IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

DONNA HITESHEW, individually and on behalf of all others similarly situated, Plaintiff, v. MARRIOTT INTERNATIONAL, INC., a Delaware corporation, and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC, a Maryland limited liability company, Defendants.	Case No.: **JURY TRIAL DEMANDED** **REDACTED**

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Donna Hiteshew brings this Class Action Complaint and Demand for Jury Trial ("Complaint") against Defendants Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC (collectively referred to as "Marriott," unless otherwise indicated). Plaintiff alleges as follows upon personal knowledge as to herself and her own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. On November 30, 2018, Marriott—the world's leading hotel chain—announced it had experienced what is now being recognized as the second largest data breach in history. Setting aside that it waited over 80 days after first learning of the breach to inform the public, Marriott revealed that the data of over 500 million of its guests, including names, mailing addresses, phone numbers, email addresses, birth dates, and even passport numbers, among other things, had been exposed to hackers *for the past four years*.

2. The breach also exposed Marriott customer's card payment numbers and the card expiration dates. Although Marriott stated that customer payment information was encrypted, it

could *not* exclude the possibility that hackers obtained the encryption keys necessary to decrypt and access this data.

3. Each detail of this breach is alarming by itself, but what is particularly egregious is Starwood (Marriott's wholly-owned subsidiary) reported a data breach in 2015 when it detected malware on its point of sale ("POS") systems in over 100 locations in North America. The investigation that began in November 2015, and concluded in January 2016, should have revealed this breach. Instead, it incorrectly found that the Starwood customer reservation database—the database at issue in this breach—had not been impacted.

4. Around this time, Marriott and Starwood also had a string of other data security incidents, including:

- A security researcher found a SQL injection bug on a Starwood website, which was likely used to gain access to Starwood databases (and vulnerabilities like this were for sale on the Dark Web at the time);
- Marriott's Computer Incident Response Team was compromised and attackers gained access to their internal email accounts, as shown in Section III below;
- Security researcher Alex Holden discovered that six starwoodhotels.com domains were controlled by a Russian botnet; and
- Starwood's cloud portals had an easily guessable password, which could allow hackers to access business financial records, security controls, and booking information.

5. And it does not get better for Marriott. As of the date this Complaint was filed, Marriott *is still not properly protecting a wealth of information, including* [redacted]. As shown in Section VI below, records from Starwood's [redacted] are, therefore, publicly accessible online. Starwood describes this system as containing [redacted]. Not only is this data sensitive as it applies to Defendants' [redacted]

but it is likely a virtual treasure trove of exploitable information for gaining access to additional customer information. The threat posed by this vulnerability is real and ongoing, and may have caused this data breach or resulted in another.

6. Ultimately, Marriott could and should have prevented the data breach by implementing and maintaining reasonable safeguards, consistent with the representations Marriott made to the public in its marketing materials and privacy statements, and compliant with industry standards, best practices, and the requirements of Maryland State law. Unfortunately, Marriott failed to do so, and as a result, exposed the personal and sensitive data of hundreds of millions of consumers.

7. By failing to secure personal and sensitive data—despite its legal obligations to do so—Marriott willfully and intentionally exposed hundreds of millions of consumers to the risks of identity theft and financial fraud, tax return scams, and other potential ongoing harm.

8. Had Marriott informed consumers that it would use inadequate security measures, customers, like Plaintiff Hiteshew, would not have stayed at its hotels.

9. While some security threats are unavoidable in a rapidly-developing technological environment, Marriott's failure to implement reasonable data security protocols jeopardized hundreds of millions of its customers' sensitive personal information, fell far short of its promises, and diminished the value of the services it provided. In other words, because Marriott failed to disclose its gross security inadequacies to Plaintiff and two Classes of consumers defined below, it delivered to them fundamentally less useful and less valuable service than the ones they paid for.

10. Accordingly, Plaintiff Hiteshew brings this suit on behalf of herself and all others similarly situated, to seek redress for Marriott's unlawful conduct. Not only does this Complaint seek damages for present and past injuries, it seeks the creation of, not unlike medical

monitoring relief in a mass tort case, a data privacy fund to compensate putative class members into the future.

PARTIES

11. Plaintiff Donna Hiteshew is a natural person and citizen of the Commonwealth of Pennsylvania.

12. Defendant Marriott International, Inc. is a Delaware corporation with its headquarters located at 10400 Fernwood Road, Bethesda, Maryland 20817. Marriott International, Inc. conducts business throughout this District, the State of Maryland, and the United States.

13. Defendant Starwood Hotels & Resorts Worldwide, LLC is a Maryland limited liability company with its principal office located at 10400 Fernwood Road, Bethesda, Maryland 20817. Starwood Hotels & Resorts Worldwide, LLC conducts business throughout this District, the State of Maryland, and the United States. Starwood Hotels & Resorts Worldwide, LLC is a wholly-owned subsidiary of Marriott International, Inc.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (a) at least one Class member is a citizen of a different state than Defendants, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) none of the exceptions under that subsection apply to this action.

15. This Court has personal jurisdiction over Defendants because they conduct significant business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated from this District. Additionally, this Court has personal jurisdiction over Defendants because they maintain their principal place of business in this District.

16. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the Complaint occurred in this District and because Defendants maintain their principal place of business in this District.

COMMON FACTUAL ALLEGATIONS

I. An Overview of Marriott.

17. Marriott is a leading hotel and hospitality company with more than 6,700 properties across 130 countries and territories, reporting revenues of more than $22 billion in fiscal year 2017.[1] Currently, Marriott owns 30 hotel brands including Marriott Vacation Club, Renaissance Hotels, The Ritz-Carlton, Moxy Hotels, and AC Hotels, among others.

18. Marriott has grown exponentially over the last few years by acquiring other hotel chains. Most notably, Marriott acquired Starwood Hotels and Resorts in 2016 for $13.6 billion, bringing Starwood's Sheraton, Westin, W Hotels, and St. Regis properties under the Marriott umbrella.[2]

19. Since the Starwood acquisition, Marriott has become the world's largest hotel chain and now accounts for 1 out of every 15 hotel rooms around the globe.

II. Marriott Collects Incredibly Sensitive Information From its Customers.

20. In order to stay at a Marriott property, guests must first make a reservation and provide Marriott their full names, mailing addresses, email addresses, telephone numbers, credit or debit card numbers, travel itinerary, and often times other sensitive information.

21. According to the Privacy Statement posted on its website, Marriott also collects

---

1 *About Marriott Hotels | Marriott Corporate Business Information*, Marriott, https://www.marriott.com/marriott/aboutmarriott.mi (last visited Dec. 6, 2018).

2 *Marriott Closes $13-Billion Purchase Of Starwood To Become World's Largest Hotel Chain*, Los Angeles Times, https://www.latimes.com/business/la-fi-marriott-starwood-20160923-snap-story.html (last visited Dec. 6, 2018).

other "Personal Data" (which it defines as "data that identif[ies] you as an individual or relate to an identifiable individual") about its guests during the course of their visits, including their:

- Name
- Gender
- Postal address
- Telephone number
- Email Address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference
- Data and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

22. In more limited circumstances, Marriott also collects:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel
- Guest preferences and personalized data ("Personal Preferences"), such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit

23. Marriott stores this incredibly sensitive trove of data and uses this information for its own commercial purposes.

24. In fact, Marriott collects and uses such detailed and sensitive consumer data that it enlisted a leading data analytics company to use that wealth of data to identify, attract, and retain the most profitable customers. In other words, Marriott uses all of the data it collects to help

predict and influence its customers' future behaviors (*i.e.*, convincing them to stay at their properties). According to the analytics company, that's because there's no lack of available data here. Together, they have access to household profiles, including number of kids, type of jobs held by family members, their salaries, where and how they spend their money, and even the type of jeans they buy. The level and granularity of data Marriott and this analytics company collects is frightening. They can even identify when a guest leaves a hotel, where they go, and when they're at home and in bed for the night (by tracking their cell phone's location and activity).

25. As discussed below, consumers place value in data privacy and security, and they consider it when making decisions on hotel room purchases. Marriott recognizes this and also the sensitivity of the information it collects and, in light of that, promises to use reasonable measures protect and keep it secure.[3] Had Plaintiff knew Marriott would not adequately protect her sensitive information, she would not have stayed there.

III. Marriott Has a Significant History of Failing to Adequately Protect Sensitive Personal Information.

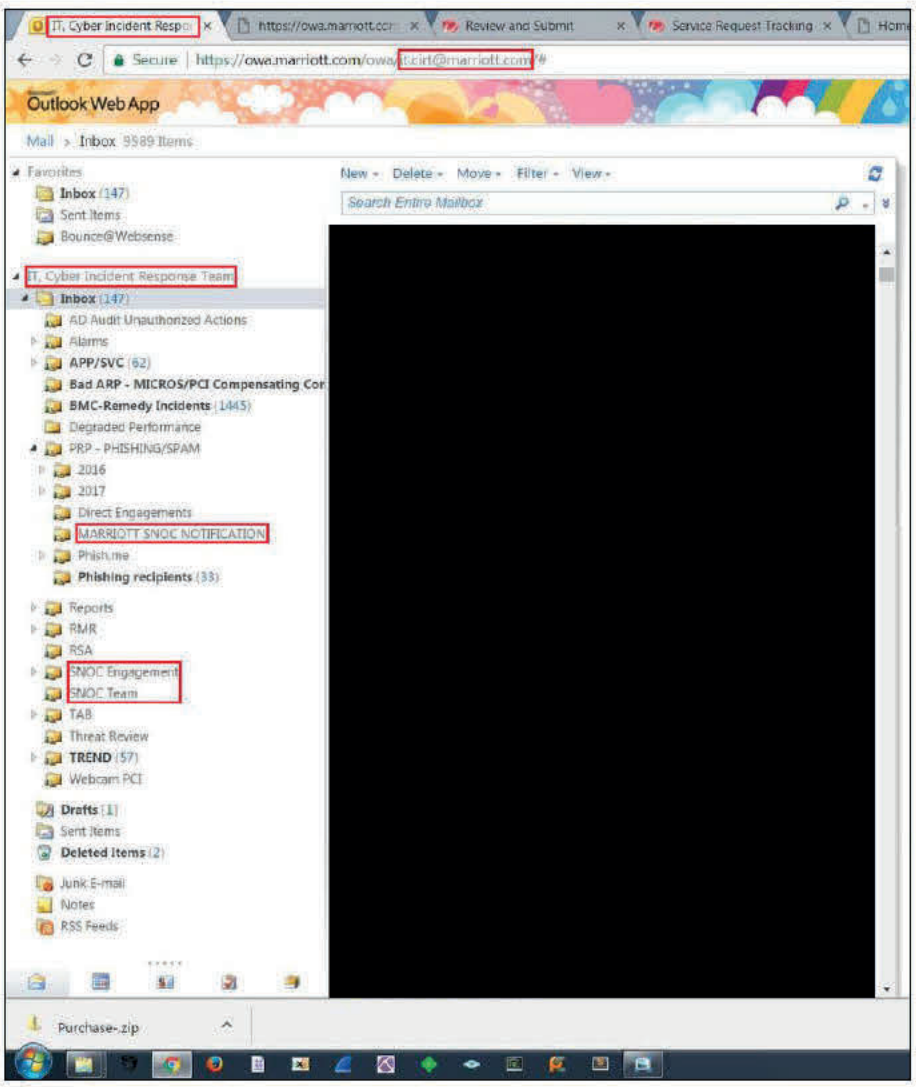
26. While not generally known to the public until recently, Marriott has a history of failing to adequately protect its computer networks.

27. For example, in 2014, a security researcher found a SQL injection bug (*i.e.*, a vulnerability in a website that an attacker with basic hacking skills can exploit to access a database) that likely was used to gain access to Starwood databases. In fact, at the time, vulnerabilities like this were for sale on the Dark Web.

28. Later, Marriott's Computer Incident Response Team ("CIRT") was compromised

[3] *Marriott Global Privacy Statement*, Marriott, https://www.marriott.com/about/privacy.mi (last visited Dec. 6, 2018).

due to an external analyst downloading a malware sample, which executed and provided attackers access to the CIRT's email accounts. Figure 1 below shows a screenshot—recovered from a Nigerian hacker's server—of Marriott's CIRT teams email inbox.[4]



(Fig. 1.)

29. In another example, security researcher Alex Holden had discovered that six servers hosting starwoodhotels.com domains were controlled by a Russian botnet (*i.e.*, a network of private computers infected with malicious software and controlled as a group without the

[4] *MalwareHunterTeam*, Twitter, https://twitter.com/malwrhunterteam/status/881089396124078080 (last visited Dec. 6, 2018).

owner's knowledge). Holden had also discovered that one of Starwood's cloud portals had an easily guessable password, which could allow hackers to access business financial records, security control, and booking information.

30. It should be no surprise then that on November 20, 2015—shortly after Marriott announced its acquisition of Starwood—Starwood announced the discovery of malware that has been installed on POS systems at a number of its hotels in North America. The malware affected Starwood's various restaurants, gift shops, and other payment processing centers at over 50 locations in North America.[5]

31. The malware collected customer's payment card information from Starwood's POS systems, including the cardholder's name, card number, security code, and expiration date.[6]

32. After the discovery of the malware in 2015, Starwood employed a third-party forensic team of experts "to conduct an extensive investigation" to determine the source of the malware and the extent of its impact.[7] Months after the initial discovery, Starwood updated its customers (in January 2016) about the details of the breach. Starwood also released a comprehensive list of all hotels and resorts affected by the malware which doubled from over 50 to 100 impacted locations.[8]

33. In an effort to "comfort" its customers and keep them coming back to its properties, Starwood (incorrectly) informed them that its guest reservation databases were not

---

5 *Letter From Our President*, Starwood Hotels and Resorts, https://www.starwoodhotels.com/Media/PDF/Corporate/Letter_1.pdf (last visited Dec. 6, 2018).

6 *Id*.

7 *FAQ*, Starwood Hotels and Resorts, https://www.starwoodhotels.com/Media/PDF/Corporate/FAQ.pdf (last visited Dec. 6, 2018).

8 *January 22, 2016 Letter From Our President*, Starwood Hotels & Resorts, https://www.starwoodhotels.com/html/HTML_Blocks/Corporate/Confidential/Letter.htm (last visited Dec. 6, 2018).

impacted.

34. Unfortunately, Marriott negligently failed to discover then that hackers actually had on-going access to Starwood's guest reservation database (since 2014, at least). Defendants failed to utilize industry-standard monitoring practices and routine audits that would have easily identified this and other data security issues.

IV. Marriott Failed to Detect A Four-Year Long Breach of its Reservation Database and Then Waited Over 80 Days to Notify its Customers.

35. On November 30, 2018, Marriott revealed that its Starwood reservation database had been hacked. The Starwood reservation database contained information pertaining to customers that stayed at Starwood properties like the Sheraton, W Hotels, Westin, and St. Regis.

36. Marriott explained that it first learned about the data breach on September 8, 2018, when a Marriott administrator received an alert from its "internal security tool" that someone attempted to access the Starwood guest reservation database. Marriott then "quickly engaged leading security experts to help determine what occurred."[9]

37. The security experts' findings were shocking. They learned that the breached database contained information on approximately 500 million guests who made a reservation at a Starwood property.

38. For approximately 327 million of its guests, the compromised information included a combination of the guest's:

- full name;
- mailing address;
- phone number;
- email address;
- passport number;
- Starwood Preferred Guest account information;
- date of birth;

[9] *Starwood Reservation Database Security Incident*, Kroll, https://answers.kroll.com/ (last visited Dec. 6, 2018).

- gender;
- arrival and departure information;
- reservation date; and
- communication preferences.[10]

39. The remaining 173 million guests likely had their names and email addresses taken.

40. The size of Marriott's data breach is the second largest in history and the largest since Yahoo's 2013 data breach affecting 3 billion individuals.[11]

41. Marriott also revealed that the breached database includes a significant numbers of customer's payment card numbers and the card expiration dates. Although Marriott claims customer's payment information was encrypted by using Advanced Encryption Standard encryption (AES-128), it has not ruled out the possibility that the two components needed to decrypt payment card numbers have also been taken. In other words, in another egregious example of its substandard security practices, it may have been possible for hackers to have obtained the necessary keys or passwords to decrypt customer's payment card numbers.

42. In an effort to put its own interests ahead of their customers, when Marriott announced this breach, it took the opportunity to improperly communicate with putative members of the Classes and created significant confusion

43. Specifically, on November 30, 2018, Marriott published a website—through a third-party company called Kroll (answers.kroll.com). On that website, Marriott directed its guests to sign up for one year of a web monitoring service, called WebWatcher. WebWatcher's terms include the following mandatory arbitration, jury waiver, and class action waiver:

---

10 *Id.*

11 *The Biggest Data Breaches Of All Time, Ranked*, Quartz, https://qz.com/1480809/the-biggest-data-breaches-of-all-time-ranked/ (last visited Dec. 6, 2018).

C. Arbitration; Jury Waiver.

Any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by binding arbitration administered in Nashville, Tennessee by the American Arbitration Association ("AAA") in accordance with its Arbitration Rules then in effect. There shall be one arbitrator agreed to by you and Kroll (or its Representatives, as applicable) within twenty (20) days of a written request for arbitration. If the parties cannot agree, an arbitrator will be appointed by the AAA in accordance with its Arbitration Rules. Any award from any such arbitration proceeding may be entered as a judgment in any court of competent jurisdiction. Each party shall bear its own costs in connection with any arbitration hereunder. Nothing herein shall prevent a party from seeking injunctive relief (or any other provisional remedy) from any court having jurisdiction over the parties and the subject matter of the dispute as is necessary to protect such party's proprietary rights.

You and Kroll agree that, to the fullest extent permitted by law, you and Kroll knowingly, voluntarily, and intentionally waive the right to a trial by jury in any action or other legal proceeding arising out of or relating to the Agreement, the Platform or the Services. The foregoing waiver applies to any action or legal proceeding, whether sounding in contract, tort or otherwise. You also agree not to include any employee of Kroll as a party in any such action or proceeding.

D. Class Action Waiver. You and Kroll (or its Representatives, as applicable) knowingly, voluntarily, and intentionally agree that each may bring claims against the other or a Representative only in your or its individual capacity, and not as a plaintiff or class member in any purported class or representative proceeding

44. In so doing, Marriott engaged in an underhanded attempt to induce putative class members to waive and limit their legal rights, creating both uncertainty about whether to accept the WebWatcher product and whether they were still permitted to pursue legal claims in court through a class action vehicle. The net result of this conduct is dissuading consumer from taking all steps to vindicate their rights.

V. Marriott Harmed its Customers by Concealing its Deficient Data Security Practices.

45. Marriott customers have already suffered significant and lasting harm as a result of Marriott's misconduct.

46. First, consumers place value in data privacy and security, and they consider that when making purchasing decisions. In fact, it is widely accepted that consumers are willing to

pay higher prices to do business with merchants that better protect their privacy and information. A number of studies have found that U.S. consider security when purchasing goods and services, and that over 50% of consumers would consider paying more to work with a company with better security.[12] Likewise, studies have shown that over 70% of U.S. consumers will provide less personally identifiable information to organizations that suffer a data breach.[13]

47. Consumer technology markets have likewise demonstrated that consumers value their privacy and security and incorporate data security practices into their purchases. For example, companies have begun providing consumers with "cloaking services" that allow them to browse the Internet anonymously for a fee. Likewise, companies now offer services that, in exchange for a monthly fee, will offer online services designed to protect data privacy.

48. Because of the value consumers place on data privacy and security, services with better security practices command higher prices than those without. Indeed, if consumers did not value their data security and privacy, profit-seeking corporations (like Marriott) would have no reason to tout their privacy and security credentials to current and prospective customers.

49. These value propositions reflect the fact that consumers view companies that promise to adequately secure customer data as being far more useful—and valuable—than those with substandard protections.

50. As a result, a hotel service with substandard data security and privacy protections is less useful and valuable than a product or service using adequate security protocols, and is, in reality, a different service entirely.

51. Stated simply, had consumers known the truth about Marriott's data security practices—*e.g.*, that it did not adequately protect and store their data—they would not have

---

12 *Beyond the Bottom Line: The Real Cost of Data Breaches*, FireEye, https://tinyurl.com/ycvtd2fl (last visited Dec. 6, 2018).

13 *Id.*

purchased rooms or otherwise stayed at Marriott hotels.

52. Second, Marriott customers have already suffered significant and lasting harm as a result of the data breach, and such harm is likely to continue and worsen over time.

53. Armed with an individual's sensitive and personal information—like names, mailing addresses, email addresses, phone numbers, passport numbers, dates of birth, and travel information—hackers and criminals can commit identity theft, financial fraud, and other identity-related crimes.

54. Identity theft results in real financial losses, lost time, and aggravation to consumers. In fact, in its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of all identity theft victims never had those losses reimbursed.[14] The average out-of-pocket loss for those victims was $2,895.

55. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings."[15] The report also noted that more than one-third of identity theft victims suffered moderate or severe emotional distress due to the crime.[16]

56. Ultimately Marriott's misconduct has substantially increased the risk that the affected Marriott customers will be, or already have become, victims of identity theft or financial fraud. Worse still, because Marriott has known about this data breach for over 2 months and has still not directly notified many of its customers affected by the breach, its customers with compromised personal information (who still do not know if they have been affected) have been

---

14 *See* U.S. Dept. of Justice, Bureau of Justice Statistics, Victims of Identity Theft 2014, at 6 & Table 6, available at http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.

15 *Id*. at 8.

16 *See id.* at 9, Table 9.

unable to adequately protect themselves from potential identity theft, including by purchasing credit monitoring services or identity theft protection.

VI. As of the Date of This Filing, Marriott Continues to Not Properly Protect Confidential Data.

57. As of the date this Complaint was filed, at least one of Starwood's own internal systems was publicly accessible [redacted].

58. Some of the largest and most significant data breaches in recent history were carried out by leaving open access to this exact type of data, [redacted]

59. Like there, the information contained in [redacted] could provide an endless roadmap of network weaknesses and attack points. Likewise, a database of this kind offers numerous data points for phishing attacks and social engineering (*e.g.*, posing as an employee and requesting system login information, or, sending an email from a spoofed address that contains malware).

60. Unfortunately, this system was not properly secured, so documents and records from it were [redacted] publicly accessible. Some of the accessible documents appear to be [redacted] as shown in Figure 2.

(**Fig. 2.**)

61. Additionally, some of the publicly [redacted] indicate that an attacker may be able to *access and actively use* the Starwood system to search for particular fields to find [redacted], as shown below in Figure 3.

[redacted]

(**Fig. 3.**)

62. Similar [redacted]—*and much more*—still appears to be publicly available. Figure 4 shows a publicly accessible document called [redacted]

[redacted]

(**Fig. 4.**)

63. Ultimately, it is not surprising that Marriott did not protect its customers' sensitive information given that it still doesn't adequately protect all of its [redacted] Moreover, depending on the information accessible as a result of these existing vulnerabilities, additional Marriott customer date may still be exposed.

VII. Poor Security Practices Lead to Irreparable Harm.

64. Loss of sensitive personal information is no trivial matter. The consequences of stolen information and potential subsequent identity theft are so severe that the FTC recommends consumers shred their medical bills to protect themselves.

65. Some victims of identity theft lose access to their own money, see their tax refunds stolen, find it difficult or impossible to obtain credit, or face other financial woes. One identity theft victim found himself arrested at his home in Georgia and extradited to face trial for check fraud in Missouri before authorities were able to ascertain that they had indicted the wrong

person.[17]

66. Once a consumer's personal information has been stolen, the risk of these adverse consequences is markedly higher, and it cannot be entirely eliminated. As a result of a data breach, it is reasonably probable that affected consumers will suffer identity theft in the future.

67. The FTC recommends that consumers take a number of proactive steps when their personal information is compromised in a data breach, including filing taxes early, placing a credit freeze on their names, and frequently checking their credit reports.

68. The FTC also has recommendations for what consumers should do after someone begins using their information fraudulently. Many of these steps are complicated and require interactions with multiple government offices and private companies. Often, they require consumers to produce originals of documents that may be difficult to obtain, especially after identity theft has occurred. In some cases, the FTC recommends seeking legal counsel.[18]

69. Even following the FTC's recommendations is not enough. A single customer, monitoring her own credit, has no way to know when other affected consumers' contemporaneously stolen data begins surfacing on criminal marketplaces and starts being used for fraudulent purposes. That is a vital warning signal that would allow consumers to act quickly to protect themselves and prevent future (and, potentially, irreparable) harm.

70. Accordingly—and like the effect of a medical surveillance program established on behalf of groups of individuals exposed to asbestos—more sophisticated surveillance maintained on behalf of a larger group of individuals can alert consumers when, based on

---

17 *Identity Theft Victim Spends 32 Days in Missouri Jail*, WSB-TV (March 24, 2015), http://www.wsbtv.com/news/news/local/identity-theft-victim-spends-32-days-missouri-jail/nkdwW/.

18 FTC, *When Information is Lost or Exposed*, IdentityTheft.gov, https://www.identitytheft.gov/info-lost-or-stolen.html.

reported fraud and other indicators, they need to take immediate action to protect their credit.

FACTS SPECIFIC TO PLAINTIFF DONNA HITESHEW

71. Plaintiff Hiteshew is a Marriott customer who has stayed at and purchased hotel rooms at a variety of Marriott and Starwood properties.

72. Plaintiff Hiteshew has also been a SPG rewards member since around 2005.

73. Each time Plaintiff reserved and purchased a room at a Marriott and Starwood hotel, she was required to provide her personal information, including her name, home address, email address, telephone number, travel information, and payment information, among other things.

74. Because she purchased her rooms from a well-known, supposedly reputable hotel chain, Plaintiff Hiteshew believed that Marriott would use reasonable and accepted security methods to secure her personal and sensitive information, and Marriott confirmed that belief in its Privacy Statements.

75. Accordingly, when Plaintiff Hiteshew stayed at Marriott properties and paid for her rooms, she paid for a service and also data privacy and security measures, whereby Marriott promised to take reasonable measures to protect her sensitive and private information.

76. Such data security was a material part of her purchases. Thus, without adequate and reasonable security protections that Marriott promised and that Plaintiff Hiteshew justifiably believed she would receive as part of her purchase, the purchased services as a whole were substantially less useful and valuable to her.

77. Had Marriott adequately disclosed (before the actual data breach) that it was not actually implementing adequate security protocols, Plaintiff Hiteshew would—through reading Marriott's privacy statements or learning through the media—have been aware of Marriott's *actual* data security practices.

78. Accordingly, had Marriott adequately disclosed its lax security practices prior to her purchases, she would not have stayed at Marriott properties in the first place.

79. Additionally, Plaintiff Hiteshew took (and continues to take) considerable precautions to protect the unauthorized dissemination of her personal and sensitive information. Unfortunately, as a result of Marriott's failure to implement its promised and paid-for security practices, Plaintiff Hiteshew's personal and sensitive information was disseminated without her consent and the value of that information was quantifiably reduced.

80. As a result, Plaintiff Hiteshew has suffered damages in (i) an amount equal to the difference in value between the services paid for and the services delivered, and (ii) the value of her personal data and lost property in the form of her breached and compromised personal and sensitive information. Additionally, as a result of Marriott's data breach and failure to adequately protect their information to this day, Plaintiff Hiteshew is now at an increased risk that unauthorized third parties will misuse her sensitive and personal information.

CLASS ALLEGATIONS

81. **Class Definitions**: Plaintiff Hiteshew brings this action on behalf of herself and two classes of similarly situated individuals, defined as follows:

> **Breach Class**: All individuals in the United States whose personal information was compromised during the data breach announced by Marriott in November 2018.
>
> **Overpayment Class**: All individuals in the United States who purchased a hotel room at a Starwood property between 2014 and September 10, 2018.

Excluded from the Breach Class and Overpayment Class (collectively referred to as the "Classes", unless otherwise indicated) are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute

and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; (6) the legal representatives, successors, and assigns of any such excluded persons; and (7) any individual who contributed to the unauthorized access of Defendants' database.

82. **Numerosity**: The exact size of each Class is unknown and not available to Plaintiff at this time, but it is clear that individual joinder is impracticable. On information and belief, there are hundreds of millions of people in each Class, making joinder of each individual member impracticable. Ultimately, members of the Classes will be easily identified through Defendants' records.

83. **Commonality and Predominance**: Common questions of law and fact exist as to all members of the Breach and Overpayment Classes and predominate over any questions affecting only individual members:

(a) whether Defendants had a duty to protect and keep its customers' personal information secure, and negligently failed to do so;

(b) whether Defendants had an implied contractual obligation to protect customers' personal information;

(c) whether Defendants' conduct described herein constitutes a breach of implied contract;

(d) whether Defendants' conduct described herein constitutes a violation of the Maryland Consumer Protection Act, Md. Comm. Code §§ 13-301, *et seq*.; and

(e) whether Defendants' conduct described herein constitutes a violation of the Maryland Personal Information Protection Act, Md. Comm. Code §§

14-3501, *et seq*.

84. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Classes. Plaintiff and members of the Classes sustained damages as a result of Defendants' uniform wrongful conduct during transactions with Plaintiff and the Classes.

85. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Classes, and has retained counsel competent and experienced in complex class actions, and privacy litigation in particular. Plaintiff has no interest antagonistic to those of the Classes, and Defendants have no defenses unique to Plaintiff.

86. **Policies Generally Applicable to the Classes**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward members of the Classes, and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants' practices challenged herein apply to and affect members of the Classes uniformly, and Plaintiff's challenge of those practices hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

87. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy given that joinder of all parties is impracticable. The damages suffered by the individual members of the Classes will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendants' misconduct. Even if members of the Classes could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation

would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered and uniformity of decisions ensured.

FIRST CAUSE OF ACTION
Violation of the Maryland Consumer Protection Act
Md. Comm. Code §§ 13-301, *et. seq.*
(On behalf of Plaintiff and the Classes)

88. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

89. The Maryland Consumer Protection Act ("MCPA") (Md. Comm. Code §§ 13-301, *et seq.*) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

90. The MCPA prohibits any unlawful, unfair, or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise, false advertising, misrepresentation, or the concealment, suppression, or omission of any material fact.

91. The MCPA applies to Defendants' actions and conduct as described herein because it protects consumers in transactions that are intended to result, or which have resulted, in the sale of goods or services.

92. Defendants are each a "person" as defined under section 13-101(h) of the MCPA.

93. Defendants' conduct as alleged herein relates to "sales," "offers for sale," or "bailment" as defined by section 13-101(i) and § 13-303 of the MCPA.

94. Plaintiff and the Classes are "consumers" as defined under section 13-101(c) of the MCPA.

95. Defendants advertise, offer, and sell "consumer goods" or "consumer services" as defined by section 13-101(d) of the MCPA.

96. Defendants advertise, offer, or sell or services in Maryland and engage in trade or commerce directly or indirectly affecting the people of Maryland.

97. Defendants engaged in unfair and deceptive practices, in violation of the MCPA, by:

- Making false or misleading oral and written representations with the capacity or tendency, or effect of deceiving or misleading consumers;
- Failing to state a material fact where the failure deceives or intends to deceive;
- Advertising or offering consumer goods or services without intent to sell them as advertised or offered; and
- Engaging in deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement.

98. Specifically, Defendants engaged in these unfair and deceptive trade practices in connection with the sale or selling of consumer goods or services, in violation of the MCPA, by:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the Classes' personal information, which was a direct and proximate cause of the data breach.
- Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents (including those directly

impacting the hospitality industry), which was a direct a proximate cause of the data breach.

- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Classes' personal information, including duties imposed by the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the data breach.
- Misrepresenting it would protect Plaintiff's and the Classes' personal information.
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Classes' personal information, including duties by the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the data breach.
- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the Classes' personal information.

99. Defendants were aware or should have been aware that they were not implementing security protections as outlined above.

100. Defendants acted intentionally, knowingly, and maliciously to violate the MCPA, as it was on notice of the possibility if the breach due to its prior data breach, infiltrations of its systems in the past, as well as similar cybersecurity incidents at its competitors.

101. Defendants intended to mislead Plaintiff and the Classes and induce them to rely on their misrepresentations and omissions.

102. Defendants representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' personal and confidential information.

103. Had Defendants not engaged in the deceptive omission of material facts described above, Plaintiff would have been presented with an informed choice as to whether or not to book a room at their hotel.

104. Plaintiff and the Classes were injured by Defendants' unfair and deceptive acts, and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages. This includes damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased imminent risk of fraud and identity theft, and the loss of value of their personal information.

105. Had Defendants disclosed their true security practices, Plaintiff and the Overpayment Class either would not have booked at Defendants' hotels or would have paid substantially less to do so (*i.e.*, the value of a hotel stay *without* adequate security protections is worth substantially less than the value of a hotel stay *with* adequate protection).

106. As a direct and proximate result of Defendants' violation of the MCPA, Plaintiff and each member of the Overpayment Class have suffered harm in the form of monies paid for Defendants' products and/or services.

107. Plaintiff, on behalf of herself and the Classes, seeks an order (1) requiring Defendants to cease the unfair practices described herein; (2) awarding damages, interest, and reasonable attorneys' fees, expenses, and costs to the extent allowable; and/or (3) requiring Defendants to restore to Plaintiff and members of each Class any money acquired by means of unfair competition (restitution).

SECOND CAUSE OF ACTION
Maryland Personal Information Protection Act
Md. Comm. Code §§ 14-3501, *et. seq.*
(On behalf of Plaintiff and the Breach Class)

108. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

109. The Maryland Personal Information Protection Act ("PIPA"), Md. Comm. Code § 13-3503(a), protects an individual's "Personal Information from unauthorized access, use, modification, or disclosure" by requiring a "business that owns or licenses Personal Information of an individual residing in the State [to] implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licenses and the nature and size of the business and its operations."

110. Defendants are businesses that own or license computerized data that includes Personal Information as defined by sections 14-3501(b)(1) and (2) of PIPA.

111. Plaintiff and Breach Class members are "individuals" and "customers" as defined and covered by sections 14-3502(a) and 14-3503 of PIPA.

112. Plaintiff's and Breach Class members' personal information, as described herein and throughout, includes Personal Information as covered under section 14-3501(d) of PIPA.

113. The data breach announced by Defendants in November 2018 was a "breach of the security of a system" as defined by section 14-3504(1) of PIPA.

114. Under section 14-3504(b)(1) of PIPA, "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

115. Under sections 14-3504(b)(2) and 14-3504(c)(2), of PIPA "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system."

116. Because Defendants discovered and had notice of a security breach, they had an obligation to disclose the data breach in a timely an accurate fashion.

117. When Defendants failed to disclose the data breach in a timely and accurate manner, they violated sections 14-3504(b)(2) and 14-3504(c)(2) of PIPA.

118. As a direct and proximate result of Defendants' violations of sections 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and Breach Class members suffered injury, as detailed above.

119. Plaintiff and the Breach Class seeks relief under section 13-408 of PIPA, including actual damages and attorneys' fees.

THIRD CAUSE OF ACTION
Negligence
(On behalf of Plaintiff and the Classes)

120. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

121. As a custodian of important and sensitive personal information, Defendants owed a duty of reasonable care to Plaintiff and the Classes in safeguarding those records from theft. Defendants knew, acknowledged, and agreed the information was private and confidential and would be protected as private and confidential.

122. Defendants breached that duty by employing substandard methods of data security, and failing to adequately protect and safeguard its customers personal, confidential, and sensitive information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to Plaintiff's and members of the Classes' personal information. Furthering its dilatory practices, Defendants failed to provide adequate oversight of the personal information to which it was entrusted, resulting in a massive breach of the personal and confidential information of potentially 500 million people, over a period of four years.

123. Moreover, the law imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of personal and confidential information to Plaintiff and the Classes so Plaintiff and Classes could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their information.

124. Defendants breached their duty to notify Plaintiff and Classes of the unauthorized access by failing to notify them of the data breach until November 30, 2018. To date, although it has been months since the breach was discovered, and four years since the breach commenced, Defendants have not provided sufficient information to Plaintiff and Classes regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Classes.

125. As a direct result of Defendants' negligent conduct, Plaintiff and Classes have suffered an increased risk of identity theft. In fact, identity theft is a reasonably probable result of Defendants' conduct.

126. But for Defendants' failure to secure this data, Plaintiff and Classes would not have suffered this harm.

127. It is reasonably foreseeable that Defendants' practices, including storing personal information in the manner described above, would put customers at a seriously increased risk of identity theft.

128. As a direct and proximate result of Defendants' negligence, Plaintiff and the Classes sustained actual losses and damages as described in detail herein.

FOURTH CAUSE OF ACTION
Data Privacy Monitoring
(On behalf of Plaintiff and the Breach Class)

129. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

130. As a custodian of important and sensitive personal information, Defendants owed a duty of reasonable care to Plaintiff and the Breach Class in safeguarding those records from theft. Defendants knew, acknowledged, and agreed the information was private and confidential and would be protected as private and confidential.

131. Defendants breached that duty by employing substandard methods of data security, and failing to adequately protect and safeguard its customers personal, confidential, and sensitive information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to Plaintiff's and members of the Breach Class's personal information. Furthering its dilatory practices, Defendants failed to provide adequate oversight of the personal information to which it was entrusted, resulting in a massive breach of the personal and confidential information of potentially 500 million people, over a period of four years.

132. Moreover, the law imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of personal and confidential information to Plaintiff and the

Breach Class, so Plaintiff and Breach Class members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their information.

133. Defendants breached their duty to notify Plaintiff and Breach Class of the unauthorized access by failing to notify them of the data breach until November 30, 2018. To date, although it has been months since the breach was discovered, and four years since the breach commenced, Defendants have not provided sufficient information to Plaintiff and Breach Class regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Breach Class.

134. As a direct result of Defendants' negligent conduct, Plaintiff and Breach Class members have suffered and will continue to suffer an increased risk of identity theft. In fact, identity theft is a reasonably probable result of Defendants' conduct.

135. Unlike some data breaches where the motives behind the breach are unclear (*e.g.*, breaking into a car that also contains an unencrypted corporate laptop), the motivation and purpose of this breach is unquestionable: to use the information obtained to cause harm to putative Class members. Not only is the intent clear, but the likelihood of harm occurring in the future is a near certainty.

136. But for Defendants' failure to secure this data, Plaintiff and Breach Class members would not have suffered this harm and be exposed to ongoing harm.

137. It is reasonably foreseeable that Defendants' practices, including storing personal information in the manner described above, would put customers at a seriously increased risk of identity theft.

138. Accordingly, Plaintiff seeks the creation of a fund in the amount required to pay for adequate class-wide monitoring of this data breach, as well as for all precautions now necessary as a result of Defendants' negligent conduct.

FIFTH CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiff and the Classes)

139. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

140. Defendants solicited and invited Plaintiff and the Classes to share personal information such as dates of birth, passport numbers, credit and debit card numbers and other payment data, employer details, geolocation information, and other personal and confidential information as described herein, when they booked a room.

141. When Plaintiff and Classes provided their personal and confidential information to Defendants when they booked a room, they entered into implied contracts with the Defendants, pursuant to which Defendants agreed to safeguard to protect their information, and to timely and accurately notify Plaintiff and the Classes if their data had been breached or compromised.

142. Plaintiffs and the Classes would not have provided and entrusted their personal and confidential information to Defendants in connection with booking a room in the absence of the implied contract between them.

143. Defendants breached the implied contracts it made with Plaintiff and the Classes by failing to safeguard and protect the personal and confidential information of Plaintiff and Classes and by failing to provide timely and accurate notice to them that their information was compromised in and as a result of the data breach.

144. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and the Classes sustained actual losses and damages as described in detail herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Donna Hiteshew, on behalf of herself and the Classes, respectfully requests that this Court issue an order:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiff Hiteshew as representative of the Classes, and appointing her counsel as class counsel;

B. Declaring that Defendants' actions, as described herein, constitute (i) violations of the MCPA, (ii) violations of the PIPA, (iii) negligence, and (iv) breach of implied contract;

C. Creating a Data Privacy Monitoring Fund in an amount necessary to pay for and protect the ongoing interests of the putative Classes;

Injunctive Relief Requested

D. Enter an injunction requiring Defendants to stop the continued exposure, described herein, of the sensitive information in Defendants' possession until such time that Defendants can confirm and demonstrate that their online systems are secure. An injunction requiring Defendants to protect sensitive information until the above-described vulnerability is addressed (even if it means briefly taking its databases off-line) will protect the putative Classes because (i) Plaintiff's (and others') information would no longer be exposed; (ii) the risk of another data breach (to the extent one has not already occurred) would be significantly diminished; and, assuming the vulnerability is addressed, (iii) this case may proceed without the threat of further and on-going irreparable harm to Plaintiff and the Classes;

E. Enter an injunction requiring Defendants to stop improperly communicating with members of the putative Classes and stop directing them to enter into an agreement the deceptively and improperly limits their rights, and further, declare that the arbitration agreement

and class waiver present in the WebWatcher Terms of Service does not limit the rights of putative class members to pursue legal action against Defendants;

F. Enter an injunction requiring Defendants to verifiably protect all consumer data collected through the course of their business in accordance with industry-standards;

G. Plaintiff and the putative Classes are likely to suffer irreparable harm in the absence of injunctive relief;

Damages

H. Awarding appropriate damages and restitution to Plaintiff and the Classes in an amount to be determined at trial;

I. Awarding Plaintiff and the Classes their reasonable litigation expenses and attorneys' fees;

J. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable; and

K. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully Submitted,

DONNA HITESHEW, individually and on behalf of all others similarly situated,

Dated: December 6, 2018

By: /s/ Jeffrey M. Mervis
One of Plaintiff's Attorneys

Rafey S. Balabanian*
rbalabanian@edelson.com
Eve-Lynn Rapp*
erapp@edelson.com
EDELSON PC
123 Townsend Street, Suite 100
San Francisco, California 94107
Tel: 415.212.9300

Fax: 415.373.9435

Jay Edelson*
jedelson@edelson.com
Benjamin H. Richman**
brichman@edelson.com
Christopher L. Dore*
cdore@edelson.com
David I. Mindell*
dmindell@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Jeffrey M. Mervis (Bar No. 10180)
jmervis@mervislaw.com
THE MERVIS LAW FIRM, LLC
12505 Park Potomac Avenue, 6th Floor
Potomac, Maryland 20854
Tel: 301.762.0020
Fax: 301.762.0229

*Admission to be sought.

**Admission pending.

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

DONNA HITESHEW, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Allegheny County, PA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

The Mervis Law Firm, LLC; 12505 Park Potomac Avenue, 6th Floor, Potomac Maryland 20854; Tel: 301.762.0020

DEFENDANTS

MARRIOTT INTERNATIONAL, INC. and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC,

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
❒ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability			❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		PROPERTY RIGHTS	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	PERSONAL PROPERTY		❒ 820 Copyrights	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	LABOR	❒ 830 Patent	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 710 Fair Labor Standards Act	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	❒ 380 Other Personal Property Damage	❒ 720 Labor/Management Relations	SOCIAL SECURITY	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 740 Railway Labor Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit
❒ 190 Other Contract	☒ 360 Other Personal Injury		❒ 751 Family and Medical Leave Act	❒ 862 Black Lung (923)	❒ 490 Cable/Sat TV
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 790 Other Labor Litigation	❒ 863 DIWC/DIWW (405(g))	❒ 850 Securities/Commodities/ Exchange
❒ 196 Franchise			❒ 791 Employee Retirement Income Security Act	❒ 864 SSID Title XVI	❒ 890 Other Statutory Actions
				❒ 865 RSI (405(g))	❒ 891 Agricultural Acts
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	❒ 893 Environmental Matters
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	Habeas Corpus:	❒ 462 Naturalization Application	❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 895 Freedom of Information Act
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee	❒ 465 Other Immigration Actions	❒ 871 IRS—Third Party 26 USC 7609	❒ 896 Arbitration
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			❒ 950 Constitutionality of State Statutes
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty			
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	Other:			
	❒ 448 Education	❒ 540 Mandamus & Other			
		❒ 550 Civil Rights			
		❒ 555 Prison Condition			
		❒ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332(d)

Brief description of cause:
Maryland Consumer Protection Act and Personal Information Protection Act, negligence, breach of implied contract.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 12/06/2018

SIGNATURE OF ATTORNEY OF RECORD Jeffrey M. Mervis

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Maryland

DONNA HITESHEW, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

MARRIOTT INTERNATIONAL, INC., a Delaware corporation, and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC, a Maryland limited liability company,

Defendant(s)

Civil Action No. 8:18-cv-03755

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* MARRIOTT INTERNATIONAL, INC.
c/o Registered Agent
THE CORPORATION TRUST INCORPORATED
2405 YORK ROAD
SUITE 201
LUTHERVILLE TIMONIUM MD 21093-2264

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Benjamin H. Richman
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 8:18-cv-03755

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Maryland

DONNA HITESHEW, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

MARRIOTT INTERNATIONAL, INC., a Delaware corporation, and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC, a Maryland limited liability company,

Defendant(s)

Civil Action No. 8:18-cv-03755

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* STARWOOD HOTELS & RESORTS WORLDWIDE, LLC
c/o Registered Agent
THE CORPORATION TRUST INCORPORATED
2405 YORK ROAD
SUITE 201
LUTHERVILLE TIMONIUM MD 21093-2264

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Benjamin H. Richman
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 8:18-cv-03755

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset