STATE OF CONNECTICUT

RETURN DATE: 11/05/24

STATE OF CONNECTICUT, *Plaintiff,*	:	SUPERIOR COURT
	:	JUDICIAL DISTRICT
	:	OF HARTFORD
v.	:	
	:	AT HARTFORD
MARRIOTT INTERNATIONAL, INC., *Defendant*.	:	OCTOBER 9, 2024

COMPLAINT

Plaintiff, State of Connecticut, by William Tong, Attorney General, State of Connecticut, brings this action against the Defendant Marriott International, Inc. ("Marriott" or "Defendant") for violations of the Connecticut Unfair Trade Practices Act ("CUTPA"), General Statutes § 42-110a, *et seq*., Connecticut's Breach of Security Law ("Breach Notification Law"), General Statutes § 36a-701b, *et seq*., and Connecticut's Safeguarding of Personal Information Law ("Safeguards Law"), General Statutes § 42-471, and states as follows:

JURISDICTION

1. This action is brought for and on behalf of the State of Connecticut by William Tong, Attorney General of the State of Connecticut (the "Attorney General"), at the request of Bryan Cafferelli, Commissioner of Consumer Protection, pursuant to CUTPA, more specifically, General Statutes § 42-110m as well as the Breach Notification Law, more specifically General Statutes § 36a-701b(j). This action is also brought pursuant to the Attorney General's authority under Connecticut's Safeguards Law, more specifically General Statutes § 42-471(e)(1).

2. This Court has jurisdiction over the Defendant pursuant to CUTPA because the Defendant was engaged in trade and commerce within the State of Connecticut at all times relevant to this Complaint. This Court also has jurisdiction over the Defendant pursuant to the Safeguards Law and the Breach Notification Law because the Defendant was also in possession of or maintains computerized data that includes Connecticut residents' personal information as defined by General Statutes § 36a-701b and General Statutes § 42-471(c).

THE PARTIES

3. Plaintiff is the State of Connecticut ("State"), William Tong, Attorney General.

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

BACKGROUND

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 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

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.

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.

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).

Information Security Practices

24. 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 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/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 the 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.

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, 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 CUTPA

1-25. The allegations of Paragraphs 1 through 25 are incorporated by reference as Paragraphs 1 through 25 of Count One as if fully set forth herein.

26. CUTPA at General Statutes § 42-110b(a) states: "[n]o person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

27. CUTPA at General Statutes § 42-110a(4) states that the terms "trade" and "commerce" shall mean: "the advertising, the sale or rent or lease, the offering for sale or rent or lease, or the distribution of any services and any property, tangible or intangible, real, personal or mixed, and any other article, commodity, or thing of value in this state."

28. Defendant was at all times relevant hereto engaged in trade and commerce in the State of Connecticut by compiling consumers' sensitive personal information, offering that information for sale in various forms, including credit reports, and accepting payment for the information.

29. While engaged in trade or commerce in Connecticut, Marriott violated CUTPA by representing to users that it protects the sensitive personal information of Connecticut residents. Contrary to this representation, intruders were able to gain access to personal information on Marriott's network and Marriott suffered a data breach. Such representations were likely to mislead consumers acting reasonably under the circumstances into believing that their personal

information was safeguarded from misuse by third parties and were material to users' decisions about whether or not to utilize or continue utilizing Marriott's services.

30. While engaged in trade or commerce in Connecticut, Marriott violated CUTPA through its failure to adequately inform consumers regarding its data protection practices. This constituted a material omission likely to mislead consumers acting reasonably under the circumstances into believing that their personal information was safeguarded from misuse by third parties.

31. By engaging in the aforementioned acts or practices, Marriott also violated the public policy of the State of Connecticut, including the public policy set forth in General Statutes § 42-471, which requires persons in possession of personal information of another person to safeguard that information.

32. Marriott's acts or practices as described herein, are oppressive unethical, immoral, and unscrupulous.

33. Marriott's acts or practices, as described herein, caused substantial injury to consumers.

34. Marriott has therefore engaged in unfair or deceptive acts and practices in violation of General Statutes § 42-110b(a).

COUNT TWO

Civil Penalties (Violations of CUTPA)

1-34. The allegations of Paragraphs 1 through 34 of Count One are incorporated by reference as Paragraphs 1 through 34 of Count Two as if fully set forth herein.

35. Marriott engaged in the acts and practices alleged herein when they knew or should have known that their conduct was unfair or deceptive, in violation of General Statutes § 42-

110b(a), and, therefore, are liable for civil penalties of up to five thousand dollars ($5,000) per willful violation pursuant to General Statutes § 42-110o(b).

COUNT THREE

Violations of Safeguards Law

1-25. The allegations of Paragraphs 1 through 25 are incorporated by reference as Paragraphs 1 through 25 of Count Three as if fully set forth herein.

26. General Statutes § 42-471(a) states: "any person in possession of personal information of another person shall safeguard the data, computer files, and documents containing the information from misuse by third parties…"

27. Marriott was in possession of Connecticut residents' "personal information" as that term is defined in General Statutes § 42-471(c).

28. Marriott's policies and procedures did not adequately safeguard Connecticut residents' personal information.

29. Marriott therefore failed to safeguard personal information in violation of General Statutes § 42-471.

COUNT FOUR

Civil Penalties (Violations of Safeguards Law)

1-29. The allegations of Paragraphs 1 through 29 of Count Three are incorporated by reference as Paragraphs 1 through 29 of Count Four as if fully set forth herein.

30. Marriott engaged in the acts or practices alleged herein in violation of General Statutes § 42-471(a) and therefore is liable for civil penalties of five thousand dollars ($5,000.00) per violation pursuant to General Statutes § 42-471(e) as a *per se* violation of CUTPA.

COUNT FIVE

Violations of Breach Notification Law

1-25. The allegations of Paragraphs 1 through 25 are incorporated by reference as Paragraphs 1 through 25 of Count Five as if fully set forth herein.

26. General Statutes § 36a-701b(b)(1) states: "Any person who owns, licenses, or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was breached or is reasonably believed to have been breached. Such notice shall be made without unreasonable delay but not later than sixty days after the discovery of such breach, … ."

27. Marriott sent notice to affected residents on or about November 30, 2018 after confirming a breach of security as the result of an internal alert on or about September 8, 2018.

28. Marriott knew or should have known that Starwood's systems were compromised earlier than September 8, 2018. But for Marriott's delays in integrating Starwood's systems into Marriott's, Marriott would have detected the breach of security and provided earlier notice to Connecticut residents.

29. Marriott knew or should have known on September 8, 2018 that it was in possession of personal information of Connecticut residents in the compromised databases.

30. Marriott therefore failed to provide timely notification of a breach of security in violation of General Statutes § 36a-701b.

COUNT SIX

Civil Penalties (Violations of Breach Notification Law)

1-30. The allegations of Paragraphs 1 through 30 of Count Five are incorporated by reference as Paragraphs 1 through 33 of Count Six as if fully set forth herein.

31. Marriott engaged in the acts or practices alleged herein in violation of General Statutes § 36a-701b (b)(1) and therefore is liable for civil penalties of five thousand dollars ($5,000.00) per violation pursuant to General Statutes § 36a-701b (j) as a *per se* violation of CUTPA.

COUNT SEVEN

Violations of CUTPA Regulations

1-25. The allegations of Paragraphs 1 through 25 are incorporated by reference as Paragraphs 1 through 25 of Count Five as if fully set forth herein.

26. Pursuant to Regulations of Connecticut Agencies § 42-110b-18 (c): "It shall be an unfair or deceptive act or practice to: … (c) Misrepresent the sponsorship, endorsement, approval, or certification of merchandise or services; … ."

27. Pursuant to Regulations of Connecticut Agencies § 42-110b-18 (e): "It shall be an unfair or deceptive act or practice to: … (e) Misrepresent the nature, characteristics, standard ingredients, uses, benefits, quantities or qualities of merchandise or services; … ." (emphasis added).

28. Marriott represented that it was affiliated with certain payment card brands, including, but not limited to, MasterCard and VISA. In order to accept such payment card brands,

Marriott is required to adhere to the data security requirements contained in the Payment Card Industry Data Security Standards ("PCI-DSS").

29. Marriott represents that it accepts branded payment cards, and therefore it is in compliance with PCI-DSS.

30. In truth and in fact, Marriott was not compliant with PCI-DSS.

31. Marriott therefore engaged in unfair or deceptive acts and practices in violation of Regulations of Connecticut Agencies § 42-110b-18 (c), (e).

COUNT EIGHT

Civil Penalties (Violations of CUTPA Regulations)

1-31. The allegations of Paragraphs 1 through 31 of Count Seven are incorporated by reference as Paragraphs 1 through 31 of Count Eight as if fully set forth herein.

32. Marriott engaged in the acts or practices alleged herein in violation of Regulations of Connecticut Agencies § 42-110b-18 (c), (e) and therefore is liable for civil penalties of five thousand dollars ($5,000.00) per violation pursuant to General Statutes § 42-110b (c) as a *per se* violation of CUTPA.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiff respectfully requests that the Court enters the following relief:

1. Enter judgment against the Defendant and in favor of the Plaintiff on each count of this Complaint;

2. Pursuant to CUTPA, specifically General Statutes § 42-110m, permanently enjoin and restrain the Defendant from engaging in unfair or deceptive practices relating to the protection of personal information.

3. Pursuant to CUTPA, specifically General Statutes § 42-110o, order the Defendant to pay civil penalties in the amount of five thousand dollars ($5,000.00) for each and every willful violation of CUTPA;

4. Pursuant to CUTPA, specifically General Statutes § 42-110m, order the Defendant to pay costs and reasonable attorneys' fees incurred by the State in connection with the investigation and litigation of this matter;

5. Permanently enjoin and restrain the Defendant from continuing the practices complained of herein under General Statutes § 42-471.

6. An order, pursuant to General Statutes § 42-471(e)(1), directing the Defendant to pay civil penalties of five thousand dollars ($5,000.00) for each violation of General Statutes § 42-471(a);

7. An order, pursuant to General Statutes § 36a-701b(j), directing the Defendant to pay civil penalties of five thousand dollars ($5,000.00) for each violation of General Statutes § 36a-701b;

8. An order, pursuant to General Statutes § 42-110b(c) directing the Defendant to pay civil penalties of five thousand dollars ($5,000.00) for each violation of Regulations of Connecticut

Agencies § 42-110b-18 (c), (e); and

9. That the Court grant such further relief in law or equity as the Court deems necessary or appropriate to remedy the effects of Defendant's unlawful practices.

The Plaintiff hereby states that the amount in controversy is more than fifteen thousand dollars ($15,000.00), exclusive of interests and costs.

Dated at Hartford, Connecticut this 9th day of October, 2024.

PLAINTIFF,
STATE OF CONNECTICUT

WILLIAM TONG
ATTORNEY GENERAL

By: _____

John Neumon, Juris # 439448
Kileigh Nassau, Juris # 444300
Assistant Attorney General
Office of the Attorney General
Privacy Section
165 Capitol Avenue
Hartford, CT 06106
Telephone: (860) 808-5440