

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
DIVISION OF LAW
124 HALSEY STREET – 5TH FLOOR
P.O. BOX 45029-5029
NEWARK, NEW JERSEY 07101
ATTORNEY FOR PLAINTIFFS

BY: Mandy K. Wang (Bar No. 373452021)
Deputy Attorney General
(609) 954-8714

SUPERIOR COURT OF NEW JERSEY
CHANCERY DIVISION, MERCER COUNTY
DOCKET NO. MER-C-_____24

**MATTHEW J. PLATKIN, Attorney General
of the State of New Jersey, and CARI FAIS,
Acting Director of the New Jersey Division of
Consumer Affairs,**

Plaintiffs,

v.

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

Defendant.

Civil Action

COMPLAINT

Plaintiffs Matthew J. Platkin, Attorney General of the State of New Jersey (“Attorney General”), with offices located at 124 Halsey Street, Fifth Floor, Newark, New Jersey, and Cari Fais, Acting Director of the New Jersey Division of Consumer Affairs (“Director”) (collectively,

“Plaintiffs”), with offices located at 124 Halsey Street, Seventh Floor, Newark, New Jersey, bring this action against Defendant Marriott International, Inc., a corporation, (“Marriott” or “Defendant”) for violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -229. (“CFA”) and the New Jersey Identity Theft Protection Act, N.J.S.A. 56:8-161 to -166 (“ITPA”), and states as follows:

PARTIES AND JURISDICTION

1. The Attorney General is charged with the responsibility of enforcing the CFA and ITPA. The Director is charged with the responsibility of administering the CFA and ITPA on behalf of the Attorney General.

2. Defendant Marriott is a Delaware corporation with its principal place of business at 7750 Wisconsin Ave., Bethesda, Maryland 20814.

3. Defendant Marriott was at all relevant times engaged in business in the State of New Jersey.

4. Plaintiffs and Defendant (collectively, the “Parties”) admit jurisdiction of this Court over the subject matter and over the Parties for purpose of the Final Consent Judgment. The Court retains jurisdiction for the purpose of enabling the Parties to apply for such further orders and relief as may be necessary for the construction, modification, enforcement, execution or satisfaction of the Final Consent Judgment.

5. Pursuant to Rule 4:3-2, venue is proper in Mercer County because Defendant, at all relevant times, has transacted business in the State of New Jersey, including, but not limited to Mercer County.

FACTUAL BACKGROUND

6. 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.

7. 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.

8. 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.

A. **Starwood Data Breach**

9. 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.

10. 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.

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

12. 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.

13. 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, a lack of multifactor authentication, and inadequate monitoring and logging practices.

14. 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

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

16. 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”).

17. 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. The intruders then resumed accessing and exporting consumers’ personal information in January 2020 and continued until they were ultimately discovered in February 2020.

18. 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.

19. 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

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

21. 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.

22. 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).

23. 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.

24. 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

25. Marriott, itself and 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, itself and 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, itself and 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.

26. As a direct result of the failures described in Paragraph 26 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 CFA)

27. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

28. The CFA, N.J.S.A. 56:8-2, prohibits:

The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . .

29. The CFA defines “merchandise” as including “any objects, wares, goods, commodities, services or anything offered, directly or indirectly to the public for sale.” N.J.S.A. 56:8-1(c).

30. The CFA defines “advertisement” as including “the attempt directly or indirectly by publication, dissemination, solicitation, indorsement or circulation or in any other way to induce directly or indirectly any person to enter or not enter into any obligation or acquire any title or interest in any merchandise or to increase the consumption thereof.” N.J.S.A. 56:8-1(a).

31. The CFA defines “sale” as including “any sale, rental or distribution, offer for sale, rental or distribution or attempt directly or indirectly to sell, rent or distribute.”

32. At all relevant times, Defendant has engaged in the advertisement, offer for sale and/or sale of merchandise within the meaning of N.J.S.A. 56:8-1(c).

33. Defendant has, in the course of offering or advertising their merchandise to residents of New Jersey for sale, engaged in fraudulent, false, misleading, or deceptive acts or practices, as set forth above, in violation of N.J.S.A. 56:8-2.

34. Defendant has, in the course of offering or advertising their merchandise to residents of New Jersey for sale, 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 N.J.S.A. 56:8-2.

35. Defendant has, in the course of offering or advertising their merchandise to residents of New Jersey for sale, knowingly failed to inform consumers of material facts regarding its data protection practices, with the intent that consumers rely on this omission of facts, in violation of N.J.S.A. 56:8-2.

36. Defendant has, in the course of offering or advertising their merchandise to residents of New Jersey, engaged in commercial practices that are unconscionable, as set forth above, in violation of N.J.S.A. 56:8-2.

37. Defendant, in the course of offering or advertising their merchandise to residents of New Jersey, failed to take reasonable steps to protect consumers' personal information from unauthorized access which caused substantial harm to consumers that consumers could not reasonably avoid, and which did not benefit the marketplace or competition, making it an unconscionable commercial practice, in violation of N.J.S.A. 56:8-2.

COUNT TWO

(VIOLATIONS OF THE ITPA)

38. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

39. Defendant collects and maintains the personal information of customers residing in New Jersey, including financial accounts.

40. As set forth above, Defendant suffered a breach of security that comprised the security, confidentiality, or integrity of the personal information of its customers residing in New Jersey.

41. Access to the personal information impacted by the breach of security, including the personal information of New Jersey customers, was not secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

42. Following the breach of security affecting the Starwood network, detected on September 7, 2018, Defendant failed to notify its New Jersey Customers of the breach of security in the most expedient time possible and without unreasonable delay, in violation of N.J.S.A. 56:6-163(a).

43. Following the Unauthorized Account Access Incidents, detected in February 2020, Defendant failed to notify its New Jersey Customers of the Unauthorized Account Access Incidents in the most expedient time possible and without unreasonable delay, in violation of N.J.S.A. 56:6-163(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request this Court enter judgment against Defendant Marriott and enter an Order:

A. Finding that Defendant violated N.J.S.A. 56:8-2 by engaging in the unlawful acts and practices alleged herein, and permanently enjoining Defendant from continuing to engage in such unlawful acts and practices;

B. Finding that Defendant violated N.J.S.A. 56:8-163 by engaging in the unlawful acts and practices alleged herein, and permanently enjoining Defendant from continuing to engage in such unlawful acts and practices;

C. Requiring Defendant to pay up to \$10,000 for each and every violation of 56:8-2 and 56:8-163, as provided by N.J.S.A. 56:8-13;

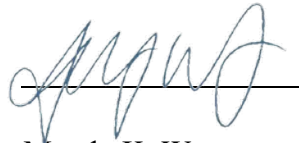
D. Requiring Defendant to pay all costs for the prosecution and investigation of this action, as provided by N.J.S.A. 56:8-11 and 56:8-19.

F. Providing any such other and further relief as the Court deems just, proper, and equitable under the circumstances.

Respectfully submitted,

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

By:

A handwritten signature in blue ink, appearing to read 'Mandy K. Wang', is written over a horizontal line.

Mandy K. Wang
Deputy Attorney General

Dated: October 9, 2024
Newark, New Jersey

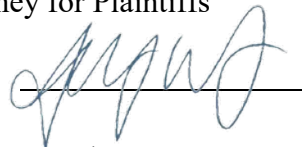
RULE 4:5-1 CERTIFICATION

I certify to the best of my information and belief, the matter in controversy in this action involving the aforementioned violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -229, and the Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166, is not the subject of any other action pending in any other court of this State.

I further certify, to the best of my information and belief, that the matter in controversy in this action is not the subject of a pending arbitration proceeding in this State, nor is any other action or arbitration proceeding contemplated. I certify that there is no other party who should be joined in this action at this time.

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

By:



Mandy K. Wang
Deputy Attorney General

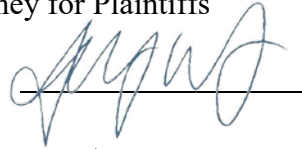
Dated: October 9, 2024
Newark, New Jersey

RULE 1:38-7(c) CERTIFICATION OF COMPLIANCE

I certify that confidential personal identifiers have been redacted from documents now submitted to the Court, and will be redacted from all documents submitted in the future in accordance with R. 1:38-7(b).

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

By:

A handwritten signature in blue ink, appearing to read 'Mandy K. Wang', is written over a horizontal line.

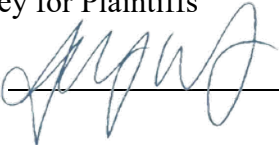
Mandy K. Wang
Deputy Attorney General

Dated: October 9, 2024
Newark, New Jersey

DESIGNATION OF TRIAL COUNSEL

Pursuant to R. 4:25-4, Mandy K. Wang and Kashif T. Chand, Deputy Attorney General, are hereby designated as trial counsel on behalf of the Plaintiffs.

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

By: 

Mandy K. Wang
Deputy Attorney General

Dated: October 9, 2024
Newark, New Jersey