As of March 15, 2021, Marriott included such a committee in its charter, entitled the Technology and Information Security Oversight Committee.

1 materials and presentations required by this Judgment and the minutes
2 shall include a list or description of such materials and presentations.

3 **33. Chief Information Security Officer:** Marriott shall employ
4 an executive or officer who shall be responsible for implementing,
5 maintaining, and monitoring the Information Security Program (hereinafter
6 referred to as the “Chief Information Security Officer”). The Chief
7 Information Security Officer shall have the education, qualifications, and
8 experience appropriate to the level, size, and complexity of the role in
9 implementing, maintaining, and monitoring the Information Security
10 Program. This Chief Information Security Officer (or his or her appropriate
11 designee) shall:

12 a. Report to the Board Committee on Marriott’s risk
13 assessment(s) and Information Security Program;

14 b. Report to the Board of Directors regarding Marriott’s
15 Information Security Program;

16 c. Report to the Chief Executive Officer within forty-eight
17 (48) hours of determining that a SECURITY EVENT both (i) involves
18 the PERSONAL INFORMATION on MARRIOTT ASSETS of one
19 thousand (1,000) or more CONSUMERS and (ii) there is reasonable
20 likelihood that the PERSONAL INFORMATION has been accessed or

1 acquired by an unauthorized third party. In the event that the Chief
2 Executive Officer is not a member of the Board of Directors, any
3 reports made pursuant to this subparagraph shall also be reported to a
4 designated member of the Board Committee by the Chief Information
5 Security Officer unless otherwise reported to the Board Committee or
6 the Board of Directors by the General Counsel; and

7 d. Inform the Board Committee at its regularly scheduled
8 meeting time of all REPORTABLE INCIDENTs.

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

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

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

13 **INFORMATION SECURITY PROGRAM**

14 **INFORMATION SECURITY PROGRAM: GENERAL**

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

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

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

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

17 40. Marriott shall enforce the policies and procedures required by
18 this Judgment. Marriott shall monitor for non-compliance and undertake

1 remedial measures for non-compliance as appropriate and without
2 unreasonable delay.

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

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

10 ***INFORMATION SECURITY PROGRAM: RISK ASSESSMENT AND***
11 ***ANALYSIS***

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

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

- 1 b. An assessment of safeguards in place to control these
2 risks;
- 3 c. The evaluation and adjustment of the Information
4 Security Program in light of the results of such testing and monitoring;
- 5 d. The implementation of reasonable safeguards to control
6 these risks; and
- 7 e. Documentation of safeguards implemented in response to
8 such annual Risk Assessments.

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

13 45. **Risk Assessment Method:** Marriott shall develop a risk
14 assessment method by utilizing method(s) published by a nationally
15 recognized security body and shall include the risk assessment criterion of
16 “harm to others” as a component of the magnitude of impact analysis as well
17 as the likelihood of that impact (“Risk Assessment Method”). Marriott shall
18 document the Risk Assessment Method including (i) the selection of
19 method(s), (ii) criteria, and (iii) what Marriott has established as the

1 acceptable risk threshold(s). Marriott, as it deems appropriate, may modify
2 the Risk Assessment Method, but shall document the change and the
3 rationale for the change.

4 46. **Risk Analysis – Applicability:** When analyzing risk to
5 determine implementation, maintenance, and compliance with the specific
6 requirements of the Information Security Program at Paragraphs 37 through
7 78 and Integration at Paragraphs 81 through 85, which incorporate the
8 Definitions as set forth in Paragraphs 6 through 26 of this Judgment,
9 Marriott shall perform such analysis consistent with a risk-based analysis
10 performed in accordance with the applicable Risk Assessment Method
11 selected at Paragraph 45.

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

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

5 ***INFORMATION SECURITY PROGRAM: VENDOR OVERSIGHT***

6 49. **Vendor Management:** Marriott shall develop, implement, and
7 maintain written, risk-based policies and procedures for overseeing a
8 Marriott vendor that has access to (i) MARRIOTT ASSETS, (ii) PERSONAL
9 INFORMATION provided by or obtained by the vendor on behalf of Marriott,
10 or used at the direction of Marriott for the benefit of Marriott, or (iii)
11 COVERED DATABASES (“relevant vendor”). These policies and procedures
12 shall include a process for including in contracts with a relevant vendor
13 executed or amended after the EFFECTIVE DATE: (a) requirements
14 appropriate to the service provided by the relevant vendor to implement and
15 maintain security safeguards; (b) periodic evaluations of the relevant
16 vendor’s cybersecurity practices; (c) a requirement that a relevant vendor
17 notifies Marriott promptly after discovering a SECURITY EVENT or
18 REPORTABLE INCIDENT; and (d) a requirement that a relevant vendor
19 notifies Marriott of a compromise of the relevant vendor’s systems that
20 compromise MARRIOTT ASSETS or COVERED DATABASES.

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

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

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

14 c. Permitting access to, or collection, retention,
15 transmission, use and storage of PERSONAL INFORMATION or any
16 of the COVERED DATABASES by the CRITICAL IT VENDOR only to
17 provide the contractually agreed upon services; and

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

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

4 ***INFORMATION SECURITY PROGRAM: MARRIOTT FRANCHISED***
5 ***HOTELS***

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

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

1 ***INFORMATION SECURITY PROGRAM: CHANGE CONTROL***

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

8 ***INFORMATION SECURITY PROGRAM: OTHER***

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

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

1 ***INFORMATION SECURITY PROGRAM:***

2 ***PERSONAL INFORMATION SAFEGUARDS AND CONTROLS***

3 **GENERAL**

4 57. **Minimum Extent Necessary:** The Information Security
5 Program shall include or incorporate written policies and procedures that are
6 modified as appropriate to require reasonable efforts to collect, use, share,
7 and retain PERSONAL INFORMATION to the minimum extent necessary to
8 satisfy legitimate business need or legal requirements.

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

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

1 ***INFORMATION SECURITY PROGRAM: SPECIFIC TECHNICAL***

2 ***SAFEGUARDS AND CONTROLS***

3 60. **Access Controls and Account Management - General:**

4 Marriott shall develop, implement, and maintain risk-based access controls,
5 where access is to MARRIOTT ASSETS or to COVERED DATABASES. Such
6 controls will be role-based, including for individual accounts, administrator
7 accounts, service accounts, or vendor accounts.

8 61. **Access Controls and Account Management – Specific:** For

9 the access controls and account management required by Paragraph 60
10 above:

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

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

17 c. Marriott shall implement enhanced measures for
18 administrator-level passwords, such as ENCRYPTION, using a

1 password vault, privileged access management solution, or measures of
2 similar efficacy.

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

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

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

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

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

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

14 63. **Threat Management:** Marriott shall develop, implement, and
15 maintain a threat management program that shall include the use of
16 automated tools to continuously monitor MARRIOTT ASSETS and
17 COVERED DATABASES for active threats. Marriott shall use reasonable
18 measures to develop the initial configuration of these tools, monitor for
19 updates, and make configuration changes and updates. Marriott shall use
20 information from these tools to support its security updates and patch

1 management program and in conjunction with its incident response plan to
2 address threats that pose an unreasonable risk to MARRIOTT ASSETS or
3 COVERED DATABASES.

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

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

1 **66. Intrusion Detection and Prevention:** Marriott shall
2 develop, implement, and maintain intrusion prevention and detection
3 systems, endpoint protection systems, threat monitoring systems, or similar
4 technologies reasonably designed to detect and restrict unauthorized access
5 to MARRIOTT ASSETS or COVERED DATABASES.

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

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

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

1 70. Vulnerability Management:

2 a. Marriott shall develop, implement, and maintain a
3 vulnerability management program reasonably designed to continually
4 identify and assess vulnerabilities of MARRIOTT ASSETS or
5 COVERED DATABASES by: (i) discovering vulnerabilities identified
6 by reputable outside sources; (ii) assigning risk rankings to new
7 vulnerabilities; (iii) running internal and external network
8 vulnerability scans at least quarterly or after any significant change to
9 MARRIOTT ASSETS or COVERED DATABASES; and (iv) performing
10 re-scans to ensure that previously identified vulnerabilities have been
11 properly remediated.

12 b. Marriott shall develop, implement, and maintain a risk-
13 based testing program reasonably designed to identify and assess
14 security vulnerabilities of MARRIOTT ASSETS or COVERED
15 DATABASES. This program shall include an appropriate schedule of
16 risk-based tests including internal and external penetration testing,
17 segmentation testing, and web application penetration testing to be
18 performed on MARRIOTT ASSETS or COVERED DATABASES that
19 adequately takes into account security risk. Such testing shall not be

1 less than annual and shall include retests where necessary to confirm
2 appropriate remediation.

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

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

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

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

14 74. **Digital Certificates:** Marriott shall use a digital certificate
15 management tool or service to inventory digital certificates. A digital
16 certificate for the purposes of this paragraph shall include a security token,
17 biometric identifier, or a cryptographic key used to protect externally facing
18 systems and applications.

19 75. **Data Loss Prevention:** Marriott shall develop, implement,
20 and maintain a process designed to detect and restrict unauthorized or

1 inadvertent transmission of PERSONAL INFORMATION from MARRIOTT
2 ASSETS.

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

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

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

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

13 **FULL IMPLEMENTATION**

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

1 or having the right in the event of dissolution to fifty (50) percent or
2 more of the assets of the entity; or (ii) having the contractual power
3 presently to designate fifty (50) percent or more of the directors of a
4 for-profit or not-for-profit corporation, or fifty (50) percent or more of
5 the trustees in the case of trusts that are irrevocable and/or in which
6 the settlor does not retain a reversionary interest.

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

18 82. **Post-Acquisition Plan:** Marriott shall create a plan and
19 timeline to address gaps and deficiencies identified by Marriott in the Post-
20 Acquisition Assessment when comparing the Acquired Entity’s information

1 security program with the Information Security Program. Where Marriott
2 acquires assets that will become MARRIOTT ASSETS through a transaction
3 that does not constitute an acquisition of an Acquired Entity pursuant to
4 Paragraph 81, Marriott may create a plan to address gaps and deficiencies
5 identified by Marriott in a risk analysis conducted consistent with Paragraph
6 46. The initial timeline for addressing such gaps and deficiencies in either the
7 acquisition of an Acquired Entity or assets shall be no longer than eighteen
8 (18) months following the closing of an acquisition.

9 83. Marriott may integrate or connect any asset or assets acquired
10 in a transaction described in Paragraph 81 or 82 of this Judgment for use in a
11 production environment of any of the MARRIOTT ASSETS at such time that
12 the applicable asset or assets comply with the Information Security Program.

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

16 85. **Documentation Requirements:** Marriott shall document its
17 efforts to comply with the requirements set forth in Paragraphs 81 through
18 84 of this Judgment.

1 **THIRD-PARTY INFORMATION SECURITY ASSESSMENTS**

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

9 a. The Assessor must be highly qualified and well
10 experienced. This shall mean that, at a minimum, the Assessor must
11 be a Certified Information Systems Security Professional (“CISSP”) or
12 a Certified Information Systems Auditor (“CISA”), or a similarly
13 qualified person or organization, and have at least five (5) years of
14 experience evaluating the effectiveness of computer system security or
15 information system security. In the event that Marriott obtains
16 approval to engage an Assessor from the Federal Trade Commission
17 pursuant to the FTC ORDER, Marriott shall be deemed to have
18 satisfied this requirement. In the event that the Federal Trade
19 Commission pursuant to the FTC ORDER rejects an Assessor,
20 Marriott shall not engage such Assessor for this Judgment.

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

15 c. The Third-Party Assessment shall:

16 i. Determine whether Marriott has implemented and
17 maintained the Information Security Program;

18 ii. Assess the effectiveness of Marriott’s
19 implementation and maintenance of the Information Security
20 Program;

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

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

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

17 d. The Assessor's Report must be completed within a
18 reasonable period of time after each Third-Party Assessment ends and
19 must be signed by the Assessor, stating that the Assessor conducted an

1 independent review of the Information Security Program and did not
2 rely primarily on assertions or attestations by Marriott's management.

3 e. Following the completion of the Third-Party Assessment
4 and receipt of the Assessor's Report, the Chief Information Security
5 Officer (or his or her designee) or General Counsel (or his or her
6 designee) shall present the Assessor's findings to the Board Committee
7 at its next regularly scheduled meeting.

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

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

1
2 **Reports**

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

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

12 b. On the first day of the seventh month following the
13 EFFECTIVE DATE, Marriott shall provide a progress report (i)
14 confirming the implementation of the policies and procedures required
15 by the Information Security Program and (ii) providing the status of
16 the implementation of the Listed Provisions. The progress report shall
17 provide the status of Marriott’s efforts to fully implement each
18 provision of the Listed Provisions to include (i) whether or not the
19 provision is fully implemented and, if not, the projected date of full
20 implementation, (ii) whether or not all necessary underlying risk
21 analyses have been performed and, if not, a schedule of performing the

1 remaining risk analyses, and (iii) a high-level description of the
2 changes made during the quarter in furtherance of achieving full
3 implementation.

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

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

11 89. The Third-Party Assessments, the Assessor's Reports, the
12 Quarterly Reports and all information contained therein shall be treated by
13 the Plaintiff as confidential to the extent permitted by the laws of the State of
14 Colorado; shall not be shared or disclosed except as provided herein; and
15 shall be treated by the Plaintiff as exempt from disclosure as permitted under
16 the relevant public records laws of the State of Colorado. In the event that
17 the Plaintiff receives any request from the public for the Third-Party
18 Assessments, the Assessor's Reports, the Quarterly Reports or other
19 confidential documents under this Judgment and believes that such
20 information is subject to disclosure under the relevant public records laws,

1 the Plaintiff agrees to provide Marriott with at least ten (10) days advance
2 notice before producing the information, to the extent permitted by state law
3 (and with any required lesser advance notice), so that Marriott may take
4 appropriate action to defend against the disclosure of such information. The
5 notice under this paragraph shall be provided consistent with the notice
6 requirements contained in Paragraph 111. Nothing contained in this
7 subparagraph shall alter or limit the obligations of the Plaintiff that may be
8 imposed by the relevant public records laws of the State of Colorado, or by
9 order of any court, regarding the maintenance or disclosure of documents and
10 information supplied to the Plaintiff.

11 **CONSUMER-RELATED RELIEF**

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

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

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

16 c. Nothing in subparagraph (b) shall abrogate Marriott's
17 rights to: (i) avail itself of any and all rights, exceptions, and
18 exemptions existing under any state or federal law or (ii) retain a
19 subset of a CONSUMER's information to comply with its legal,
20 regulatory, or other obligations. Marriott is not obligated to comply

1 with the requirements under subparagraph (b) when the requirements
2 conflict with Marriott's ability to comply with federal, state, or local
3 laws or regulations; any civil, criminal, or regulatory inquiry,
4 investigation, subpoena, or summons by federal, state, local or other
5 governmental authorities; or any transactional, tax, escheatment,
6 corporate accountability, or other legitimate business need compatible
7 with the context in which the CONSUMER provided the information.

8 91. Loyalty Rewards Program Review:

9 Marriott shall:

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

19 b. In the event of a SECURITY EVENT specifically
20 involving the unauthorized use of authentication credentials for

1 CONSUMER LOYALTY REWARDS PROGRAM account(s), timely
2 undertake reasonable steps to determine if any suspicious or
3 unauthorized activity has occurred in CONSUMER LOYALTY
4 REWARDS PROGRAM account(s).

5 c. Following any review pursuant to subparagraph (91.a) or
6 (91.b) above, in the event that Marriott determines that suspicious or
7 unauthorized activity by a third party resulted in any reduction of
8 points associated with a CONSUMER's LOYALTY REWARDS
9 PROGRAM account, unless Marriott determines that the CONSUMER
10 violated the terms of use of the LOYALTY REWARDS PROGRAM,
11 Marriott shall restore the reduced points in the relevant
12 CONSUMER's LOYALTY REWARDS PROGRAM account.

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

17 93. **Consumer Transparency:**

18 a. Marriott shall continue to provide for CONSUMERS a
19 link to its consumer privacy policy on the U.S. homepage of its website
20 and in its U.S. version of its mobile application. The policy shall

1 continue to be provided in a manner that is: (i) in readily
2 understandable language and syntax, and (ii) in a type size, font, color,
3 appearance, and location sufficiently noticeable for a CONSUMER to
4 read and comprehend it, and, at a minimum, in a print that contrasts
5 with the background against which it appears.

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

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

10 ii. How Marriott collects the PERSONAL
11 INFORMATION;

12 iii. How Marriott uses the PERSONAL
13 INFORMATION;

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

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

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

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

IV. **DOCUMENT RETENTION**

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

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

5 b. Written complaints either received by Marriott's Global
6 Privacy Office directly from CONSUMERS through the dedicated
7 Marriott privacy email address published on Marriott's Group Global
8 Privacy Statement (privacy@marriott.com) or received by Marriott
9 indirectly from a Consumer Protection Agency pursuant to Paragraph
10 94, and any written response;

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

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

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

18 96. Marriott shall maintain all materials the Assessor relied upon
19 to conduct the Third-Party Assessment to the extent identified by the

1 Assessor in the Assessor's Report, that are in the possession of Marriott,
2 whether prepared by or on behalf of Marriott, including all plans, reports,
3 studies, reviews, audits, audit trails, policies, training materials, and
4 assessments, and any other materials concerning Marriott's compliance with
5 related provisions of this Judgment for a period of five (5) years from the date
6 of the delivery of the Assessor's Report pursuant to Paragraph 86.d.

V. MONETARY PAYMENT

7 97. No later than thirty (30) days after the EFFECTIVE DATE,
8 Marriott shall pay the sum of Fifty-Two Million Dollars (\$52,000,000.00) to
9 be divided by and among the participating states⁴ and paid by Marriott directly to
10 the Plaintiff in the amount designated in sub-paragraph (a).

11 a. Out of the sum in this paragraph, Marriott shall pay to the
12 Plaintiff Eight hundred and twenty-two thousand four hundred and
13 thirty-five Dollars (\$822, 435.).

14 b. All payments to the Colorado Attorney General under this
15 paragraph are to be held, along with any interest thereon, in
16 trust by the Attorney General to be used in the Attorney
17 General's sole discretion for reimbursement of the State's actual

⁴ *Supra*, note 1.

1 costs and attorneys' fees, the payment of restitution, if any, and
2 for future consumer fraud or antitrust enforcement, consumer
3 education, or public welfare purposes.

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

9 d. Costs or expenditures incurred by Marriott to implement
10 the provisions of Section III and Section IV of this Judgment are
11 costs to come into compliance with the laws alleged by Plaintiff
12 to have been violated. For the avoidance of doubt, neither the
13 Plaintiff nor Marriott makes any warranty or representation as
14 to the tax consequences of such costs or expenditures incurred
15 by Marriott to implement the provisions of Section III and
16 Section IV of this Judgment. Additionally, Plaintiff does not
17 make any warranty or representation and has not agreed to the
18 amount of costs or expenditures appropriate for Marriott to
19 implement the provisions of Section III and Section IV.

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

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

VI. **RELEASE**

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

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

16 a. Any criminal liability that any person or entity, including
17 Marriott, has or may have to the States; and

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

5 i. State or federal antitrust violations;

6 ii. State or federal securities violations; or

7 iii. State or federal tax claims.

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

VII. NO ADMISSION OF LIABILITY

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

16 104. Nothing contained in this Judgment shall be construed as an
17 admission or concession of liability by Marriott, nor to any express or implied

1 allegations relating to current or historical information security policies and
2 practices. Nothing contained in this Judgment shall be construed to create
3 any third-party beneficiary rights or give rise to or support any right of action
4 in favor of any CONSUMER or group of CONSUMERS or confer upon any
5 person other than the Plaintiff and Marriott any rights or remedies. By
6 entering into this Judgment, Marriott does not intend to create any legal or
7 voluntary standard of care and expressly denies that any practices, policies,
8 or procedures inconsistent with those set forth in this Judgment violate any
9 applicable legal standard. This Judgment is not intended to be and shall not
10 be construed as, deemed to be, represented as, or relied upon in any manner
11 by any party in any civil, criminal, or administrative proceeding before any
12 court, administrative agency, arbitration, or other tribunal as an admission,
13 concession, or evidence that Marriott has violated any federal, state, or local
14 law, or that Marriott's current or prior practices related to whether its
15 Information Security Program is or was not in accordance with any federal,
16 state, or local law.

VIII. GENERAL PROVISIONS

17 105. Nothing herein shall be construed to exonerate any failure to
18 comply with any provision of this Judgment after the EFFECTIVE DATE or
19 other date as applicable to the specific provision to compromise the authority

1 of the Plaintiff to initiate a proceeding for any failure to comply with this
2 Judgment, or to alter or modify any federal or state law as to the use or
3 enforcement of this Judgment.

4 106. Nothing in this Judgment shall be construed to limit the
5 authority or ability of the Plaintiff to protect the interests or the people of
6 Colorado. This Judgment shall not bar the Plaintiff or any other
7 governmental entity from enforcing laws, regulations, or rules against
8 Marriott for conduct subsequent to or otherwise not covered by this
9 Judgment. Further, nothing in this Judgment shall be construed to limit the
10 ability of the Plaintiff to enforce the obligations that Marriott has under this
11 Judgment, subject to the meet and confer requirements in Paragraph 113.

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

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

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

15 110. This Judgment shall not be construed to waive any claims of
16 sovereign immunity that Colorado may have in any action or proceeding.

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

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

4 Jill Szewczyk, Assistant Attorney General, Colorado Department of Law,
5 1300 Broadway, 10th Floor, Denver CO 80203, Jill.Szewczyk@coag.gov.

6 Lauren Dickey, First Assistant Attorney General, Consumer Fraud Unit,
7 Colorado Department of Law, 1300 Broadway, 10th Floor, Denver CO 80203,
8 Lauren.Dickey@coag.gov.

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

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

14 Rena Hozore Reiss, Executive Vice President and General Counsel, 7750
15 Wisconsin Avenue, Bethesda, MD 20814, OGC@marriott.com.

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

18 Marriott may update its designee and contact information by sending written notice

1 to the Plaintiff informing it of the change. In the event that Marriott does not have
2 a valid designee on file, the Plaintiff may send notice to Marriott's registered agent
3 or counsel of record in this Judgment to satisfy this requirement.

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

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

1 114. Nothing herein shall be construed to exonerate any failure to
2 comply with any provision of this Judgment, or to compromise the authority
3 of the Plaintiff to initiate a proceeding for any failure to comply with this
4 Judgment after receiving the response from Marriott described in Paragraph
5 113 above, the Plaintiff determines that an enforcement action is in the
6 public interest.

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

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

19 The clerk is ordered to enter this Judgment forthwith.

20

1 ORDERED AND ADJUDGED at Denver, Colorado this ____ day of _____,
2 2024.

3

4

5

Judge of the Superior Court

6

PLAINTIFF, STATE OF COLORADO

Philip J. Weiser
Attorney General

By: /s/ Lauren Dickey
Lauren Dickey
First Assistant Attorney General

Date: 10/9/2024

By: /s/ Jill Szewczyk
Jill Szewczyk
Assistant Attorney General II

Date: 10/9/2024

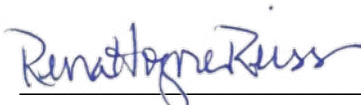
COUNSEL FOR DEFENDANT, MARRIOTT INTERNATIONAL, INC.

By:  _____

Date: October 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

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

MARRIOTT MULTISTATE APPENDIX A

STATE	CONSUMER PROTECTION LAWS	DATA BREACH NOTIFICATION & PERSONAL INFORMATION PROTECTION LAWS
AK - ALASKA	Unfair Trade Practices Act, Alaska Stat. 45.50.471, <i>et seq.</i>	Alaska Stat. 45.48.010, <i>et seq.</i>
AL - ALABAMA	Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-1, <i>et seq.</i>	Data Breach Notification Act of 2018, Ala. Code § 8-38-1, <i>et seq.</i>
AR - ARKANSAS	Arkansas Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101, <i>et seq.</i>	Arkansas Personal Information Protection Act, Ark. Code Ann. § 4-110-101, <i>et seq.</i>
AZ - ARIZONA	Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-1521, <i>et seq.</i>	Ariz. Rev. Stat. §§ 18-551 and 18-552
CO - COLORADO	Colorado Consumer Protection Act, C.R.S. §§ 6-1-101 <i>et seq.</i>	C.R.S. § 6-1-716 and C.R.S. § 6-1-713.5
CT- CONNECTICUT	Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110b, <i>et seq.</i>	Breach of Security, Conn. Gen. Stat. § 36a-701b; Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471
DC - DISTRICT OF COLUMBIA	Consumer Protection Procedures Act, D.C. Code §§ 28-3901, <i>et seq.</i>	District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851, <i>et seq.</i>
DE - DELAWARE	Consumer Fraud Act, 6 Del. C. §§ 2511 <i>et seq.</i>	Delaware Data Breach Notification Law, 6 Del. C. § 12B-100 <i>et seq.</i>
FL - FLORIDA	Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, §501.201 <i>et seq.</i> , Florida Statutes	Florida Information Protection Act, Section 501.171, Florida Statutes
GA - GEORGIA	Georgia Fair Business Practices Act, O.C.G.A. §§ 10-1-390 through 408	Georgia Personal Identity Protection Act, O.C.G.A §§ 10-1-910 through 915
HI - HAWAII	Uniform Deceptive Trade Practice Act, Haw. Rev. Stat. ch. 481A and Haw. Rev. Stat. § 480-2	Haw. Rev. Stat. ch. 487J and Haw. Rev. Stat. ch. 487N
IA - IOWA	Iowa Consumer Fraud Act, Iowa Code § 714.16	Personal Information Security Breach Protection Act, Iowa Code Chapter 715C
ID - IDAHO	Idaho Consumer Protection Act, Idaho Code §§ 48-601, <i>et seq.</i>	Idaho Code, Title 28, Chapter 51, , §28-51-103 <i>et seq.</i>
IL - ILLINOIS	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 <i>et seq.</i>	Illinois Personal Information Protection Act, 815 ILCS 530/1 <i>et seq.</i>
IN - INDIANA	Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5 <i>et seq.</i>	Disclosure of Security Breach Act, Ind. Code §§ 24-4.9 <i>et seq.</i>
KS - KANSAS	Kansas Consumer Protection Act, K.S.A §§ 50-623 <i>et seq.</i>	Security Breach Notification Act, K.S.A. §§ 50-7a01, <i>et seq.</i> ; The Wayne Owen Act, K.S.A. § 50-6,139b

MARRIOTT MULTISTATE APPENDIX A

KY - KENTUCKY	Kentucky Consumer Protection Act, KRS §§ 367.110-367.300, 367.990	KRS 365.732
LA - LOUISIANA	Unfair Trade Practices and Consumer Protection Law, La. R.S. §§ 51:1401, <i>et seq.</i>	Database Security Breach Notification Law, La. R.S. §§ 51:3071, <i>et seq.</i>
MA - MASSACHUSETTS	Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A	Mass. Gen. Laws ch. 93H; 201 Code Mass. Regs. 17.00 <i>et seq.</i>
MD - MARYLAND	Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101, <i>et seq.</i>	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law §§ 14-3501, <i>et seq.</i>
ME - MAINE	Maine Unfair Trade Practices Act, 5 M.R.S.A. §§ 205-A, <i>et seq.</i>	Maine Notice of Risk to Personal Data Act, 10 M.R.S.A. §§ 1346, <i>et seq.</i>
MI - MICHIGAN	Michigan Consumer Protection Act, MCL 445.901 <i>et seq.</i>	Identity Theft Protection Act, MCL 445.61, <i>et seq.</i>
MN - MINNESOTA	Uniform Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43-.48; Consumer Fraud Act, Minn. Stat. §§ 325F.68-.694	Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61 and Minnesota Health Records Act, Minn. Stat. § 144.291-144.34
MO - MISSOURI	Mo. Rev. Stat. §§ 407.010, <i>et seq.</i>	Mo. Rev. Stat. § 407.1500
MS - MISSISSIPPI	Mississippi Consumer Protection Act, Miss. Code §§ 75-24-1, <i>et seq.</i>	Miss. Code Ann. § 75-24-29
MT - MONTANA	Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. §§ 30-14-101 <i>et seq.</i>	Mont. Code Ann. §§ 30-14-1701 <i>et seq.</i>
NC - NORTH CAROLINA	North Carolina Unfair and Deceptive Trade Practices Act, N.C.G.S. §§ 75-1.1, <i>et seq.</i>	Identity Theft Protection Act, N.C.G.S. §§ 75-60, <i>et seq.</i>
ND - NORTH DAKOTA	Unlawful Sales or Advertising Practices, N.D.C.C. §§ 51-15-01 <i>et seq.</i>	Notice of Security Breach for Personal Information N.D.C.C. §§ 51-30-01 <i>et seq.</i>
NE - NEBRASKA	Nebraska Consumer Protection Act, Neb. Rev. Stat. §§ 59-1601 <i>et seq.</i>	Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 <i>et seq.</i>
NH - NEW HAMPSHIRE	New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann § 358-A:1, <i>et seq.</i>	N.H. Rev. Stat. Ann § 359-C: 19-21
NJ - NEW JERSEY	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 <i>et seq.</i>	New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166
NM - NEW MEXICO	New Mexico Unfair Practices Act, NMSA 1978, §§ 57-12-1 <i>et seq.</i>	Data Breach Notifications Act, NMSA 1978, Sections 57-12C-1 <i>et seq.</i>

MARRIOTT MULTISTATE APPENDIX A

NV - NEVADA	Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§ 598.0903 <i>et seq.</i>	Nev. Rev. Stat. §§ 603A.010-603A.290
NY - NEW YORK	Executive Law 63(12), General Business Law 349/350	General Business Law 899-aa and 899-bb
OH - OHIO	Ohio Consumer Sales Practices Act, R.C. § 1345.01, <i>et seq.</i>	R.C. §§ 1349.19 to 1349.192
OK - OKLAHOMA	Oklahoma Consumer Protection Act, 15 O.S. Section 751, <i>et seq.</i>	Oklahoma Security Breach Notification Act, 24 O.S. Section 161, <i>et seq.</i>
OR - OREGON	Oregon Unlawful Trade Practices Act, ORS 646.605, <i>et seq.</i>	Oregon Consumer Information Protection Act, ORS 646A.600, <i>et seq.</i>
PA - PENNSYLVANIA	Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, <i>et seq.</i>	Breach of Personal Information Notification Act, 73 P.S. §§ 2301, <i>et seq.</i>
RI - RHODE ISLAND	Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws §§ 6-13.1-1, <i>et seq.</i>	Rhode Island Identity Theft Protection Act R.I. Gen. Laws §§ 11-49.3-1, <i>et seq.</i>
SC - SOUTH CAROLINA	South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5-10, <i>et seq.</i>	South Carolina Data Breach Notification Law, S.C. Code Ann. § 39-1-90
SD - SOUTH DAKOTA	SDCL Chapter 37-24	SDCL Chapter 22-40
TN - TENNESSEE	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 to -135	Tennessee Identify Theft Deterrence Act of 1999, Tenn. Code Ann. §§ 47-18-2101 to -2111
TX - TEXAS	Texas Deceptive Trade Practices – Consumer Protection Act, Tex. Bus. & Com. Code Ann. §§ 17.41 – 17.63	Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. § 521.001 - 521.152
UT - UTAH	Utah Consumer Sales Practices Act Utah Code §§ 13-11-1, <i>et seq.</i>	Utah Protection of Personal Information Act, Utah Code §§ 13-44-101, <i>et seq.</i>
VA - VIRGINIA	Virginia Consumer Protection Act, Virginia Code §§ 59.1-196 through 59.1-207	Virginia Breach of Personal Information Notification Law, Virginia Code § 18.2-186.6
VT - VERMONT	Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 <i>et seq.</i>	9 V.S.A §§ 2430, 2431, and 2435
WA - WASHINGTON	Washington Consumer Protection Act, RCW 19.86.010 <i>et seq.</i>	Washington Data Breach Notification Law, RCW 19.255.005 <i>et seq.</i>
WI - WISCONSIN	Wis. Stat. § 100.18(1)	Wis. Stat. § 134.98
WV - WEST VIRGINIA	W. Va. Code §§ 46A-1-101, <i>et seq.</i>	W. Va. Code §§ 46A-2A-101 <i>et seq.</i>
WY - WYOMING	Wyoming Consumer Protection Act, W.S. §§ 40-12-101 <i>et seq.</i>	W.S. §§ 40-12-501 <i>et seq.</i>