UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
GREENBELT DIVISION

RONALD N. WALTERS AND KENNETH TEW, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

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

Defendants.

Case No.: GJH 18 CV3804

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

I. INTRODUCTION

Plaintiffs Ronald N. Walters and Kenneth Tew ("Plaintiffs") bring this class action against Marriott International, Inc. (referred to herein as "Marriott" or "Marriott International"), parent of Starwood Hotels & Resorts Worldwide, LLC (referred to herein as "Starwood") (collectively, "Defendants"), 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"). Marriott and 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. Marriott and Starwood also failed to provide timely, accurate, and adequate notice to Plaintiffs and other Class Members (defined below) 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.

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").

On or about 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.

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.

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 make transactions and databases more secure, on information and belief Starwood and Marriott did not.

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; Plaintiffs' PCD was encrypted. 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.

II. THE PARTIES

A. Plaintiffs

1. Plaintiff and class representative Ronald N. Walters is a United States citizen and resident of Kanawaha County, West Virginia, and has been a long-time SPG member. Mr. Walters provided his personal and confidential information to Defendants on the basis that they would keep his information secure, 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, Plaintiff Walters was notified that his information was compromised by the Data Breach. Plaintiff Walters was notified of the breach again on December 10, 2018 by Marriott International. As a result of the Data Breach, Mr. Walters 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.

2. Plaintiff and class representative Kenneth Tew, Ph.D. is a dual citizen of the United States and the United Kingdom, and resident of Charleston County, South Carolina. Plaintiff Tew has been a long-time SPG member. Dr. Tew provided his personal and confidential information to Defendants on the basis that they would keep his information secure, 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, Plaintiff Tew was notified that his information was compromised by the Data Breach. As a result of the Data Breach, Dr. Tew 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.

B. Defendants

3. Defendant Marriott International, Inc. is a Delaware corporation with its principal place of business located in the State of Maryland at 10400 Fernwood Road, Bethesda, Maryland 20817.

4. Defendant Marriott operates, franchises, and licenses hotel, residential, and time share properties worldwide through various subsidiaries, each of which act as an agent of or in concert with Marriott.

5. Defendant Starwood Hotels & Resorts Worldwide, LLC is a subsidiary company of Marriott International, Inc., with its principal place of business at One StarPoint, Stamford, Connecticut.

III. JURISDICTION AND VENUE

6. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, because this suit is a class action, the parties are diverse, and the amount in controversy exceeds $5 million, excluding interest and costs. The Court has supplemental jurisdiction over the related state law claims pursuant to 28 U.S.C. § 1367.

7. Venue is proper under 28 U.S.C. §1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in the District of Maryland. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this district, including decisions made by Defendants Marriott and Starwood to permit the unauthorized collection of the personally identifiable information of the class.

IV. FACTUAL ALLEGATIONS

A. Background

8. Defendant Marriott is the largest hotel chain in the world, with more than 6,500 properties located in 127 countries and territories globally. Marriott owns and operates a variety of hotel, lodging, and hospitality brands, including hotels under its Starwood brands, which include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels. Hundreds of millions of customers have made reservations and stayed at Marriott properties around the globe.

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

10. 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]

11. When booking reservations at a Marriott property, including its Starwood brand properties, customers provide Marriott with sensitive PII, including their names, addresses, passport numbers and details, phone numbers, email addresses, dates of birth, gender, and credit card numbers with expiration dates.

12. Booking hotel reservations, and thus, collecting the PII of its customers, is therefore at the heart of Marriott's business.

13. Starwood's reservation system is purportedly separate from other Marriott-branded

---

[1] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," THE NEW YORK TIMES (NOV. 30, 2018), available at https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last visited Dec. 11, 2018).

[2] Starwood Guest Reservation Database Security Incident website, available at https://answers.kroll.com/ (last visited Dec. 11, 2018).

hotels' systems, but the company has plans to merge the two systems.[3]

14. Individuals who entrust Marriott with PII, which includes extremely sensitive data such as passport details and credit card information, do so with the understanding that Marriott will safeguard that information. That expectation is directly reinforced by Marriott, which publicly touts its commitment to safeguarding customers PII, including for example in its Marriott Group Global Privacy Statement, where it purports to "use reasonable organizational, technical and administrative measures to protect Personal Data."[4] Likewise, Defendants' Marriott U.S. Privacy Shield Guest Privacy Policy represents to customers that it will "use reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction."[5]

15. Marriott's privacy policy further states:

> 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.

---

[3] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," THE NEW YORK TIMES (NOV. 30, 2018), available at https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last visited Dec. 11, 2018).

[4] *See* https://www.marriott.com/about/privacy.mi (last visited Dec. 11, 2018).

[5] *See* https://www.marriott.com/about/global-privacy.mi (last visited Dec. 11, 2018).

"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.

16. Furthermore, on November 9, 2016, Marriott filed a Form 10-Q for the quarterly period ended September 30, 2016 with the United States Securities & Exchange Commission ("SEC"), which provided the following statement concerning the security of systems that store Marriott and Starwood customer data:

> Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. The integrity and protection of that customer, employee, and company data is critical to our business.
>
> * * *
>
> Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information.

17. On February 21, 2017, Marriott filed a Form 10-K for the fiscal year ended December 31, 2016 with the SEC, which provided the following statement concerning the security of systems that store Marriott and Starwood customer data:

> Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. The integrity and protection of that customer, employee, and company data is critical to our business.
>
> * * *
>
> Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information.

18. On February 15, 2018, Marriott filed a Form 10-K for the fiscal year ended December 31, 2017 with the SEC, which provided the following statement concerning the security of systems that store Marriott and Starwood customer data:

> *We are exposed to risks and costs associated with protecting the integrity and security of company employee and guest data.* Our businesses process, use, and transmit large volumes of employee and guest data, including credit card numbers and other personal information in various information systems that we maintain and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. The integrity and protection of that guest, employee, and company data is critical to our business.
>
> * * *
>
> Our guests and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information.

19. 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.

20. 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.

21. 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. The Data Breach

22. Despite its promises and commitments to safeguarding guests' PII, Defendant Marriott announced on November 30, 2018, that data for approximately 500 million guests was exposed in a hack that allowed unauthorized access to its Starwood Hotels reservation database since as early as 2014, and that hackers have actively copied and encrypted information from this database.[6]

---

23. The statement further revealed that Defendant initially discovered the Breach months earlier, on September 8, 2018.[7]

24. The Breach compromised "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 at least 327 million individuals, and names, mailing addresses and unidentified "other information" for at least 150 million other individuals.[8] For some, the information also included payment card numbers and payment card expiration dates.

25. The payment card information was encrypted using Advanced Encryption Standard (AES-128). Marriott has not publicly ruled out the possibility that unauthorized parties have bypassed AES-128.

26. At this time, it is unclear why the Breach was not discovered for four years, or why it took over two-and-a-half months for Marriott to verify and report the Breach to the victims whose PII had been stolen. Such a delay is damaging to the Breach's victims, in that they could have immediately acted in a manner to protect themselves and their PII from further harm.

27. 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."[9]

---

[6] "Marriott Announces Starwood Guest Reservation Database Security Incident," Marriott News Center (Nov. 30, 2018), available at http://news.marriott.com/2018/11/marriott-announces-starwoodguest-reservation-database-security-incident/ (last visited Dec. 11, 2018).

[7] *Id.*

[8] *Id.*

[9] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," THE NEW YORK TIMES (NOV. 30, 2018), available at

28. As Marriott's President and Chief Executive Officer Arne Sorenson has admitted, "[Marriott] fell short of what our guests deserve and what we expect of ourselves" in allowing this Breach to occur. "We are doing everything we can to support our guests, and using lessons learned to be better moving forward."[10]

C. Data Breaches Lead to Identity Theft

29. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. The FTC notes this information is "as good as gold" to identity thieves; and once identity thieves have this personal information, "they can drain your bank account, run up your credit cards, open new accounts, or get medical treatment on your health insurance."[11] 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

---

https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last visited Dec. 11, 2018).

[10] "Marriott Announces Starwood Guest Reservation Database Security Incident," Marriott News Center (Nov. 30, 2018), available at http://news.marriott.com/2018/11/marriott-announces-starwoodguest-reservation-database-security-incident/ (last visited Dec. 11, 2018).

[11] "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); *see also* FTC, "Signs of Identity Theft," available at http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last visited Dec. 11, 2018).

Members.

30. 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]

31. 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]

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

33. 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.

34. 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."[16] PII data has been stolen and sold by the criminal underground on many occasions in

---

[12] Amie Tsang & Adam Stariano, "Marriott Breach Exposes Data of Up to 500 Million Guests," THE NEW YORK TIMES (NOV. 30, 2018), available at https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last visited Dec. 11, 2018).

[13] *Id.*

[14] *Id.*

[15] Verizon 2014 PCI Compliance Report, at 54, available at http://www.verizonenterprise.com/resources/reports/rp_pci-report-2014_en_xg.pdf (hereafter "2014 Verizon Report") (last visited Dec. 11, 2018).

[16] *Id.*

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 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.

35. Unfortunately for Plaintiff and the Classes, a person whose PII has been compromised may not fully experience the effects of the breach for years to come:

> [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.[17]

36. The information implicated in the instant Breach is particularly susceptible to delay tactics in that an individual's name, address, and passport numbers are not easily changed to mitigate risk over time. Accordingly, Plaintiff and the Class Members will bear a heightened risk of identity theft or fraud for the unforeseeable future.

37. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from

---

[17] G.A.O., "Personal Information: Data Breaches are Frequent, But Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown" (June 2007), available at http://www.gao.gov/assets/270/262904.html.

unanticipated uses of data."[18]

38. 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 cavalier, reckless, or at the very least, negligent.

39. The risks associated with identity theft are serious. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, banking or finance fraud, and government fraud. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[19]

40. Having obtained the Plaintiff and Class Members' names, addresses, passport details, phone numbers, email addresses, dates of birth, gender, and credit card numbers and expiration dates, cybercriminals can simply use the data revealed or pair the data with other available information to commit a broad range of fraud in a victim's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing fraudulent tax returns;
- obtaining medical care and filing prescriptions;
- stealing Social Security and other government benefits; and

---

[18] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change (March 2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. (last visited Dec. 11, 2018).

[19] Seton Hall University, 'Identity Theft," available at https://www.shu.edu/technology/identity-theft.cfm (last visited Dec. 11, 2018).

- applying for a driver's license, birth certificate, or other public documents.

41. Having obtained the Plaintiff and Class Members' passports, cybercriminals can use the data to commit a broad range of fraud in a victim's name, including opening bank accounts, and illegally entering the country and masking their identity from the authorities.[20]

42. Beyond using the data exposed for nefarious purposes themselves, the cybercriminals who obtained Plaintiff and Class Members' PII may also exploit the data by selling it on the "black market" or "dark market" for years following a breach.

43. Indeed, there is a well-established international black market where hackers may quickly and efficiently sell—in part or in whole—precisely the type of PII stolen in the instant Data Breach.

44. Moreover, much like regular online marketplaces (such as eBay), many dark market websites (such as AlphaBay) include feedback systems for vendors, refund policies, and easily navigable search categories.[21]

45. Cybercriminals can further post stolen PII on the internet, thereby making such information publicly available.

46. Moreover, individuals whose PII is subject to a reported security breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud or identity theft.[22]

47. According to Javelin Strategy and Research, "1 in 4 [data breach] notification

---

[20] Gabriel Wood, "Common Forms of ID Criminal Use to Commit Identity Theft," available at https://www.nextadvisor.com/blog/common-forms-of-id-criminals-use-to-commit-identity-theft/. (last visited Dec. 11, 2018).

[21] Keith Collins, "Here's what your stolen identity goes for on the internet's black market," QUARTZ (July 23, 2015), available at https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-theinternets-black-market/. (last visited Dec. 11, 2018).

[22] Insurance Information Institute, "Data Breach Victims More Likely to Suffer Identity Fraud," (Feb. 23, 2012), available at http://www.iii.org/insuranceindustryblog/data-breach-victims-more-likely-to-suffer-identity-fraud/comment-page-1/ (last visited Dec. 11, 2018).

recipients became a victim of identity fraud."[23] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

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

D. PII versus PCD

49. 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.

50. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data."[25]

51. 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 remainder of an entity's network is not a PCI DSS requirement."[26] However, segregation is recommended because, among other reasons, "[i]t's not just cardholder data that's important;

---

[23] "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," available at www.javelinstrategy.com/brochure/276 (last visited Dec. 11, 2018).

[24] "Victims of Identity Theft, 2012" (Dec. 2013) at 10, available at http://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited Dec. 11, 2018).

[25] PCI Security Standards Council, "Payment Card Industry Data Security Standard Version 2.0" (October 2010), available at https://www.senseofsecurity.com.au/consulting/pci-compliance (last visited Dec. 11, 2018).

[26] *Id.*

criminals are also after personally identifiable information (PII) and corporate data."[27]

52. 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.

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

54. 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.

55. 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.

56. 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 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. Plaintiffs and Class Members Suffered Damages As A Result of the Data Breach

57. The Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiff and Class Members' PII against reasonably foreseeable threats to the security or integrity of such information.

[27] 2014 Verizon Report at 54.

58. Marriott failed to identify, implement, maintain, and monitor appropriate data security measures, polices, procedures, controls, protocols, and software and hardware systems to ensure the security of Plaintiff and Class Members' PII.

59. Additionally, Plaintiff and Class Members' PII was improperly handled, stored, segregated, and in some cases, either unencrypted or improperly partially encrypted, inadequately protected, readily able to be copied by data thieves, and not kept in accordance with basic security protocols.

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

61. Had Marriott taken appropriate security measures, the Data Breach would not have occurred.

62. Marriott's wrongful actions, inactions, and omissions directly and proximately caused the theft of Plaintiff and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harms for which they are entitled compensation, including, *inter alia*:

a. actual or attempted identity theft or fraud;
b. increased risk of harm, including actual identity theft and fraud;
c. the untimely and inadequate notification of the Data Breach;
d. improper disclosure of their PII;
e. diminution in the value of their PII;
f. loss of privacy;
g. 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 identity theft, identity fraud, and medical fraud;
h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to mitigate or avert the increased risk of identity theft, identity fraud, and medical fraud;
i. 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;
j. 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;

k. 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

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

63. Moreover, consumers value data security and are willing to pay more for services that come with data security. It is for this reason that Marriott goes to such lengths to assure customers that their PII is safe.

64. Studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49–44.62."[28] When consumers were surveyed regarding how much they value their PII in terms of its protection against improper access and unauthorized secondary use—the very concerns at issue here—they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[29]

65. 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.

F. Marriott's Offer of Credit Monitoring is Inadequate

66. At present, Marriott has offered one year of free enrollment in "WebWatcher," which monitors internet sites where PII is shared and generates alerts if evidence of the consumer's PII is found.

67. As previously alleged, consumers' PII may exist on the Dark Web for months, or

---

[28] Il-Horn Hann et al., "The Value of Online Information Privacy: An Empirical Investigation" (Oct. 2002), available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (emphasis added); Tsai, Cranor, Acquisti, and Egelman, "The Effect of Online Privacy Information on Purchasing Behavior," 22 (2) INFORMATION SYSTEMS RESEARCH 254, 254 (June 2011).

[29] *Id.*

even years, before it is used for ill gains and actions. With only one year of monitoring, and no form of insurance or other protection, Plaintiffs and Class members remain unprotected from the real and long-term threats against their PII.

68. Therefore, the "monitoring" services are inadequate, and Plaintiffs and Class Members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

V. CLASS ACTION ALLEGATIONS

69. Plaintiffs bring this class action claim pursuant to Rule 23 of the Federal Rules of Civil Procedure. The requirements of Rule 23 are met with respect to the class defined below.

70. Plaintiff Walters brings his claim on his own behalf, and on behalf of the following class (the "U.S. Class"):

> All citizens of the United States whose personal and/or financial information was disclosed in the Data Breach affecting Marriott and Starwood from 2014 to 2018.

71. Plaintiff Tew brings his claim on his own behalf, and on behalf of the following class (the "UK and EU Class"):

> All citizens of the United Kingdom and/or a country within the European Union whose personal and/or financial information was disclosed in the Data Breach affecting Marriott and Starwood from 2014 to 2018.

72. Excluded from each Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest, and Defendants' officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, and any member of the judge's immediate family.

73. Plaintiffs reserve the right to amend or modify the Class definitions in connection with a motion for class certification and/or the result of discovery.

74. This lawsuit is properly brought as a class action for the following reasons. The Class is so numerous that joinder of the individual members of the proposed Class is impracticable. Plaintiffs reasonably believe that the Class includes eighty-seven (87) million people or more in the aggregate and well over 1,000 in the smallest of the classes. The precise number and identities of Class members are unknown to Plaintiffs, but are known to Defendants and can be ascertained through discovery regarding the information kept by Defendants or their agents.

75. Questions of law or fact common to each Class exist as to Plaintiffs and all Class members, and these common questions predominate over any questions affecting only individual members of the Class. The predominant common questions of law and/or fact include the following:

a. Whether Defendants represented that they would safeguard Plaintiffs' and Class members' Personally Identifiable Information and not to disclose it without consent;

b. Whether Defendants were aware of the improper collection of Plaintiff's and Class members' Personally Identifiable Information;

c. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personally Identifiable Information;

d. Whether Defendants breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personally Identifiable Information;

e. Whether Class members' Personally Identifiable Information was obtained by unauthorized third-parties;

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

g. Whether the conduct of Defendants was in violation of the GDPR, or General Data Protection Regulation;

h. Whether Defendants' conduct violated Md. Comm. Code §§ 14-3501, *et seq.*.;

i. Whether Defendants' conduct was an unlawful and/or violated Md. Comm. Code §§ 13-301, *et seq.*;

j. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;

k. Whether Defendants breached their promises of privacy to their customers;

l. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

m. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

76. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs and the Class. Individual questions, if any, pale by comparison to the numerous common questions that predominate.

77. Plaintiffs' claims are typical of the claims of Class members. The injuries sustained by Plaintiffs and the Class flow, in each instance, from a common nucleus of operative facts based on the Defendants' uniform conduct as set forth above. The defenses, if any, that will be asserted against Plaintiffs' claims likely will be similar to the defenses that will be asserted, if any, against Class members' claims.

78. Plaintiffs will fairly and adequately protect the interests of Class members. Plaintiffs have no interests materially adverse to or that irreconcilably conflict with the interests of Class members and have retained counsel with significant experience in handling class actions and other complex litigation, and who will vigorously prosecute this action.

79. A class action is superior to other available methods for the fair and efficient group-wide adjudication of this controversy, and individual joinder of all Class members is impracticable, if not impossible. The cost to the court system of individualized litigation would be substantial. Individualized litigation would likewise present the potential for inconsistent or contradictory judgments and would result in significant delay and expense to all parties and multiple courts hearing virtually identical lawsuits. By contrast, a class

action presents fewer management difficulties, conserves the resources of the parties and the courts and protects the rights of each Class member.

80. Defendants have acted on grounds generally applicable to the entire Class, thereby making injunctive relief or corresponding declaratory relief appropriate with respect to the Class as a whole.

81. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether (and when) Defendants knew about the improper collection of Personally Identifiable Information;

b. Whether Defendants' representations that they would secure and not disclose without consent the Personally Identifiable Information of Plaintiffs and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Marriott International, Inc.'s services;

c. Whether Defendants misrepresented the safety of their many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs' and Class members' Personally Identifiable Information;

d. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

f. Whether Defendants breached their promises of privacy to their customers;

g. Whether Defendants failed to adhere to their posted privacy policy concerning the care they would take to safeguard Plaintiffs' and Class members' Personally Identifiable Information in violation of the Maryland Personal Information Protection Act, Md. Comm. Code §§ 14-3501, *et seq.*;

h. Whether Defendants negligently and materially failed to adhere to their posted privacy policy with respect to the extent of their disclosure of customers' data, in violation of the Maryland Consumer Protection Act, Md. Comm. Code §§ 13-301, *et seq.*;

i. Whether the conduct of Defendants was in violation of the GDPR, or General Data Protection Regulation;

COUNT ONE

Negligence as Against Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC

82. Plaintiffs hereby incorporate all the above allegations by reference as if fully set forth herein. Plaintiffs assert this count individually and on behalf of the proposed Class.

83. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining and protecting their Personally Identifiable Information, and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.

84. Defendants knew that the Personally Identifiable Information of Plaintiffs and the Class was personal and sensitive information that is valuable.

85. By being entrusted by Plaintiffs and the Class to safeguard their Personally Identifiable Information, Marriott International, Inc. had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up for Marriott International, Inc.'s services and agreed to provide their Personally Identifiable Information with the understanding that Marriott International, Inc. would take appropriate measures to protect it, and would inform Plaintiffs and the Class of any breaches or other security concerns that might call for action by Plaintiffs and the Class. But, Marriott International, Inc. did not. Marriott International, Inc. failed to prevent unauthorized individuals from improperly obtaining Plaintiffs' and the Class Members' Personally Identifiable Information.

86. Defendants breached their duties by failing to adopt, implement, and maintain adequate security measures to safeguard the Personally Identifiable Information, or by obtaining that Personally Identifiable Information without authorization.

87. Marriott International, Inc. breached its duties by allowing a third-party to access and obtain the Personally Identifiable Information of approximately 500 million customers that did not consent to provide this information.

88. Marriott International, Inc. also breached their duty to timely disclose that Plaintiffs' and the other class members' Personally Identifiable Information had been, or was reasonably believed to have been, improperly obtained. Marriott International, Inc. first discovered that its customers' information had been improperly obtained as early as 2014, but did not disclose the privacy breach until media pressure forced it to respond on November 30, 2018.

89. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and the Class, their Personally Identifiable Information would not have been improperly obtained. Defendants' negligence was a direct and legal cause of the theft of the Personally Identifiable Information of Plaintiffs and the Class and all resulting damages.

90. The injury and harm suffered by Plaintiffs and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' Personally Identifiable Information.

91. These damages include, but are not limited to, invasion of privacy, theft of Personally Identifiable Information, increased risk of data breaches, increased risk of identity theft, emotional distress, lost time, effort and money in responding to Marriott International, Inc.'s negligence and misuse of their personal data beyond what Marriott International, Inc. promised.

COUNT TWO

Negligent Misrepresentation as Against Marriott International, Inc. And Starwood Hotels & Resorts Worldwide, LLC

92. Plaintiffs incorporate all of the above allegations by reference as if fully set forth herein.

93. As alleged herein, Defendant Marriott International, Inc. repeatedly assured Plaintiffs and Class Members that their data would be private and protected.

94. Marriott International, Inc. further assured that customers' data would not be shared with third-party applications without customers' express permission.

95. At the time Defendant Marriott International, Inc. made these representations, Defendant knew or should have known that these representations were false or made them without knowledge of their truth or veracity.

96. At minimum, Defendant Marriott International, Inc. negligently misrepresented and/or negligently omitted material facts concerning its commitment to privacy and the safety of customer data.

97. The negligent misrepresentations and omissions made by Defendant, upon which Plaintiffs and all Class members reasonably and justifiably relied, were intended to induce, and actually induced, Plaintiffs and all Class members to create Marriott International, Inc. profiles, share personally identifiable information with Marriott International, Inc., and depend upon Marriott International, Inc. to use that data only in the ways defined in the data use policy.

98. Plaintiffs and Class members would not have used Marriott International, Inc.'s product, or would not have provided personally identifiable information to Marriott International, Inc., if the true manner in which their data was being used was known to them, contrary to Marriott International, Inc.'s repeated assurances.

99. The negligent actions of Defendant caused damage to Plaintiffs and all Class members, who are entitled to damages and other legal and equitable relief as a result.

COUNT THREE

Invasion of Privacy—Intrusion Upon Seclusion

100. Plaintiffs incorporate all of the above allegations by reference as if fully set forth herein.

101. Plaintiffs and Class Members have reasonable expectations of privacy with respect to their personal information being maintained by Marriott International, Inc. & Starwood Hotels& Resorts Worldwide, LLC.

102. The reasonableness of such expectations of privacy is supported by Defendants' unique position to monitor Plaintiffs' and Class Members' behavior through its access to Plaintiffs' and Class members' customer data. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Defendants' collective tracking and exfiltrating of Plaintiffs' and Class Members' personal data.

103. Defendants intentionally intruded on and into Plaintiffs' and Class Members' solitude, seclusion, or private affairs. Marriott International, Inc. intentionally designed its platform—and established commensurate policies and procedures governing such platform—to enable the exfiltration, without authorization, of Class Members' personal data. Defendants intentionally availed themselves of Marriott International, Inc.'s privacy-invasive measures in order to acquire Class Members' personal data without consent.

104. Defendants intentionally intruded on and into Plaintiffs' and Class Members' solitude, seclusion, or private affairs by intentionally facilitating the exfiltration of Class Members' personal data to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiffs' and Class members' personal data and activities through the monitoring technologies and policies described herein.

105. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the immense outcry following the revelation of these acts and practices—not only from the public, but also from regulators and legislators. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Class members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor Plaintiffs' and Class Members—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

106. Plaintiffs and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

107. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Class Members.

108. As a result of Defendants' actions, Plaintiffs and Class Members seek injunctive relief, in the form of (1) certification by Marriott International, Inc. that no third parties presently are able to access Plaintiffs' and Class Members' customer data without first obtaining express consent; (2) audits, by Marriott International, Inc., of all third parties who obtained customers' data; (3) notification, by Marriott International, Inc. to Plaintiffs and Class members, of each instance in which a third party obtained customer data—including the type of customer data; and, (4) destruction of all improperly obtained customer data of Plaintiffs and Class Members.

109. As a result of Defendants' actions, Plaintiffs and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT FOUR

Declaratory Relief Pursuant to 28 U.S.C. § 2201

110. Plaintiffs incorporate all of the above allegations by reference as if fully set forth herein.

111. An actual controversy, over which this Court has jurisdiction, has arisen and now exists between the parties relating to the legal rights and duties of Plaintiffs and Defendants for which Plaintiffs desire a declaration of rights.

112. Plaintiffs contend and Defendants dispute that Defendants, in whole or in part, were authorized by Plaintiffs and Class Members to acquire customer data without the express consent, from each developer, of all customers whose personal data was thereby acquired.

113. Plaintiffs, on behalf of themselves and the Class, are entitled to a declaration that Defendants were *not* so authorized through their contracts with Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC, and accordingly that Defendants' behavior violated the Stored Communications Act, CIPA, the UCL, and Plaintiffs' common law claims.

COUNT FIVE

Conversion

114. Plaintiffs incorporate all of the above allegations by reference as if fully set forth herein.

115. Plaintiffs and Class Members were the owners and possessors of their private information. As the result of Defendants' wrongful conduct, Defendants have interfered with the Plaintiffs' and Class Members' rights to possess and control such property, to which they had a superior right of possession and control at the time of conversion.

116. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class Members suffered injury, damage, loss or harm and therefore seek compensatory damages.

117. In converting Plaintiffs' Private Information, Defendants have acted with malice, oppression and in conscious disregard of the Plaintiffs' and Class Members' rights. Plaintiffs, therefore, seek an award of punitive damages on behalf of the class.

COUNT SIX

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

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

119. 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.

120. 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."

121. Defendant Marriott International, Inc. 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).

122. Defendant Starwood Hotels & Resorts Worldwide, LLC 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).

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

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

125. Defendants 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.

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

127. 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."

128. 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."

129. Because Defendants discovered a security breach and had notice of a security breach, Defendants 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).

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

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

132. Pursuant to Md. Comm. Code § 14-3508, Defendants' 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.

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

COUNT SEVEN

MARYLAND CONSUMER PROTECTION ACT
Md. Comm. Code §§ 13-301, *et seq.*
AND APPLICABLE STATE CONSUMER PORTECTION ACTS AND UNFAIR BUSINESS PRACTICES

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

135. 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.

136. 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.

137. Defendant Marriott International, Inc. is a "person" as defined by Md. Comm. Code § 13-101(h).

138. Defendant Starwood Hotels & Resorts Worldwide, LLC is a "person" as defined by Md. Comm. Code § 13-101(h).

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

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

141. Defendants advertise, offer, or sell "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

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

143. Defendants 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.

144. Defendants 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.

145. 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. Defendants' misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

146. Defendants intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

147. Had Defendants disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendants 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.

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

149. As a direct and proximate result of Defendants' 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.

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

COUNT EIGHT

VIOLATION OF THE GENERAL DATA PROTECTION REGULATION REGULATION (EU) 2016/679 THAT APPLIES TO MARRIOTT BECAUSE MARRIOTT HAS AN ESTABLISHMENT IN THE EUROPEAN UNION

151. At all relevant times, Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC operated hotels throughout Europe.

152. Marriott is subject to the *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (published OJ L 119, 04.05.2016; or OJ L 127, 23.5.2018) ("GDPR") applicable as of May 25, 2018 in all member states and to organizations based outside of the European Union when certain circumstances apply as more fully described in the following paragraphs.

153. GDPR Article 3.1: "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not". "Establishment" is not defined by the GDPR. GDPR clarifies the concept as follows:

> Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

154. EDPB (European Data Protection Board)'s Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, adopted on 16 November 2018 ("Guidelines") defines the scope of the concept of an "establishment." Guidelines at 5.[30] "[I]n some circumstances, the presence of a single employee or agent of the non-EU entity may be

[30] See, in particular, Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12), Weltimmo v NAIH (C- 230/14), Verein für Konsumenteninformation v Amazon EU (C-191/15) and Wirtschaftsakademie Schleswig- Holstein (C-210/16).

sufficient to constitute a stable arrangement if that employee or agent acts with a sufficient degree of stability." Id. Upon information and belief, Marriott has stable arrangements in many if not all the member states and therefore has (at least) one "establishment" in the Union for the purpose of Article 3.1

155. Marriott is a "controller" in the language of the GDPR, i.e. GDPR Article 4.7 "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." By contrast, a "processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" GDPR Article 4.8.

156. As the EDPB correctly points out: "Once it is concluded that a controller or processor is established in the EU, an *in concreto* analysis should then follow to determine whether the processing is carried out in the context of the activities of this establishment, in order to determine whether Article 3(1) applies." Id. at 6. Upon information and belief, Marriott's processing is carried out "in the context of the activities of this establishment". Article 3.1.

157. By "processing", the GDPR means:

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by restriction, erasure or destruction. GDPR Article 4.2.

158. By its own admission, Marriott performs "processing" by collecting (see "Collection of Personal data" in MARRIOTT GROUP GLOBAL PRIVACY STATEMENT, available at https://www.marriott.com/about/privacy.mi, "MGGPS"), using (see "Use of Personal Data and Other Data" in MGGPS); disclosing (see "Disclosure of Personal Data and

Other Data" in MGGPS); using and disclosing as they "believe to be necessary or appropriate" (see "Other Uses and Disclosures" in MGGPS); aggregating (See "Aggregate Data" in MGGPS); and simply by storing (see "Retention" in MGGPS) personal data. On information and belief Marriott performs other activities with data that constitute "processing" within the meaning of the GDPR.

159. Marriott's processing concerns "personal data" under the GDPR. By "personal data", the GDPR means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". GDPR Article 4.1. The concept of "personal data" under GDPR is broader than PII, among other things because it applies to information of an individual that is "identified or identifiable" and because it is well established that the information that is protected includes even dynamic IP addresses.[31]

160. By its own admission, Marriott processes, at the very least, the following personal data:

- 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

[31] See ECJ's decision in *Patrick Breyer v. Bundesrepublik Deutschland* (case C582/14)

- 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. [Source: MGGPS]

161. The above information is "personal data" as defined by GDPR Article 4.1.

162. The processing by Marriott of all the above information – and possibly others – is relevant under the GDPR and must be done in accordance to the GDPR's requirements. The GDPR started its application in May of 2018. However, because storage itself is processing, it is irrelevant whether Marriott collected personal data before or after May of 2018. Compliance with the GDPR is required for *all* personal data present in its database, whether collected after May 2018 or before.

163. Having established that Marriott processes personal data and has an establishment in the European Union, Plaintiffs' allege Marriott's global processing is performed "in the context of the activities of this establishment". Upon information and belief, this is exactly the case.

164. The EDPB clarified that "with a view to fulfilling the objective of ensuring effective and complete protection, the meaning of 'in the context of the activities of an establishment' cannot be interpreted restrictively". Guidelines at 6. The EDPB puts the

threshold of relevance of the connection quite low expressly excluding from the application of Article 3.1 only cases of "remotest link" between and commercial activities that "so far removed from the processing of personal data by this entity that the existence of the commercial activity in the EU would not be sufficient to bring that data processing within the scope of EU data protection law". Id. When the connection between the processing performed by the EU establishment and the processing performed by the non-resident organization is more than this *de minimis* level (as identified by the EDPB), all the processing of the organization is at issue here under the GDPR:

> The activities of a local establishment in a Member state and the data processing activities of a data controller or processor established outside the EU may be inextricably linked, and thereby may trigger the applicability of EU law, even if that local establishment is not actually taking any role in the data processing itself14. If a case by case analysis on the facts shows that there is an inextricable link between the activities of an EU establishment and the processing of data carried out by a non-EU controller, EU law will apply to that processing by the non-EU entity, whether or not the EU establishment plays a role in that processing of data.[32]

And also:

> Revenue-raising in the EU by a local establishment, to the extent that such activities can be considered as "inextricably linked" to the processing of personal data taking place outside the EU and individuals in the EU, may be indicative of processing by a non-EU controller or processor being carried out "in the context of the activities of the EU establishment", and may be sufficient to result in the application of EU law to such processing. Guidelines at 7 internal quotation omitted.

165. There is no doubt that Marriott raises revenues in the EU and that such activities are "inextricably linked to the processing of personal data taking place outside the EU". In fact, Marriott has more than 6500 properties located throughout the world, a substantial number of

---

[32] Guidelines at 6-7 (internal quotation omitted) (Reference made to WP 179 update - Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, 16th December 2015 and to Google Spain, Case C 131/12, cited above).

which are in the EU. Guests book Marriott hotels through its world-wide website. Marriott receives revenues from these bookings, a substantial number of which are in the EU; Marriott's world-wide revenues are more than $22 billion. Marriott maintains common databases of European and non-European data subjects and processes of personal data of European and non-European data subjects together. The activities of its European hotels are "inextricably linked" to the processing performed in the US because the booking (and possibly other activities) is through the Marriott's website.

166. Marriott's conduct confirmed the above allegations by its MGGPS and its conduct following the breach.

167. While the MGGPS does not expressly mention the GDPR, the MGGPS is modelled on the GDPR privacy statements given by GDPR's bound organizations (even if defective as we will explain below). The MGGPS is identical in the US website and in the UK website (https://www.marriott.co.uk/about/privacy.mi). While we have not compared the privacy statements of the other European websites of Marriott, it appears that those websites contain a verbatim translation of MGGPS (*see, e.g.*, the "Charte de Confidentialite'" on the French website at https://www.marriott.fr/a-propos/declaration-de-confidentialite-france.mi and then and the "Informativa informativa globale sulla privacy del gruppo Marriott" available at https://www.marriott.it/chi-siamo/informativa-sulla-privacy.mi)

168. Marriott conceded being subject to the GDPR by notifying the ICO (Information Commissioner, the UK Data Protection Authority) of the breach. On November 30, 2018, the ICO informed the public:

> We have received a data breach report from Marriott Hotels involving its Starwood Hotels and are making enquiries.

> We advise people who may have been affected to be vigilant and to follow advice from the ICO and National Cyber Security Centre websites about how they can protect themselves and their data online." ICO statement in response to Marriott Hotels breach announcement available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-statement-in-response-to-marriott-hotels-breach-announcement/

169. Plaintiffs are not aware of other notifications made by Marriott to other data protection authorities. Marriott admits the ICO is the authority of its "main establishment" in the Union in the definition of Article 4.16 (Definition of "main establishment") and therefore the ICO as its "lead supervisory authority" under Article 56. Marriott operates and maintains one or more establishments in the European Union being the UK one, its main establishment.

170. Marriott is subject to the GDPR in relation to the processing of ALL its personal data and that all of Marriott's customers (and other data subjects whose data Marriott processes) – wherever located – including class representatives Mr. Walters and Dr. Tew, are entitled to the protection of the EU Regulation.

171. The conduct of Defendants acted in violation of the GDPR at least in the following particulars: (i) violation of GDPR Article 32 (Security of processing); (ii) violation of GDPR Article 33 (Notification of a personal data breach to the supervisory authority); (iii) violation of GDPR Article 34 (Communication of a personal data breach to the data subject); (iv) violation of GDPR Article 5 (Principles relating to processing of personal data); (v) violation of GDPR Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject); (vi) violation of Article GDPR 13 (Information to be provided where personal data are collected from the data subject) and 14 (Information to be provided where personal data have not been obtained from the data subject); (vii) violation of GDPR Article 37 (Designation of the data protection officer) and others as they will be determined in discovery.

172. *Violation of GDPR Article 32's Security of processing.* The GDPR imposes security requirements for single processing and the devices being used and overall organizational structure. GDPR Article 32 (Security of processing) imposes duties including but not limited to:

> 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> (a) the pseudonymisation and encryption of personal data;
>
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
>
> 2. In assessing the proper level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Defendants employed insufficient data security practices and those data security practices were not compliant with the requirements of Article 32 of the GDPR.

173. *Violation of GDPR Article 33 ("Notification of a personal data breach to the supervisory authority").* Under GDPR Article 33, Defendant should have "without undue delay and, where feasible, not later than 72 hours after having become aware of it "notified the data processing authorities of the data breach. A "personal data breach" under the GDPR means " a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed", a concept that is recognized to be broader than what it is usually intended in the

U.S. By its own admission, Defendant initially discovered an unlawful attempt of access to its reservation the Breach on September 8, 2018.[33] "On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database."[34]

174. Upon information and belief, the notification required by Article 33 only happened on November 30, 2018, i.e., 83 days after Marriott had learned of the attempt of access and 11 days after Marriott had made a final determination of the breach. This is not compliant with GDPR Article 33. Had the notification been done within the proper framework, the data protection authority would have notified the public of the breach before November 30, 2018. The customers whose data was at risk in the database could have taken protective measures much sooner than they did had Marriott complied with the law. The late communication deprived the ICO of the possibility to interact immediately with Marriott advising measures to take to mitigate privacy data breach harm and damages.

175. *Violation of GDPR Article 34 ("Communication of a personal data breach to the data subject").* GDPR Article 34 requires a communication of the breach to the data subjects "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons".[35] Such communication must be done "without undue delay". Here Marriott's data breach "is likely to result in a high risk" for Marriott's customers and possibly others natural persons because of, among other reasons, the breadth of data that Marriott collects.

---

[33] *See* "Marriott Announces Starwood Guest Reservation Database Security Incident," Marriott News Center (Nov. 30, 2018), available at http://news.marriott.com/2018/11/marriott-announces- starwoodguest-reservation-database-security-incident/ (last accessed Dec. 11, 2018).

[34] *Id.*

[35] GDPR Article 34.1.

Marriott did perform the communication to the data subjects. However, that communication only happened on November 30, 2018, i.e, again 83 days after Marriott had learned of the attempt of access and 11 days after Marriott had made a final determination of the breach. In addition, upon information and belief the communication did not contain the elements required Article 34 [36] Had the communication been done within the proper framework, the customers could have taken protective measures much sooner.

176. *Violation of GDPR Article 5 (Principles relating to processing of personal data).* Upon information belief, Marriott did not process data consistently with the principles established in Article 5. Among other violations, Marriott violated the principle of "data minimization" which imposes the controllers to perform only a processing of that data that are "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Article 5.1(c). As an example of this violation, Marriott admittedly processes "Biometric data, such as digital images", a type of data that is extremely sensitive and whose processing is discouraged: the processing of biometrics together with other special categories of information indicated in Article 9 is in principle "prohibited"[37] absent the conditions of Article 9.2. Plaintiffs fail to see how the processing of biometrics can ever be "adequate, relevant and

---

[36] The communication to the data subjects must "describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).GDPR Article 34. The elements in question are: The "name and contact details of the data protection officer or other contact point where more information can be obtained", Article 33.2(b); a description of "the likely consequences of the personal data breach" Article 33.2(c); "measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects." Article 33.2(d)

[37] GDPR Article 9 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

limited to the purpose" when the business of Marriott is proving a hotel stay to customer. Had the minimization principle been properly implemented in Marriott's processing, the magnitude of the data breach would have been reduced.

177. *Violation of GDPR Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject).* The information provided by Marriott to its customers is not transparent because, among other issues, i) the MGGPS fails to make any reference to the GDPR so that the data subjects are not put in a position to know what their rights and ii) the purposes of processing are not well defined for certain processing.[38]

178. *Violation of Article GDPR 13 ("Information to be provided where personal data are collected from the data subject") and possibly 14 (Information to be provided where personal data have not been obtained from the data subject).* The MGGPS (i) fails to identify in Marriott or anyone else the controller of the data as required by Article 13.1(a); (ii) the identity of the data protection officer (DPO) is not indicated as required by Article 13.1(b). If Marriott has not appointed a DPO, this is a further violation of the GDPR that caused damaged to the data subjects as we specify below (iii) the MGGPS seems to confuse the grounds for processing pursuant to GDPR Article 6 with the purposes of processing that must be disclosed pursuant to Article 13.1(c) in some parts of the MGGPS[39]; (iv) the MGGPS confuses in certain parts the ground of processing contract performance (Article 6(1)(b) with the ground of legitimate interest (Article 6.1(f)). The is a problem because data subjects have different rights under the two grounds; (iv) Marriott never specifies – not even by general categories – which are the "legitimate interests" that is cited in several parts of the MGGPS as a ground for processing; (v)

[38] From the MGGPS "We may use and disclose Other Data for any purpose, except where we are not allowed to under applicable law".
[39] From the MGGPS: "We use Personal Data and Other Data in this way to manage our contractual relationship with you, comply with a legal obligation and/or because we have a legitimate interest to do so."

while the MGGPS informs data subjects that they can request to access, change, delete or restrict the use of their personal data,[40] the MGGPS fails to qualify these options as "rights".[41] In addition, the reference is only to Marriott's "use" of data, while the GDPR grants the data subject the right to obtain all of this and more in relation to any processing (not only use). Further, the catalogue of rights that a controller should inform the data subjects about is incomplete in the MGGPS, most notably the right to withdraw consent when processing is based on consent (Article 13.2(c)) and to lodge a complaint with a supervisory authority (Article 13.2(d).) Had the data subjects (including Mr. Walters and Mr. Tew) been properly informed of their rights – as they should have –many of those data subjects would more likely than not exercised those rights and the data breach would not have struck those data subjects or would have struck only a reduced amount of data for them.

179. *Noncompliance with GDPR Article 37 (Designation of the data protection officer).* GDPR Article 37 requires controllers and processors to designate a DPO when:

---

[40] From the MGGPS:

How You Can Request to Access, Change, Delete, or Restrict the Use of Your Personal Data

If you would like to request to access, change, delete, or restrict the use of your Personal Data that you have previously provided to us, or if you would like to receive an electronic copy of your Personal Data for purposes of transmitting it to another company (to the extent these rights are provided to you by law), please complete this form

If you have any questions about the form or our process, feel free to contact us at privacy@marriott.com, or by mail at:
Marriott International, Inc.
Global Compliance, Privacy
10400 Fernwood Road
Bethesda, MD 20817
United States of America

[41] Article 13.2 (b) requires the controller to inform the data subjects of "the existence of the **right** to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;"

> (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
>
> (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article10."

180. Marriott is not a "public authority or body", however, upon information and belief, it performs and needs to perform "a systematic monitoring of data subjects on a large scale" (safety of the guests requires cameras monitoring the premises as the MGGPS also informs)[42]. As the Article 29 Data Protection Working Party (W29) (predecessor in interest of the EDPB) clarifies in its Revised Guidelines on DPOs issued by WP29 in April 2017 (DPO Guidelines), "core activities of the controller or processor" in Article 37.1(b) and (c) needs to be interpreted as covering the "primary activities" and those "activities where the processing of data forms an inextricable part of the controller's or processor's activity". Id. at 6.[43] In addition, upon information and belief Marriott also performs processing of sensitive data on a large scale[44] so that Marriott is subject to the obligation to appoint a DPO also under Article 37.1(c).

---

[42] From the MGGPS /Collection of Personal Data:
> 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.

[43] The WP29 gives the example of a hospital:
> For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. DPO Guidelines at 6.

[44] The GDPR does not give a definition of "large scale", though recital 91 provides some guidance. The WP29 clarifies on this regard that "it is not possible to give a precise number either with regard to the amount of data processed or the number of individuals concerned, which would be applicable in all situations" (DPO Guidelines at 7) and recommends consideration of the following factors:

Indeed, the MGGPS specifies that Marriott processes "Biometric data" which is an Article 9's special category of data. Upon information and belief, other "sensitive data" is also being processed by Marriott. [45]

181. Upon information and belief, Marriott failed to appoint a DPO. Had a DPO been appointed, he or she would have more probably than not (i) advised Marriott in relation to its obligations under the GDPR (as provided by GDPR Article 39.1(a)); ii) effectively monitored Marriott's compliance with the GDPR as provided by GDPR Article 39.1(b); (iii) provided advice as requested on the data protection impact assessment (see below) as provided by GDPR Article 39.1(c); and (iv) cooperated with the supervisory authority pursuant to GDPR Article 39.1(d).

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity. *Id.*

Based on those factors, there could be no doubt that Marriott's processing (e.g., the processing related to the monitoring) is on a large scale.

[45] The Biometric data is not the only sensitive data processed by. Marriott. As Marriott implicitly concedes in the MGGPS there are cases in which Marriott requests customers to deliver "sensitive data":

> **Unless specifically requested**, we ask that you not send us, and you not disclose, on or through the Services or otherwise to us, any Sensitive Personal Data (*e.g.*, social security numbers, national identification number, data related to racial or ethnic origin, political opinions, religion, ideological or other beliefs, health, biometrics or genetic characteristics, criminal background, trade union membership, or administrative or criminal proceedings and sanctions). MGGPS in section "Sensitive Data".

In fact, upon information and belief, Marriott processes "sensitive data", for example, when it accommodates religious dietary restriction. (*See, e.g.*, "Kosher events by Marriott" at the Warsaw Marriott Hotel in Warsaw, Poland; https://www.marriott.com/hotelwebsites/us/w/wawpl/wawpl_pdf/Kosher_Buffet_Offer_ENG_2014.pdf) or when Marriott allows customers with allergies to book special allergy-friendly rooms http://deals.marriott.com/courtyard/usa/ga/alpharetta/atlph-pure-allergy-friendly-guestroom

182. *Other particulars*. Marriott failed to perform a Data Protection Impact Assessment (GDPR Article 35 of the GDP) – also known as PIA - which is mandated, among other cases, in case of "processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10". Marriott processes "sensitive data" on a large scale. Marriott should have therefore, "prior to the processing, carr[ied] out an assessment of the impact of the envisaged processing operations on the protection of personal data." If the PIA – which must be performed as provided in GDPR Article 35.7—"indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk" the controller must consult the supervisory authority prior to processing. Upon information and belief, had Marriott performed a PIA on its processing, the data protection authority would have been informed of the risk and could have suggested protective measures that would have decreased the risk.

183. Defendants failed in the compliance with all the above GDPR requirements and possibly others) and violated the rights of the Class or Classes, resulting in material harm to the Classes, placing them at a higher risk of identity theft, and causing financial and non-financial damage to the Plaintiffs.

184. GDPR Article 82 entitles "**Any person** who has suffered **material or non-material damage** as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." Whereas [146] clarifies:

> The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State

> law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered.

185. Plaintiffs suffered and will suffer in the future: damage to personal dignity, autonomy and integrity and Defendants' violations and the data breach in particular caused anxiety and distress. Plaintiffs allege these and all other types of damages recoverable under the Regulation.[46]

186. Marriott is a controller in the meaning of Article 4(7) of the Regulation. Any controller involved in processing "**shall be liable for the damage caused by the processing which infringes on this Regulation**" and Article 82.3 provides that "A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage." It is evident that, once the violation of the GDPR is ascertained, it is up to Defendants to demonstrate that they are "in… [no] way responsible for the event giving rise to the damage."

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully request that this Court enter a judgment against Defendants as follows:

(a) Certifying the Nationwide Class and appointing Plaintiffs as Class Representatives;

(b) Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

(c) Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

---

[46] The UK Court of Appeal in *Vidall-Hall v Google*, recognized exactly those damages as compensable under Directive 46/1995, the predecessor in interest of the GDPR. *Vidall-Hall v Google para 19.* It is worth noting that the recognition of those damages happened based on the case law of the ECJ. In fact, the Directive, unlike the GDPR did not expressly mention "material or non-material damages."

(d) Awarding Plaintiffs and the Class members nominal, actual, compensatory, and consequential damages;

(e) Awarding Plaintiffs and the Class members statutory damages and penalties, as allowed by law;

(f) Awarding Plaintiffs and the Class members restitution and disgorgement;

(g) Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest;

(h) Awarding Plaintiffs and the Class members reasonable attorneys' fees costs and expenses, and;

(i) Granting such other relief as the Court deems just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of all others similarly situated, demand a trial by jury on all issues so triable.

DATED: December 11, 2018

Respectfully Submitted,

/s/ Jodi Westbrook Flowers
Jodi Westbrook Flowers (SC Bar #66300)
Fred Baker, *pro hac vice forthcoming*
Ann Ritter, *pro hac vice forthcoming*
Andrew Arnold, *pro hac vice forthcoming*
Annie Kouba, *pro hac vice forthcoming*
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
Email: jflowers@motleyrice.com
Email: fbaker@motleyrice.com
Email: aritter@motleyrice.com
Email: aarnold@motleyrice.com
Email: akouba@motleyrice.com

/s/ William F. Askinazi
William F. Askinazi (MD Bar #12522)
Askinazi Law & Business LLC
12504 Palatine Court

Potomac, MD 20854
Telephone: 301-540-5380
Facsimile: 240-715-9113
Email: askinazilaw@gmail.com

/s/ Charles R. "Rusty" Webb
Charles R. "Rusty" Webb (WVSB #4782)
The Webb Law Centre, PLLC
716 Lee Street East
Charleston, WV 25301
Telephone: (304) 344-9322
Facsimile: (304) 344-1157
Email: rusty@rustywebb.com

/s/ Cari Campen Laufenberg
Lynn Lincoln Sarko
Gretchen Freeman Cappio
Cari Campen Laufenberg
KELLER ROHRBACK LLP
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Telephone: (206) 623-1900
Facsimile: (206) 623-3384
Email: lsarko@kellerrohrback.com
Email: gcappio@kellerrohrback.com
Email: claufenberg@kellerrohrback.com

/s/ Chris Springer
Chris Springer
KELLER ROHRBACK LLP
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Telephone: (805) 456-1496
Facsimile: (805) 456-1497
Email: cspringer@kellerrohrback.com

Attorneys for Plaintiffs and the proposed class