UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

PETER TAPLING and DAVID SPARKS, individually and on behalf of all others similarly situated, Plaintiffs, v. MARRIOTT INTERNATIONAL, INC., Defendant.	Case No. COMPLAINT AND DEMAND FOR JURY TRIAL

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Marriott International, Inc. (referred to herein as "Marriott" or "Defendant"), parent of Starwood Hotels & Resorts Worldwide, LLC (referred to herein as "Starwood"), for Starwood's failure to secure and safeguard its customers' personally identifiable information ("PII") such as the passport information, customers' names, mailing addresses, and other personal information, as well as credit and debit card numbers and other payment card data ("PCD") (collectively, "Private Information"). Starwood collected this information at the time customers registered on its website, checked-in to one of its hotels, used its loyalty program (the "Loyalty Program"), and/or used it at one of its dining or retail operations within its hotels. Starwood also failed to provide timely, accurate, and adequate notice to Plaintiffs and other Class Members that their Private Information had been stolen, as well as precisely what types of information were stolen. When consumers provided information in their Starwood accounts or checked in to Starwood hotels, Starwood (now Marriott) electronically

collected and stored this information, making it a treasure trove of useful information attractive to hackers who used the information to profit and cause damage, as was done here, to consumers.

2. Beginning in or around 2014 (and perhaps even earlier) and continuing through November 2018, hackers exploiting vulnerabilities in Starwood's network accessed the guest reservation system at Starwood hotels and stole this data (the "Data Breach").

3. On November 30, 2018, Marriott acknowledged an investigation had determined that there was unauthorized access to the Starwood guest reservation database, which contained guest information relating to reservations at Starwood properties on or before September 10, 2018.

4. Marriott has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates.

5. Marriott could have prevented this Data Breach. Numerous other hotel chains, including Hilton, Starwood (previously), Kimpton, Mandarin Oriental, White Lodging (on two occasions), and the Trump Collection, have been hit with similar data breaches. While many retailers, banks, and card companies responded to recent breaches by adopting technology that helps makes transactions and databases more secure, Starwood and Marriott did not.

6. Marriott disregarded Plaintiffs' and Class Members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its

data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Private Information. On information and belief, Plaintiffs' and Class Members' Private Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs' and Class Members' Private Information was compromised and stolen. However, as this same information remains stored in Marriott's computer systems, Plaintiffs and Class Members have an interest in ensuring that their information is safe, and they are entitled to seek injunctive and other equitable relief, including independent oversight of Marriott's security systems.

PARTIES

7. Plaintiff Peter Tapling is a citizen and resident of the State of Illinois and a frequent user of the Defendant's Loyalty Program, having been a member for at least 31 years. Mr. Tapling provided his personal and confidential information to the Defendant on the basis that they would keep his information secure, and employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. On November 30, 2018, Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Mr. Tapling is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised.

8. Plaintiff David Sparks is a citizen and resident of the State of California and a frequent user of the Defendant's Loyalty Program, having been a member for over a decade. Mr. Sparks provided his personal and confidential information to the Defendant on the basis that they

would keep his information secure, and employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. As of November 30, 2018, Mr. Sparks still awaits notification from the Defendant that his information was compromised; however, based upon information publicly available to him, Mr. Sparks believes that his information was involved in the Data Breach. Aa result of the Data Breach, Mr. Sparks is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised.

9. Marriott International, Inc. is a Delaware corporation with its principal place of business in Bethesda, MD. Marriott primarily derives its revenues from hotel and restaurant operations. Starwood is now a wholly-owned subsidiary of Defendant Marriott.

JURISDICTION AND VENUE

10. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00, exclusive of interest and costs, and this is a class action in which more than two-thirds of the proposed plaintiff class, on the one hand, and Marriott, on the other, are citizens of different states.

11. This Court has jurisdiction over Marriott as it maintains its corporate headquarters in this District and for the following reasons: Marriott makes decisions regarding overall corporate governance and management with regards to the hotels that it owns or manages, including the security measures to protect its customers' Private Information, in this District; it is authorized to conduct business throughout the United States, including Maryland; it owns and operates many hotels throughout Maryland and the United States; and it advertises in a variety of media throughout the United States, including Maryland. Via its business operations throughout

the United States, Marriott intentionally avails itself of the markets within this state to render the exercise of jurisdiction by this Court just and proper.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and because Marriott is headquartered in this District.

FACTUAL BACKGROUND

A. Marriott Gathers Massive Amounts of Private Information from Its Guests.

13. The Marriott hotel chain operates more than 6,700 properties around the world.

14. In November 2015, Marriott announced that it was purchasing Starwood for $13.6 billion, creating the world's largest hotel empire.[1]

15. Starwood includes the following hotel brands: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels, as well as Starwood-branded timeshare properties.[2]

16. Starwood's reservation system is purportedly separate from other Marriott-branded hotels' systems, but the company has plans to merge the two systems.[3]

17. Marriott maintains a privacy policy available on its website:

---

[1] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," The New York Times, *available at* https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last accessed November 30, 2018).

[2] Starwood Guest Reservation Database Security Incident website, *available at* https://answers.kroll.com/ (last accessed November 30, 2018).

[3] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," The New York Times, *available at* https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last accessed November 30, 2018).

This Privacy Statement describes the privacy practices of the Marriott Group for data that we collect:

- through websites operated by us from which you are accessing this Privacy Statement, including Marriott.com and other websites owned or controlled by the Marriott Group (collectively, the "**Websites**")
- through the software applications made available by us for use on or through computers and mobile devices (the "**Apps**")
- through our social media pages that we control from which you are accessing this Privacy Statement (collectively, our "**Social Media Pages**")
- through HTML-formatted email messages that we send you that link to this Privacy Statement and through your communications with us
- when you visit or stay as a guest at one of our properties, or through other offline interactions

Collectively, we refer to the Websites, the Apps and our Social Media Pages, as the "**Online Services**" and, together with offline channels, the "**Services.**" By using the Services, you agree to the terms and conditions of this Privacy Statement.

"**Personal Data**" are data that identify you as an individual or relate to an identifiable individual.

At touchpoints throughout your guest journey, we collect Personal Data in accordance with law, such as:

- Name
- Gender
- Postal address
- Telephone number
- Email address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference
- Date 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

In more limited circumstances, we also may collect:

- 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

If you submit any Personal Data about other people to us or our Service Providers (e.g., if you make a reservation for another individual), you represent that you have the authority to do so and you permit us to use the data in accordance with this Privacy Statement.[4]

18. Marriott stores massive amounts of PII and PCD on its servers and utilizes this information to maximize its profits through predictive marketing and other marketing techniques.

19. Consumers place value in data privacy and security, and they consider it when making decisions on where to stay for travel. Plaintiffs would not have stayed at the Starwood hotels nor would they have used their debit or credit cards to pay for their Starwood stays had they known that Marriott does not take all necessary precautions to secure the personal and financial data given to it by consumers.

20. Marriott failed to disclose its negligent and insufficient data security practices and consumers relied on or were misled by this omission into paying, or paying more, for accommodations at Starwood.

B. Marriott Takes Four Years to Discover the Data Breach and Delays Informing Those Impacted.

[4] https://www.marriott.com/about/privacy.mi (last accessed November 30, 2018).

21. According to Marriott's statement and current news reports, on September 8, 2018, Marriott received an alert from an internal system that there was an attempt to access the Starwood guest reservation database.[5]

22. Marriott began to investigate the attempt and learned that unauthorized users had gained access to the Starwood network since 2014 – *four years* before detection.[6]

23. The investigation further revealed that the unauthorized users had copied and encrypted information, as well as attempted to remove (or "exfiltrate") it.[7]

24. On November 19, 2018, Marriott decrypted the information and confirmed that the contents were from its Starwood guest reservation database.[8]

25. Marriott has confirmed that, subject to de-duplicating its records, approximately 500 million guests who made a reservation at a Starwood property since 2014 may have been impacted.[9]

26. The database contains approximately 327 million guests' information including some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.[10]

27. For other guests, the information also includes payment card numbers and payment card expiration dates.

---

[5] https://answers.kroll.com/ (last accessed November 30, 2018).
[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," The New York Times, *available at* https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last accessed November 30, 2018).
[10] *Id*.

28. Other guests' accounts included a name and potentially a mailing address, email address, or other information.

29. According to Gus Hosein, executive director of Privacy International, "It's astonishing how long it took them to discover they were breached. For four years, data was being pilfered out of the company and they didn't notice. They can say all they want that they take security seriously, but they don't if you can be hacked over a four-year period without noticing."[11]

C. Stolen Private Information Is Valuable to Hackers and Thieves.

30. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. PII data is often easily taken because it may be less protected and regulated than payment card data. In the hospitality industry, and as identified earlier, many hotel chains were the targets of data breaches. Moreover, Marriott—along with the other hotel chains that were hacked—was aware or should have been aware of the federal government's heightened interest in securing consumers' PII when staying in hotels located in the United States due to the very public litigation commenced by the Federal Trade Commission against Wyndham Worldwide Corporation founded upon that company's failure to provide reasonable cybersecurity protections for customer data. Despite this well-publicized litigation and the frequent public announcements of data breaches by retailers and hotel chains, Marriott opted to maintain an insufficient and inadequate system to protect the PII of Plaintiffs and Class Members.

[11] *Id*.

31. In fact, in August of this year, the U.S. Department of Justice indicted members of an Eastern European cybercrime ring called Fin7, which targeted, *inter alia*, hotel chains.[12]

32. According to Richard Gold, head of security engineering at the cybersecurity firm Digital Shadows, "hotels are an attractive target for hackers because they hold a lot of sensitive information, including credit card and passport details, but often don't have security standards as tough as those of more regulated industries, like banking."[13]

33. Mr. Gold put this breach "among the largest of consumer data, on par with breaches at Yahoo and the credit-storing giant, Equifax."[14]

34. Legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn't aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[15] Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

35. Biographical data is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id.* PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of theft and unauthorized access have been the subject of many media reports. One form of identity theft, branded "synthetic identity theft," occurs when thieves create

---

[12] *Id*.
[13] *Id*.
[14] *Id*.
[15] Verizon 2014 PCI Compliance Report, available at <http://www.nocash.info.ro/wp-content/uploads/2014/02/ Verizon_pci-report-2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited Sept. 24, 2014).

new identities by combining real and fake identifying information then use those identities to open new accounts. “This is where they’ll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of a bionic person,” said Adam Levin, Chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft, experts said: “It’s tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person.” In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

36. Unfortunately, and as is alleged below, despite all this publicly available knowledge of the continued compromises of PII in the hands of third parties, such as hoteliers, Marriott’s approach at maintaining the privacy of Plaintiffs’ and Class Members’ PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

D. Marriott Failed to Segregate PCD From PII.

37. Unlike PII data, PCD is heavily regulated. The Payment Card Industry Data Security Standard (“PCI DSS”) is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

38. “PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data.”[16]

39. One PCI DSS requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code. “Network segmentation of, or isolating (segmenting), the cardholder data environment from the

[16] PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY DATA SECURITY STANDARD VERSION 2.0 at 5 (October 2010) (hereafter PCI Version 2).

remainder of an entity's network is not a PCI DSS requirement."[17] However, segregation is recommended because, among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data."[18]

40. Illicitly obtained PII and PCD, sometimes aggregated from different data breaches, are sold on the black market, including on websites, as products at a set price.[19]

41. Without such detailed disclosure, Plaintiffs and Class Members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

42. Marriott has failed to provide a cogent picture of how the Data Breach occurred and its full effects on consumers' PII and PCD information.

43. Hacking is often accomplished in a series of phases, including reconnaissance; scanning for vulnerabilities and enumeration of the network; gaining access; escalation of user, computer and network privileges; maintaining access; covering tracks; and placing backdoors. On information and belief, while hackers scoured Marriott's networks to find a way to access PCD, they had access to and collected the PII stored on Marriott's networks.

44. The Data Breach was caused and enabled by Marriott's knowing violation of its obligations to abide by best practices and industry standards in protecting its customers' Private Information.

45. In this regard, more than likely the software used in the attack was a variant of "BlackPOS," a malware strain designed to siphon data from cards when they are swiped at

---

[17] *Id.* at 10.

[18] *See* Verizon Report at 54.

[19] *See, e.g.*, Brian Krebs, *How Much Is Your Identity Worth?*, KREBSONSECURITY.COM (Nov. 8, 2011), https://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/ (last visited January 18, 2016).

infected point-of-sale systems. Hackers previously utilized BlackPOS in other recent cyber-attacks, including breaches at Home Depot and Target. While many retailers, banks, and card companies have responded to these recent breaches by adopting technology and security practices that help makes transactions and stored data more secure, Marriott has acknowledged that it did not do so.

E. This Data Breach Will Result In Additional Identity Theft and Identify Fraud.

46. Marriott failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach.

47. The ramifications of Marriott's failure to keep Plaintiffs' and Class Members' data secure are severe.

48. The information Marriott compromised, including Plaintiffs' identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[20] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration date, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account [as occurred to Plaintiffs here], run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[21]

---

[20] FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf (last visited Sept. 24, 2014).

[21] FTC, Signs of Identity Theft, *available at* http://www.consumer.ftc.gov/articles/ 0271-signs-identity-theft (last visited November 30, 2018).

49. According to Javelin Strategy and Research, "1 in 4 notification recipients became a victim of identity fraud."[22] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

50. Identity thieves can use personal information such as that of Plaintiffs and Class Members, which Marriott failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years. The IRS paid out 43.6 billion in potentially fraudulent returns in 2012, and the IRS identified more than 2.9 million incidents of identity theft in 2013. The IRS has described identity theft as the number one tax scam for 2014.

51. Among other forms of fraud, identity thieves may get medical services using consumers' compromised personal information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

52. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving

[22] See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, *available at* www.javelinstrategy.com/brochure/276 (last visited November 30, 2018) (the "2013 Identity Fraud Report").

problems."[23] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."[24]

F. Annual monetary Losses from Identity Theft are in the Billions of Dollars.

53. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[25]

54. There may be a time lag between when harm occurs versus when it is discovered, and between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

55. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether such charges are ultimately reimbursed by the credit card companies.

G. Marriott Has Already Botched Its Post-Data Breach Response.

---

[23] Victims of Identity Theft, 2012 (Dec. 2013) at 10, *available at* http://www.bjs.gov/content/pub/pdf/vit12. pdf (last visited Sept. 24, 2014).

[24] *Id*. at 11.

[25] *See* 2013 Identity Fraud Report.

[26] GAO, Report to Congressional Requesters, at p.33 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (emphases added) (last visited Sept. 24, 2014).

56. While Marriott set up a dedicated website and call center to handle inquiries following its announcement of the Data Breach, the incredible number of impacted guests has meant long wait times, and the lack of information about who was impacted and how has left guests confused and worried.

57. Further, the one year of free enrollment in Web Watcher only applies to guests who live in the United States, Canada, and Britain and is not a credit monitoring service. Web Watcher merely "keeps an eye on internet sites where thieves swap and sell personal information and then alerts people if anyone is selling their information."[27]

58. As an initial matter, Marriott appears to misapprehend how the sale of stolen data works. Nearly all sales of stolen data occur on the Deep Web. The Deep Web is not Google. While the internet as most people know it contains at least 4.5 billion websites indexed by search engines, the Deep Web is 400 to 500 times larger, according to estimates, and is not indexed.[28] Web Watchers' service may detect some sales on the Deep Web, but cannot alone identify and prevent identity theft.

59. Moreover, data thieves are aware of the one-year expiration period associated with Marriott's offer. As explained herein, thieves will often wait years to purchase and use stolen data, waiting for the clock to run out on monitoring services.[29]

---

[27] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," The New York Times, *available at* https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last accessed November 30, 2018).

[28] Mae Rice, "The Deep Web Is the 99% of the Internet You Can't Google," Curiousity, *available at* https://curiosity.com/topics/the-deep-web-is-the-99-of-the-internet-you-cant-google-curiosity/ (last accessed November 30, 2018).

[29] *See, e.g.*, Matt Tatham, "A Year After the Equifax Breach: Are You Protecting Your Data?", *available at* https://www.experian.com/blogs/ask-experian/a-year-after-the-equifax-breach-are-you-protecting-your-data/ (last accessed November 30, 2018).

60. Finally, the rollout of signup for the service confused many customers, who complained that the user interface was unclear.[30]

H. Plaintiffs and Class Members Suffered Damages.

61. The Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Marriott's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

62. Plaintiffs' and Class members' PII is private and sensitive in nature and was left inadequately protected by Marriott. Marriott did not obtain Plaintiffs' and Class Members' consent to disclose their PII to any other person as required by applicable law and industry standards.

63. As a direct and proximate result of Marriott's wrongful action and inaction and the resulting Data Breach, Plaintiffs (as was addressed above) and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying

[30] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," The New York Times, *available at* https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last accessed November 30, 2018).

financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

64. Marriott's "deep[] regret [for] this incident" is no comfort to Plaintiffs and Class Members, though undoubtedly they agree that Marriott "fell short of what [its] guest deserve . . ."[31]

65. Marriott's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their passport, credit/debit card, and personal information being placed in the hands of criminals;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

[31] *Id*.

h. overpayments to Marriott for products and services purchased during the Data Breach in that a portion of the price paid for such products and services by Plaintiffs and Class Members to Marriott was for the costs of reasonable and adequate safeguards and security measures that would protect customers' Private Information, which Marriott did not implement and, as a result, Plaintiffs and Class members did not receive what they paid for and were overcharged by Marriott;

i. the loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and

j. deprivation of rights they possess under the various state statutes.

66. While the Private Information of Plaintiffs and members of the Class has been stolen, the same or a copy of the Private Information continues to be held by Marriott. Plaintiffs and Class Members have an undeniable interest in insuring that this information is secure, remains secure, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

67. Plaintiffs seek relief in their individual capacities and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of a Nationwide class as described herein. The national class is initially defined as follows: all persons residing in the United States whose personal and/or financial information was disclosed in the Data Breach affecting Marriott from 2014 to 2018 (the "Nationwide Class").

68. Excluded from each of the Class are Marriott, including any entity in which Marriott has a controlling interest, is a parent or subsidiary, or which is controlled by Marriott, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Marriott. Also excluded are the judges and court personnel in this case and any members of their immediate families.

69. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, Marriott has acknowledged that information of over 500 million customers may have been compromised.

70. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Marriott violated the various state Deceptive and Unfair Trade Practices Act by failing to implement reasonable security procedures and practices;

b. Whether Marriott violated laws by failing to promptly notify class members their personal information had been compromised;

c. Whether class members may obtain injunctive relief against Marriott under privacy laws to require that it safeguard or destroy, rather than retain, the Private Information of Plaintiffs and Class members;

d. Which security procedures and which data-breach notification procedure should Marriott be required to implement as part of any injunctive relief ordered by the Court;

e. Whether Marriott has an implied contractual obligation to use reasonable security measures;

f. Whether Marriott has complied with any implied contractual obligation to use reasonable security measures;

g. What security measures, if any, must be implemented by Marriott to comply with its implied contractual obligations;

h. Whether Marriott violated state privacy laws in connection with the actions described herein; and

i. What the nature of the relief should be, including equitable relief, to which Plaintiffs and the Class members are entitled.

71. All members of the proposed Class are readily ascertainable. Marriott has access to addresses and other contact information for millions of members of the Class, which can be used for providing notice to many Class members.

72. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other Class Member, was misused and/or disclosed by Marriott.

73. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation.

74. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting

adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

75. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Marriott's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

76. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Marriott has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

77. Plaintiffs incorporate the substantive allegations contained in paragraphs 1 through 76 as if fully set forth herein.

78. Defendant solicited and invited Plaintiffs and Class Members to join its Loyalty Program, which required that Plaintiffs and Class members 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.

79. Defendant then invited Plaintiffs and Class Members to continually use its Loyalty Program to book rooms, and earn and redeem rewards. Plaintiffs and Class Members accepted certain offers made by Defendant in connection with use of the Loyalty Program,

continuing to allow Defendant to store, maintain, and safeguard their personal and confidential information.

80. When Plaintiffs and Class Members provided their personal and confidential information to Defendant in connection with joining the Loyalty Program, they entered into implied contracts with the Defendant, pursuant to which Defendant agreed to safeguard to protect their information, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached or compromised.

81. Plaintiffs and Class Members would not have provided and entrusted their personal and confidential information to Defendant in connection with joining Defendant's loyalty program in the absence of the implied contract between them.

82. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

83. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the personal and confidential information of Plaintiffs and Class Members 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.

84. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

SECOND CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

85. Plaintiffs incorporate the substantive allegations contained in paragraphs 1 through 76 as if fully set forth herein.

86. Upon accepting and storing Plaintiffs' and Class Members' personal and confidential information in its respective computer database systems, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Defendant knew, acknowledged, and agreed the information was private and confidential and would be protected as private and confidential.

87. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of personal and confidential information to Plaintiffs and the Class so Plaintiffs and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their information.

88. Defendant breached its duty to notify Plaintiffs and Class Members of the unauthorized access by failing to notify Plaintiffs and Class Members 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, Defendant has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

89. Defendant also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to Plaintiffs' and Class Members' Private Information. Furthering its dilatory practices, Defendant failed to provide adequate oversight of the Private Information to which it was entrusted, resulting in a massive breach of the personal and confidential information of potentially 500 million people, undetected over a period of four years.

90. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' personal and confidential information from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' information during the time it was within Defendant's possession or control.

91. Further, through Defendant's failure to provide timely and clear notification of the Data Breach to consumers, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

92. Upon information and belief, Defendant improperly and inadequately safeguarded the personal and confidential information of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

93. Defendant's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive personal and confidential information violated its duty to protect that data and prevent its dissemination to third parties.

94. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of the Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendant did not protect Plaintiffs' and Class Members' information from hackers.

95. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting

commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

96. Defendant's acknowledged the importance of keeping this information secure, and stated that they sought 'to use reasonable organizational, technical and administrative measures to protect Personal Data."[32] Despite acknowledging their responsibility to keep this information secure, Defendant improperly put the burden on Plaintiffs' and Class Members to notify *Defendant* if they suspected that their information was not secure, when individuals would not have access to this information, and Defendant was in a superior position to know this information, and were in the exclusive possession of such information.[33]

97. Upon information and belief, Defendant improperly and inadequately safeguarded the personal and confidential information of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

98. Defendant's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive personal and confidential information has caused Plaintiffs and Class Members to suffer injury and damages. As described herein, the Plaintiffs received notice that their information was compromised, and now must take and have taken affirmative steps to ensure that their identity is not stolen and their financial information is not compromised.

THIRD CAUSE OF ACTION
MARYLAND PERSONAL INFORMATION PROTECTION ACT
Md. Comm. Code §§ 14-3501, *et seq.*

---

[32] *See* Privacy Center, Marriott Group Global Privacy Statement, https://www.marriott.com/about/privacy.mi (last accessed Nov. 30, 2018).

[33] *Id.*

(On Behalf of Plaintiffs and the Nationwide Class)

99. Plaintiffs incorporate the substantive allegations contained in paragraphs 1 through 76 as if fully set forth herein.

100. Included in the terms and conditions of the Loyalty Program is a Choice of Law and Venue Provision that provides that Maryland law applies to the Loyalty Program.

101. Under Md. Comm. Code § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations."

102. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

103. Plaintiffs and Class Members are "individuals" and "customers" as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

104. Plaintiffs' and Class Members' Private Information, as described herein and throughout, includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

105. Defendant did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

106. The Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(1).

107. Under Md. Comm. Code § 14-3504(b)(1), "[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."

108. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), "[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."

109. Because Defendant discovered a security breach and had notice of a security breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

110. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

111. As a direct and proximate result of Defendant's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiffs and Class Members suffered damages, as described above.

112. Pursuant to Md. Comm. Code § 14-3508, Defendant's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101, *et seq.* and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

113. Plaintiffs and Class Members seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

FOURTH CAUSE OF ACTION
MARYLAND CONSUMER PROTECTION ACT,
Md. Comm. Code §§ 13-301, *et seq.*
AND APPLICABLE STATE CONSUMER PROTECTION ACTS AND UNFAIR BUSINESS PRACTICES ACTS
(On Behalf of Plaintiffs and the Nationwide Class)

114. Plaintiffs incorporate the substantive allegations contained in paragraphs 1 through 76 as if fully set forth herein.

115. Included in the terms and conditions of the Loyalty Program is a Choice of Law and Venue Provision that provides that Maryland law applies to the Loyalty Program.

116. To the extent Maryland law does not apply, Plaintiffs bring this claim on behalf of themselves and Class Members on behalf of applicable state consumer protection and deceptive business practices acts.

117. Defendant is a "person" as defined by Md. Comm. Code § 13-101(h).

118. Defendant's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

119. Plaintiffs and Class Members are "consumers" as defined by Md. Comm. Code § 13-101(c).

120. Defendant advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

121. Defendant advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

122. Defendant engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Failing to state a material fact where the failure deceives or tends to deceive;

c. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

d. 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, sale lease or rental.

123. Defendant engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Comm. Code § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' personal and confidential information, which was a direct and proximate cause of the Data Breach;

b. 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, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal and

confidential information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' personal and confidential information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e,

the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

124. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal and confidential information. Defendant's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

125. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

126. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in Loyalty Program and it would have been forced to adopt reasonable data security measures and comply with the law.

127. Defendant acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Class Members' rights. Defendant was on notice of the possibility of the Data Breach due to its prior data breach and infiltrations of its systems in the past.

128. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including 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 loss of value of their Personal Information.

129. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

REQUEST FOR RELIEF

130. **WHEREFORE**, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Marriott as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' personal and confidential information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiffs and Class members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class members the type of PII and PCD compromised.

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e. For an award of actual damages and compensatory damages, in an amount to be determined;

f. For an award of costs of suit and attorneys' fees, as allowable by law; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: November 30, 2018

Respectfully submitted,

/s/ Andrew N. Friedman

Andrew N. Friedman (admitted to D. Md. #14421)
Douglas J. McNamara (to file *pro hac vice*)
Sally Handmaker Guido (to file *pro hac vice*)
Eric A. Kafka (to file *pro hac vice*)
Julia A. Horwitz (Maryland Bar #19841)
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699
afriedman@cohenmilstein.com
dmcnamara@cohenmilstein.com
shguido@cohenmilstein.com
ekafka@cohenmilstein.com
jhorwitz@cohenmilstein.com

Adam J. Levitt (to file *pro hac vice*)
Amy E. Keller (to file *pro hac vice*)
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Telephine: (312) 214-7900
alevitt@dlcfirm.com
akeller@dlcfirm.com

James J. Pizzirusso (to file *pro hac vice*)
Megan E. Jones (Maryland Bar #15671)
HAUSFELD
1700 K St. NW, Suite 650
Washington, D.C. 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeld.com
mjones@hausfeld.com

Attorneys for Plaintiffs

JS 44 (Rev. 08/16)

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

PETER TAPLING & DAVID SPARKS, on behalf of themselves and all others similarly situated

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

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

See Attachment A.

DEFENDANTS

MARRIOTT INTERNATIONAL, INC.

County of Residence of First Listed Defendant Bethesda, MD
(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
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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) Class Action Fairness Act

Brief description of cause:
Nationwide class action regarding a data breach.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ Greater than $5,000,000

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 11/30/2018

SIGNATURE OF ATTORNEY OF RECORD _____

FOR OFFICE USE ONLY

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

ATTACHMENT A

Andrew N. Friedman (admitted to D. Md. #14421)
Douglas J. McNamara (to file *pro hac vice*)
Sally Handmaker Guido (to file *pro hac vice*)
Eric A. Kafka (to file *pro hac vice*)
Julia Horwitz (Maryland Bar #19841)
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
afriedman@cohenmilstein.com
dmcnamara@cohenmilstein.com
shguido@cohenmilstein.com

Adam J. Levitt (to file pro hac vice)
Amy E. Keller (to file pro hac vice)
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
312.214.7900
alevitt@dlcfirm.com
akeller@dlcfirm.com

James J. Pizzirusso (to file *pro hac vice*)
Megan E. Jones (Maryland Bar #15671)
HAUSFELD
1700 K St. NW, Suite 650
Washington, D.C. 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeld.com
mjones@hausfeld.com
iengdahl@hausfeld.com

Attorneys for Plaintiffs

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

UNITED STATES DISTRICT COURT

for the

District of Maryland

PETER TAPLING & DAVID SPARKS, on behalf of themselves and all others similarly situated

Plaintiff(s)

v.

MARRIOTT INTERNATIONAL, INC.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Marriott International, Inc.
10400 Fernwood Road
Bethesda, MD 20817

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:

Andrew N. Friedman
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave, Suite 500
Washington, D.C. 20009

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: 11/30/2018

Signature of Clerk or Deputy Clerk

Civil Action No.

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: