UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

PATI SPRINGMEYER, an individual and Nevada Resident, on behalf of herself and all others similarly situated, Plaintiff, v. MARRIOTT INTERNATIONAL, INC., a Montgomery County, Maryland Resident, Defendant.	CASE NO. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED (1) Negligence (2) Negligence *Per Se* (3) Breach of Contract (4) Breach of Implied Contract (5) Breach of Confidence (6) Deceptive & Unfair Trade Practices

For her Class Action Complaint, Plaintiff Pati Springmeyer, on behalf of herself and all others similarly situated, allege the following against Defendant Marriott International, Inc. ("Marriott"), based on personal knowledge as to herself and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiff's counsel:

SUMMARY OF THE CASE

1. Marriott is one of the largest hotel chains in the world servicing tens of millions of customers every year.

2. As part of the reservation and booking process for staying at a Marriott property, Marriott's guests create, maintain, and update profiles containing significant amounts of personal identifiable information ("PII"), including their names, birthdates, addresses, locations, email addresses, and payment card information.

3. On March 31, 2020, Marriott announced that the login credentials of two of its employees had been compromised and "an unexpected amount of guest information" had been

improperly accessed as early as mid-January 2020. The compromised guest PII included: Contact Details (e.g., name, mailing address, email address, and phone number); Loyalty Account Information (e.g., account number and points balance, but not passwords); Additional Personal Details (e.g., company, gender, and birthday day and month); Partnerships and Affiliations (e.g., linked airline loyalty programs and numbers); and Preferences (e.g., stay/room preferences and language preference) ("Data Breach").

4. This Data Breach comes on the heels of another massive breach Marriott announced in November 2018, wherein the PII of 500 million guests contained in Marriott's Starwood reservation database was exposed due to a flaw in its reservation and database systems.

5. This Data Breach was a direct result of Marriott's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its guests' PII.

6. Marriott disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard guest PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members with prompt and accurate notice of the Data Breach.

7. As a result of Marriott's failure to implement and follow basic security procedures, guest PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

8. Plaintiff, on behalf of all others similarly situated, allege claims for negligence, breach of confidence, and violation of the Maryland's Consumer Protection Act, and seek to compel Defendant to adopt reasonably sufficient security practices to safeguard guest PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

9. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. Venue is proper under 28 U.S.C. § 1391(c) because Defendant is a corporation that does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Marriott's governance and management personnel that led to the breach. Further, Marriott's terms of service governing users in the United States provides for Maryland venue for all claims arising out of Plaintiff' relationship with Marriott.

PARTIES

11. Plaintiff Pati Springmeyer is a resident and citizen of Las Vegas, Nevada. Plaintiff Springmeyer has stayed at a number of Marriott properties and hotels over the past 10 years, entrusting Marriott with her PII. On March 31, 2020, Ms. Springmeyer received an email from

Marriott International stating that her PII had been compromised and "accessed without authorization."

12. Since the announcement of the Data Breach, Ms. Springmeyer continues to monitor her various accounts in an effort to detect and prevent any misuses of her personal information.

13. Ms. Springmeyer has, and continues to spend her valuable time to protect the integrity of her PII — time which she would not have had to expend but for the Data Breach.

14. Ms. Springmeyer suffered actual injury from having her PII exposed as a result of the Data Breach including, but not limited to: (a) paying monies to Marriott for its services which she would not have, had Marriott disclosed that it lacked data security practices adequate to safeguard consumers' PII from theft; (b) damages to and diminution in the value of her PII—a form of intangible property that the Plaintiff entrusted to Marriott as a condition for hotel services; (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

15. As a result of the Data Breach, Ms. Springmeyer will continue to be at heightened risk for fraud and identity theft, and their attendant damages for years to come.

16. Defendant Marriott, Inc., is a corporation with its principal executive offices located at 10400 Fernwood Rd, Bethesda, Maryland 20817.

FACTUAL BACKGROUND

A. The Marriott 2020 Data Breach

17. In February 2020, Marriott learned that the login credentials of two employees at a franchise property had been compromised a large amount of guest PII had been improperly accessed. Over a month later, Marriott notified approximately 5.2 million guests that their PII such as names, addresses, phone numbers, birthdays, loyalty information had been compromised. Although Marriott said it doesn't believe that credit card information, passport numbers or driver's

license information were accessed, they stated the investigation was ongoing and they did not rule out the possibility.[1]

18. On March 31, 2020, Marriott sent an email to affected guests and posted an incident notification on its website stating in relevant part as follows:

> Marriott International: Incident Notification
> This site has information concerning the incident, answers to questions, and steps guests can take.
>
> March 31, 2020
>
> **What Happened?**
>
> Hotels operated and franchised under Marriott's brands use an application to help provide services to guests at hotels. At the end of February 2020, we identified that an unexpected amount of guest information may have been accessed using the login credentials of two employees at a franchise property. We believe this activity started in mid-January 2020. Upon discovery, we confirmed that the login credentials were disabled, immediately began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests.
>
> Although our investigation is ongoing, we currently have no reason to believe that the information involved included Marriott Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers.
>
> At this point, we believe that the following information may have been involved, although not all of this information was present for every guest involved:
>
> - Contact Details (e.g., name, mailing address, email address, and phone number)
> - Loyalty Account Information (e.g., account number and points balance, but not passwords)

[1] *Millions of Guests Impacted in Marriott Data Breach, Again*, Threatpost, Mach 31, 2020, https://threatpost.com/millions-guests-marriott-data-breach-again/154300/

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.