DISTRICT COURT, CITY AND COUNTY OF DENVER, COLORADO 1437 Bannock Street Denver, CO 80202 STATE OF COLORADO, *ex rel* PHILIP J. WEISER, ATTORNEY GENERAL, Plaintiff v. MARRIOTT INTERNATIONAL, INC., a corporation, Defendant	▲ **COURT USE ONLY** ▲
PHILIP J. WEISER, Attorney General LAUREN M. DICKEY, #45773* First Assistant Attorney General JILL M. SZEWCZYK, #46902* GABRIAL LENNON, #58130 Assistant Attorneys General Ralph L. Carr Colorado Judicial Center 1300 Broadway, Floor Denver, CO 80203 Telephone: 720-508-6217 E-Mail: Jill.Szewczyk@coag.gov *Counsel of Record	Case No.
COMPLAINT	

Plaintiff, the State of Colorado (the "State" or the "Plaintiff"), appearing through Philip J. Weiser, Attorney General of Colorado, brings this action against Defendant Marriott International, Inc., a corporation, ("Marriott" or "Defendant") for violations of the Colorado Consumer Protection Act ("CCPA"), C.R.S. § 6-1-101-115, and the Colorado Personal Information Protection Act ("Information Protection Law"), C.R.S. § 6-1-713.5, and states as follows:

THE PARTIES

1. Plaintiff, the State of Colorado, by and through Attorney General Philip J. Weiser, is statutorily responsible for the enforcement of the Colorado Consumer Protection Act, C.R.S. §§ 6-1-101 – 115, and the Colorado Personal Information Protection Act, C.R.S. § 6-1-713.5, *See* C.R.S. § 6-1-103 (Attorney General is responsible for enforcing title 6, article 1 of the Colorado Revised Statutes).

2. Defendant Marriott International, Inc. ("Marriott") is a Delaware corporation with its principal office or place of business at 7750 Wisconsin Ave., Bethesda, Maryland 20814.

JURISDICTION AND VENUE

3. This enforcement action is brought by the Attorney General, in the name of the State of Colorado and in the public interest pursuant to the authority granted under C.R.S. 6-1-103. The Attorney General has reason to believe that Marriott may have engaged in violations of the Colorado Consumer Protection Act, C.R.S. §§ 6-1-101 – 115, and the Colorado Personal Information Protection Act, C.R.S. § 6-1-713.5.

4. Plaintiff has reason to believe that Marriott has caused and will cause injury, loss, and damage to the State of Colorado.

5. The court has jurisdiction over Marriott pursuant to C.R.S. § 13-1-124(1)(A) because at all times relevant to this Complaint, Marriott was engaged in trade and commerce affecting consumers in the State. Marriott was also in possession of the personal information of State residents.

6. Venue for this action properly lies in the District Court for the Second Judicial District to C.R.S. § 6-1-103 and C.R.C.P. 98(C)(1), because Marriott transacted business in the City and County of Denver and/or some of the transactions upon which this action is based occurred in Denver, Colorado.

7. Defendant agrees to waive notice as required by C.R.C.P. 3(a) and 4.

BACKGROUND

8. 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.

9. On or about November 16, 2015, Marriott announced that it would acquire Starwood Hotels and Resorts Worldwide, LLC ("Starwood") for $12.2 billion. Marriott's acquisition of Starwood closed the following year, on or about September 23, 2016, and 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 over 1.1 million hotel rooms, accounting for one out of every fifteen hotel rooms worldwide.

10. After the legal close of 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 itself and Starwood. Additionally, following the legal close of the acquisition, Marriott

commenced a two-year process to integrate some Starwood systems into the Marriott networks. Marriott fully integrated those Starwood systems into its own network in December 2018.

Starwood Data Breach

11. Despite having responsibility for Starwood's information security practices and network following the acquisition, Marriott failed to identify an ongoing breach within the Starwood network. In fact, Marriott did not detect this breach until September 7, 2018, nearly two years after the legal close of Marriott's acquisition of Starwood. The incident (hereinafter, the "Starwood Data Breach") was announced by Marriott on November 30, 2018.

12. Forensic examiners determined that, on or about July 28, 2014, malicious actors compromised Starwood's external-facing webserver, installing malware on its network. This malware allowed the intruders to perform network reconnaissance activities, harvest highly privileged Starwood administrative and user credentials, and use those credentials to move throughout Starwood's internal network for a four-year period, until Marriott's system finally detected an attempt to export consumer data from the guest reservation database on September 7, 2018.

13. Even after discovery of the breach, on September 10, 2018, the intruders exported additional guest information from Starwood's systems.

14. During this period spanning more than four years, from July 2014 to September 2018—including the two years following Marriott's acquisition of

Starwood and its integration of certain Starwood systems—the intruders went undetected, installing key loggers, memory-scraping malware, and Remote Access Trojans in over 480 systems across 58 locations within the Starwood environment. Those locations included a combination of corporate, data center, customer contact center, and hotel property locations.

15. Following the breach, a forensic examiner assessed Starwood's systems and identified failures, 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.

16. The Starwood Data Breach exposed the personal information of 339 million consumer records globally, including 131.5 million guest records pertaining to customers associated with the United States, some of which included contact information, gender, dates of birth, payment card information, passport numbers, legacy Starwood Preferred Guest information, reservation information, and hotel stay preferences.

Unauthorized Account Access Incidents

17. The information security failures detailed in this Complaint are not limited to Starwood's computer networks, systems, and databases.

18. 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 (hereinafter, the "Unauthorized Account Access Incidents").

19. The intruders began accessing and exporting consumers' personal information without detection from September 2018—the same month that Marriott became aware of the Starwood Data Breach—to December 2018 and resumed in January 2020 and continued until they were ultimately discovered in February 2020.

20. The intruders were able to access over 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.

21. 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 that could be used or redeemed, including for booking stays at hotel properties.

Defendant's Deceptive Information Security Statements

22. Prior to its acquisition, Starwood controlled and operated its website, www.starwood.com, where consumers could make reservations for hotel rooms.

23. Following the acquisition of Starwood, Marriott controlled and continued to operate the Starwood website until approximately May 2018 when Marriott merged Starwood's website into the Marriott website.

24. At all relevant times, the privacy policy posted on the Starwood website stated:

> **SECURITY SAFEGUARDS**: Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your personal data against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although "guaranteed security" does not exist either on or off the Internet, ***we safeguard your information using appropriate administrative, procedural and technical safeguards,*** including password controls, "firewalls" and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit. (emphasis added).

25. In addition to the Starwood website, Marriott operates its own Marriott-branded website, www.marriott.com, where consumers can make reservations for Marriott-branded hotels, as well as Starwood-branded hotels.

26. At all relevant times, the privacy policy posted on the Marriott website stated:

> "Personal Information" is information that identifies you as an individual or relates to an identifiable individual. We may collect Personal Information such as:
>
> Name[s] . . . home and work address[es], telephone number[s] and email address[es], your business title, date and place of birth, nationality,

> passport, visa or other government-issued identification information, guest stay information, including the hotels where you have stayed, date of arrival and departure, goods and services purchased, special requests made, information and observations about your service preferences (including room type, facilities, holiday preferences, amenities requested, ages of children or any other aspects of the Services used); . . . credit and debit card number; Marriott [] Rewards information online user accounts details, profile or password details and any frequent flyer or travel partner program affiliation . . .
>
> ***We seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization.*** Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section, below. (emphasis added).

Information Security Practices

27. Marriott and/or Marriott as successor to Starwood failed to provide reasonable or appropriate security for the personal information that they collected and maintained about consumers. Among other things, Marriott and/or Marriott as successor to Starwood:

a. Failed to patch outdated software and systems in a timely manner, leaving Starwood's network susceptible to attack;

b. Failed to adequately monitor and log network environments, limiting the ability to detect malicious actors and distinguish between authorized and unauthorized activity. This failure prevented Marriott and/or Marriott as successor to Starwood from detecting

intruders in its network and further prevented it from determining the information exfiltrated from its network;

c. Failed to implement appropriate access controls. For example, on numerous occasions, the accounts of former employees were not terminated in a timely manner, and separate unique accounts for users' remote access were not created;

d. Failed to implement appropriate firewall controls. This failure resulted in malicious actors making unauthorized connections from outside of Starwood's network;

e. Failed to implement appropriate network segmentation, which allowed intruders to move easily between Starwood hotel property systems and Starwood's corporate networks;

f. Failed to apply adequate multifactor authentication to protect sensitive information. For example, Starwood failed to comply with contractual obligations and/or internal policies requiring multifactor authentication for remote access to sensitive environments, including environments containing payment card data;

g. Failed to properly eradicate threats from the Starwood or Marriott environment after incidents, and failed to implement improvements based on lessons learned from previous incidents; and

h. Failed to implement appropriate password controls. As a result of this failure, employees often used default, blank, or weak passwords;

28. As a direct result of the failures described in Paragraph 27 above, between 2014 and 2020, malicious actors were able to gain unauthorized access to the personal information of millions of consumers, including passport information, payment card numbers, Starwood loyalty numbers, along with name, gender, date of birth, address, email address, telephone number, username, and hotel stay and other travel information.

COUNT ONE

Violations Of the Colorado Consumer Protection Act

(C.R.S. § 6-1-105(1)(rrr))

29. Plaintiff realleges and incorporates Paragraphs 1 through 28 as if fully set forth herein.

30. Defendant has, in the conduct of trade or commerce, engaged in false, misleading, or deceptive acts or practices, as set forth above, in violation of C.R.S. § 6-1-105(1)(rrr).

31. Defendant made false and misleading statements to consumers regarding its data protection practices which had the capacity, tendency or effect of deceiving or misleading consumers in violation of C.R.S. § 6-1-105(1)(rrr).

32. Defendant's failure to adequately inform consumers regarding its data protection practices constitutes a failure to state material facts, the omission of which

has deceived or tended to deceive consumers, as set forth above in violation of C.R.S. § 6-1-105(1)(rrr).

33. Defendant's failure to take reasonable steps to protect consumers' personal information and subsequent data breach caused substantial harm to consumers, that consumers could not reasonably avoid, and which did not benefit the marketplace or competition, making it an unfair trade practice in violation of C.R.S. § 6-1-105(1)(rrr).

COUNT TWO

Violations of the Colorado Personal Information Protection Act

(C.R.S. §§ 6-1-713.5)

34. Plaintiff realleges and incorporates Paragraphs 1 through 28 as if fully set forth herein.

35. Defendant collects, owns and/or licenses the personal information of consumers residing in Colorado.

36. Defendant has violated the Colorado Personal Information Protection Act, C.R.S. § 6-1-713.5 by failing to implement and maintain reasonable security measures to protect records that contain personal information concerning Colorado consumers from unauthorized access, use, modification, or disclosure.

37. Defendant's failure to take reasonable steps to protect consumers' personal information constitutes unfair or deceptive trade practices that violate the Colorado Personal Information Protection Act, C.R.S. § 6-1-713.5.

REMEDIES

44. Pursuant to C.R.S. § 6-1-110, Plaintiff is entitled to a Judgment providing injunctive relief against Defendant.

45. Pursuant to C.R.S. § 6-1-112, Plaintiff is entitled to a Judgment for Civil Penalties against Defendant.

46. Pursuant to C.R.S. § 6-1-113, "[c]osts and attorney fees shall be awarded to the attorney general … in all actions where the attorney general … successfully enforces this article." All payments to the Colorado Attorney General under this paragraph are to be held, along with any interest thereon, in trust by the Attorney General to be used in the Attorney General's sole discretion for reimbursement of the State's actual costs and attorneys' fees, the payment of restitution, if any, and for future consumer fraud or antitrust enforcement, consumer education, or public welfare purposes.

PRAYER FOR RELIEF

47. Plaintiff respectfully requests that this Court enter Judgment in favor of Plaintiff and against Defendant as outlined in the Stipulated Consent Judgment that is being filed simultaneously with this Complaint.

48. Plaintiff further requests that this Court grant all other relief to which Plaintiff is entitled.

Respectfully submitted,

PHILP J. WEISER
Attorney General

s/ Lauren M. Dickey
LAUREN M. DICKEY, # 45773*
First Assistant Attorney General
JILL M. SZEWCZYK, # 46902*
GABRIEL LENNON, # 58130*
Assistant Attorneys General
Counsel of Record*

Dated: 10/9/2024