IN THE CIRCUIT COURT OF FAULKNER COUNTY, ARKANSAS
CIVIL DIVISION

STATE OF ARKANSAS, *ex rel.*
TIM GRIFFIN, ATTORNEY GENERAL **PLAINTIFF**

v. **CASE NO. 23CV-24-_____**

MARRIOTT INTERNATIONAL, INC.,
a corporation **DEFENDANT**

COMPLAINT

Plaintiff, the State of Arkansas, *ex rel.* Tim Griffin, Attorney General, brings this action against Defendant Marriott International, Inc., a corporation, ("Marriott" or "Defendant") for violations of the Arkansas Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101 *et seq.*, ("ADTPA") and the Arkansas Personal Information Protection Act, Ark. Code Ann. § 4-110-101 *et seq.* ("APIPA").

I. PARTIES

1. Plaintiff is the State of Arkansas, *ex rel.* Tim Griffin, Attorney General, who is authorized to enforce the ADTPA and APIPA pursuant to Ark. Code Ann. §§ 4-88-104 and 4-88-113.

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.

II. JURISDICTION

3. This court has jurisdiction over this matter under Ark. Code Ann. §§ 4-88-104, 4-88-112, and 16-4-101 because Marriott has transacted business within the State of Arkansas at all times relevant to this Complaint and within the applicable statute of limitations.

4. Venue for this action properly lies in Faulkner County, Arkansas, under Ark. Code Ann. §§ 4-88-104, 4-88-112, and the common law of the State of Arkansas.

III. FACTUAL ALLEGATIONS

5. 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.

6. 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.

7. 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 Starwood and itself. 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.

A. Starwood Data Breach

8. 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.

9. 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.

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

11. 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.

12. 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.

13. 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.

B. Unauthorized Account Access Incidents

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

15. 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").

16. 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.

17. 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.

18. 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.

C. Defendant's Deceptive Information Security Statements

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

20. 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.

21. 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).

22. 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.

23. 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).

D. Information Security Practices

24. Marriott and 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 Marriott as successor to Starwood:

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

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 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 the Starwood 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 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.

25. As a direct result of the failures described in Paragraph 24 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, and Starwood loyalty numbers, along with name, gender, date of birth, address, email address, telephone number, username, and hotel stay and other travel information.

IV. CAUSES OF ACTION

COUNT 1

Arkansas Deceptive Trade Practices Act
Ark. Code Ann. § 4-88-101 *et seq.*

26. The State repeats and incorporates by reference each allegation contained in the preceding paragraphs. Ark. R. Civ. P. 10(c).

27. 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 the Arkansas Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101 *et seq.* Defendant's practices, as set forth above, constitute unconscionable or deceptive trade practices in the sale and offer for sale of consumer services in violation of Ark. Code Ann. § 4-88-107(a)(10).

28. 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 Ark. Code Ann. § 4-88-107(a)(1) & (a)(3).

29. 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 Ark. Code Ann. § 4-88-108.

30. 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 unconscionable trade practice in violation of Ark. Code Ann. § 4-88-107(a)(10).

COUNT 2

Arkansas Personal Information Protection Act
Ark. Code Ann. § 4-110-101 *et seq.*

31. The State repeats and incorporates by reference each allegation contained in the preceding paragraphs. Ark. R. Civ. P. 10(c).

32. Defendant acquires, owns, or licenses the personal information of Arkansas residents.

33. Defendant has violated the Arkansas Personal Information Protection Act, Ark. Code Ann. § 4-110-101 *et seq.* by failing to implement and maintain reasonable security

procedures to protect records that contain personal information concerning Arkansas residents from unauthorized access, destruction, use, modification, or disclosure.

34. Defendant's failure to take reasonable steps to protect consumers' personal information constitutes an unfair or deceptive trade practice that violates the ADTPA. Ark. Code Ann. § 4-88-101 *et seq.*

V. JURY DEMAND

35. The State demands a trial by jury.

VI. PRAYER FOR RELIEF

36. Based on the unlawful acts described in this Complaint, the State of Arkansas is entitled to an Order from this Court:

a. Declaring that Defendant violated the ADTPA and the APIPA;

b. Enjoining Defendant and any agents, successors, assigns, and employees acting directly or through any corporate or business device, from engaging in acts and practices alleged in this Complaint and for any other acts and practices that violate the ADTPA and the APIPA;

c. Awarding actual and compensatory damages;

d. Awarding the maximum statutory damages;

e Awarding reasonable attorneys' fees and costs;

f. Awarding pre-judgment and post-judgment interest;

g. Granting further just and proper relief.

Respectfully submitted,

TIM GRIFFIN
Attorney General

/s/ Matthew M. Ford
Matthew M. Ford, ABN 2013180
Senior Assistant Attorney General
323 Center Street, Suite 200
Little Rock, AR 72201
Telephone: (501) 320-3069
Fascimile: (501) 681-8118
Matthew.Ford@ArkansasAG.gov