UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

PATI SPRINGMEYER, an individual and Nevada Resident, and JOE LOPEZ, an individual and California Resident, on behalf of themselves and all others similarly situated, Plaintiff, v. MARRIOTT INTERNATIONAL, INC., a Montgomery County, Maryland Resident, Defendant.	CASE NO. 8:20-CV-00867-PWG **AMENDED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

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

SUMMARY OF THE CASE

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

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

3. On March 31, 2020, Marriott announced that the login credentials of two of its employees had been compromised and "an unexpected amount of guest information" had been improperly accessed as early as mid-January 2020 (hereinafter, the "Data Breach"). The compromised guest data included: Contact Details (e.g., name, mailing address, email address, and phone number); Loyalty Account Information (e.g., account number and points balance, but not passwords); Additional Personal Details (e.g., company, gender, and birthday day and month); Partnerships and Affiliations (e.g., linked airline loyalty programs and numbers); and Preferences (e.g., stay/room preferences and language preference) (hereinafter, the "PII").

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

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

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

7. As a result of Marriott's failure to implement and follow basic security procedures, guest PII is now in the hands of thieves. Plaintiffs and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from

the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

8. Plaintiffs, on behalf of all others similarly situated for the Nationwide Class (defined below), allege claims for negligence, negligence *per se*, breach of contract, breach of implied contract, unjust enrichment, declaratory judgment, breach of confidence, and California- and Nevada-state-based claims for the respective subclasses, and seek to compel Marriott to adopt reasonably sufficient security practices to safeguard guest PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

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

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

PARTIES

11. Plaintiff Pati Springmeyer is a resident and citizen of Las Vegas, Nevada. Ms. Springmeyer has stayed at a number of Marriott properties and hotels over the past 10 years, entrusting Marriott with her PII. On March 31, 2020, Ms. Springmeyer received an email from Marriott International stating that her PII had been compromised and "accessed without authorization" (the "Breach Notice").

12. Since the announcement of the Data Breach, and prompted by the receipt of the Breach Notice, Ms. Springmeyer purchased credit monitoring services at an annual cost of $159.96, which she continues to pay from her own personal funds each month, and will be compelled to continue to spend due to the increased risk of identity theft and fraud caused by the Data Breach.

13. Since the announcement of the Data Breach, Ms. Springmeyer continues to spend her valuable time to monitor her various accounts in an effort to detect and prevent any misuses of her PII.

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

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

to Marriott as a condition for hotel services; (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

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

17. Plaintiff Joe Lopez is a resident and citizen of Los Angeles County, California. Mr. Lopez has stayed at a number of Marriott properties and hotels, entrusting Marriott with his PII. Mr. Lopez also received the Breach Notice.

18. Since the announcement of the Data Breach, Mr. Lopez continues to spend his valuable time to monitor his various accounts in an effort to detect and prevent any misuses of his PII.

19. Mr. Lopez has, and continues to spend his valuable time to protect the integrity of his PII—time which he would not have had to expend but for the Data Breach.

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

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

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

FACTUAL BACKGROUND

A. The Marriott 2020 Data Breach

23. In February 2020, Marriott learned that the login credentials of two employees at a franchise property had been compromised and a large amount of guest PII had been improperly accessed. Over a month later, Marriott notified approximately 5.2 million guests that their PII, such as names, addresses, phone numbers, birthdays, loyalty information, had been compromised. Although Marriott said it doesn't believe that credit card information, passport numbers or driver's license information were accessed, Marriott stated the investigation was ongoing and it did not rule out the possibility.[1]

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

> Marriott International: Incident Notification
>
> This site has information concerning the incident, answers to questions, and steps guests can take.
>
> March 31, 2020
>
> **What Happened?**
>
> Hotels operated and franchised under Marriott's brands use an application to help provide services to guests at hotels. At the end of February 2020, we identified that an unexpected amount of guest information may have been accessed using the login credentials of two employees at a franchise property. We believe this activity started in mid-January 2020. Upon discovery, we confirmed that the login credentials were disabled, immediately began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests.
>
> Although our investigation is ongoing, we currently have no reason to believe that the information involved included Marriott Bonvoy

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

> account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers.
>
> At this point, we believe that the following information may have been involved, although not all of this information was present for every guest involved:
>
> • Contact Details (e.g., name, mailing address, email address, and phone number)
>
> • Loyalty Account Information (e.g., account number and points balance, but not passwords)
>
> • Additional Personal Details (e.g., company, gender, and birthday day and month)
>
> • Partnerships and Affiliations (e.g., linked airline loyalty programs and numbers)
>
> • Preferences (e.g., stay/room preferences and language preference)
>
> **Guest Notification**
>
> On March 31, 2020, Marriott sent emails about the incident to guests involved. The email was sent from marriott@email-marriott.com because this is the standard email account used to communicate with our guests.[2]

B. Marriott Acquires, Collects, and Stores Plaintiffs' and Class Members' PII

25. Marriott is an American multinational, diversified hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities, including 30 brands with more than 7,000 properties across 130 countries and territories globally. Founded in 1927, the company is headquartered in Bethesda, Maryland, and maintains hotel brands including Marriott, Courtyard, and Ritz-Carlton. Marriott reported revenues of $20.75 billion in the 2018 fiscal year.

[2] https://mysupport.marriott.com/

26. As a condition of staying at one of its properties, Marriott requires that guests entrust it with their PII.

27. Marriott collects, stores, and maintains the PII of all guests who stay at Marriott properties. Marriott retains and stores this personal information beyond the time reasonably necessary to delivery hotel accommodations, food and beverage services, and similar services to guests.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Marriott assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

29. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and the Class Members relied on Marriott to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

30. In its Global Privacy Statement (the "Privacy Statement"), with an effective date of June 3, 2019, which was, upon information and belief, the Global Privacy Statement in effect at the time of the Data Breach[3] Marriott represents that: "The Marriott Group, which includes Marriott International, Inc., Starwood Hotels & Resorts Worldwide, LLC … and their affiliates, values you as our guest and recognizes that privacy is important to you." It explains that the Marriott Group collects data:

> • 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")

[3] http://web.archive.org/web/20200328180639/https://www.marriott.com/about/privacy.mi

> • 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.[4]

31. The Privacy Statement defines "Collection of Personal Data" as follows: "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.

[4] http://web.archive.org/web/20200328180639/https://www.marriott.com/about/privacy.mi

32. Marriott represents that:

> We use Personal Data and Other Data to provide you with Services, to develop new offerings and to protect the Marriott Group and our guests as detailed below. In some instances, we will request that you provide Personal Data or Other Data to us directly. If you do not provide the data that we request, or prohibit us from collecting such data, we may not be able to provide the requested Services.[5]

33. Marriott then lists the numerous "legitimate business interests," which include services related to, *inter alia*: reservations, accepting payments, assisting with meetings and events, ensuring room availability, providing electronic receipts, personalizing services, sending marketing and promotional communications, and administering its loyalty programs.[6]

34. Additionally, Marriott makes numerous representations that it uses consumers' PII to "manage our contractual relationship with you and/or because we have a legitimate interest to do so. […] 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."[7]

35. Further, Marriott represents that: "We seek to use reasonable organizational, technical and administrative measures to protect Personal Data."[8] Upon information and belief, these statements were in the Privacy Statement as of March 28, 2020—days prior to Marriott's announcement of the Data Breach.

36. Yet, despite all of these "legitimate interests," "contractual obligations," and associated promises to protect consumers' PII, Marriott failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' PII. Marriott had the resources to prevent a breach and

[5] http://web.archive.org/web/20200328180639/https://www.marriott.com/about/privacy.mi
[6] http://web.archive.org/web/20200328180639/https://www.marriott.com/about/privacy.mi
[7] http://web.archive.org/web/20200328180639/https://www.marriott.com/about/privacy.mi
[8] http://web.archive.org/web/20200328180639/https://www.marriott.com/about/privacy.mi

has made significant expenditures to market their hotels and hospitality services, but neglected to adequately invest in data and cyber security, despite being engaged in litigation regarding one of the largest data breaches in history.

C. Marriott's Promises to California Residents

37. In addition to the policies applicable to U.S.-based consumers, Marriott also represents to California residents that it collects name, nationality, passport, visa, and other government-issued identification data and online identifiers.[9] Marriott also collects "Personal information," as defined in California's safeguard law, such as name, contract information, and financial information. Further, Marriott represents it collects information related to gender, age, medical conditions, primary language, national origin, citizenship, and marital status.

38. In short, the information Marriott collects is expansive, valuable, and exhaustive.

39. Additionally, Marriott represents that any information "disclosed" to third parties is done so "for [Marriott's] operational business purposes."[10]

40. Finally, Marriott represents that it sells categories of Personal Information.[11]

41. The Data Breach, however, involves neither the "disclosure" or "sale" described in Marriott's promises and representations to California residents; instead, Marriott failed to detect malicious actors stealing Plaintiffs' and Class Members' PII.

D. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure

42. The types of information compromised in the Data Breach are highly valuable to identity thieves. Names, email addresses, mailing address, telephone numbers, birthdate, gender,

[9] https://www.marriott.com/about/ccpa.mi
[10] https://www.marriott.com/about/ccpa.mi
[11] https://www.marriott.com/about/ccpa.mi

and other valuable PII can all be used to gain access to a variety of existing accounts and websites and can be used in other ways to effectuate identity theft.

43. Identity thieves can also use the PII to harm Plaintiffs and Class Members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, ... individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[12]

44. To put it into context, the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime was around $113 billion at that time, with the average cost per victim being $298 dollars.

45. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the PII they have obtained. Indeed, in

[12] The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf

order to protect themselves, Class Members will need to remain vigilant against unauthorized data use for years and decades to come.

46. Once stolen, PII can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII.[13] Websites appear and disappear quickly, making it a very dynamic environment.

47. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

E. Marriott Failed to Comply With FTC Requirements

48. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.[14]

[13] Brian Hamrick, The *dark web: A trip into the underbelly of the internet*, WLWT News (Feb. 9, 2017 8:51 PM), http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419.

[14] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.[15] The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

50. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[16]

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission

[15]Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

[16] FTC, *Start With Security*, *supra* note 5.

Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

52. Marriott was at all times fully aware of its obligation to protect the personal and financial data of its guests and consumers. Marriott was also aware of the significant repercussions if it failed to do so.

53. Marriott's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

F. The Marriott Data Breach Caused Harm and Will Result in Additional Fraud

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

55. Consumer victims of data breaches are much more likely to become victim of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[17]

56. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[19]

57. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can

[17] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.
[18] 17 C.F.R § 248.201 (2013).
[19] *Id.*

drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[20]

58. Identity thieves can use personal information, such as that of Plaintiffs and Class Members, which Marriott failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

59. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[21]

60. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[22]

61. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all

[20] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

[21] *https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point*

[22] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf.

unauthorized transactions at roughly US $215 per cardholder incurring these charges,[23] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

63. Thus, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

G. Plaintiffs and Class Members Suffered Damages

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

65. The Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common

[23] Hadley Malcom, *Consumers rack up $14.3 billion in gray charges, research study commissioned for Billguard by Aite Research, USA Today* (July 25, 2013), available at: https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/.

[24] GAO, Report to Congressional Requesters, at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf

law, including Marriott's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

66. Marriott had the resources to prevent a breach. Marriott made significant expenditures to market its hotels and hospitality services, but neglected to adequately invest in data and cyber security, despite the growing number of data intrusions and several years of well-publicized data breaches, including its own massive breach a little over a year ago.

67. Had Marriott remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Marriott would have prevented intrusion into its information storage and security systems and, ultimately, the theft of its consumers' confidential PII.

68. As a direct and proximate result of Marriott's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to purchase credit monitoring services and take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

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

a. monies paid for credit monitoring and identity theft prevention services;

b. theft of their personal and financial information;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft;

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

e. the improper disclosure 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 the Data Breach;

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

i. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach.

70. While Plaintiffs' and Class Members' PII have been compromised, Marriott continues to hold consumers' PII, including Plaintiffs' and Class Members'. Particularly because Marriott has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

H. Marriott's Offer of Credit Monitoring is Inadequate

71. In recognition of the increased risk of identity theft that Plaintiffs and Class Members now face due to the Data Breach, Marriott has offered one year of free enrollment in Experian's IdentityWorks, a credit monitoring service. This one-year period of time is woefully short of what is necessary to protect Plaintiffs and Class Members who now face a lifetime of increased risk of identity theft, fraud, and other tortious and criminal behavior.

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

73. 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.

74. Marriott's response to the Data Breach, and the services it offered to consumers to address the breach, are insufficient, resulting in consumers spending a significant amount of time taking measures to protect themselves. Thus, Marriott cannot be heard to complain about consumers taking its advice and suggestions for how to respond in the face of this latest Data Breach to be suffered by Marriott consumers.

CLASS ACTION ALLEGATIONS

75. Pursuant to Rules 23(b)(2), (b)(3) and (c)(4), Plaintiff, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following class (the "Nationwide Class"):

> All persons in the United States who provided PII to Marriott and whose PII was accessed, compromised, or stolen from Marriott in the Data Breach announced on March 31, 2020.

76. Excluded from the Nationwide Class are Marriott and any entities in which any Marriott or its subsidiaries or affiliates have a controlling interest, and Marriott's officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family.

77. The Nationwide Class asserts claims against Marriott for Negligence, Negligence *Per Se*, Breach of Contract, Breach of Implied Contract, Unjust Enrichment, Declaratory Judgment, and breach of confidence.

78. Mr. Lopez, individually and on behalf of all California residents in the alternative, brings this lawsuit on behalf of himself and those similarly-situated California residents on behalf of the following California Subclass (the "California Subclass"):

> All persons in California who provided PII to Marriott and whose PII was accessed, compromised, or stolen from Marriott in the Data Breach announced on March 31, 2020.

79. Ms. Springmeyer, individually and on behalf of all Nevada residents in the alternative, brings this lawsuit on behalf of herself and those similarly-situated Nevada residents on behalf of the following Nevada Subclass (the "Nevada Subclass"):

> All persons in Nevada who provided PII to Marriott and whose PII was accessed, compromised, or stolen from Marriott in the Data Breach announced on March 31, 2020.

80. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. The Class consists of approximately 5.2 million Marriott consumers. The names and addresses of Class Members are identifiable through documents maintained by Marriott.

81. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class Members, including:

i. Whether Marriott represented to the Class that it would safeguard Class Members' PII;

ii. Whether Marriott owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iii. Whether Marriott breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iv. Whether Class Members' PII was accessed, compromised, or stolen in the Data Breach;

v. Whether Marriott knew or should have known that its computer data and cyber security systems were vulnerable to attack;

vi. Whether Marriott knew about the Data Breach before it was announced to the public and Marriott failed to timely notify the public of the Data Breach;

vii. Whether Marriott's conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*,

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

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

82. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

83. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiffs and the other Class Members were injured through the substantially uniform misconduct by Marriott. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. Plaintiffs' claims and those of other Class Members arise from the same operative facts and are based on the same legal theories.

84. **Adequacy of Representation:** Plaintiffs are adequate representatives of the class because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation and Plaintiffs will prosecute this action vigorously. The Class Members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

85. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other members of their respective classes are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Marriott, making it impracticable for Class Members to individually seek redress for Marriott's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

86. Further, Marriott has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

87. 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 Class Members' PII was accessed, compromised, or stolen in the Data Breach;

b. Whether (and when) Marriott knew about any security vulnerabilities that led to the Data Breach before it was announced to the public and whether Marriott failed to timely notify the public of those vulnerabilities and the Data Breach;

c. Whether Marriott's representations that it would secure and protect the PII of Plaintiffs and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Marriott's services;

d. Whether Marriott misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs' and Class Members' PII;

e. Whether Marriott concealed crucial information about its inadequate data and cyber security measures from Plaintiffs and the Class;

f. Whether Marriott failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data and cyber security;

g. Whether Marriott knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and Class Members' PII secure and prevent the loss or misuse of that information;

h. Whether Marriott failed to "implement and maintain reasonable security procedures and practices" for Plaintiffs' and Class Members' PII in violation of Section 5 of the FTC Act;

i. Whether Marriott failed to provide timely notice of the Data Breach;

j. Whether Marriott owed a duty to Plaintiffs and the Class to safeguard their PII and to implement adequate data and cyber security measures;

k. Whether Marriott breached that duty;

l. Whether such representations were false with regard to storing and safeguarding Plaintiffs' and Class Members' PII; and

m. Whether such representations were material with regard to storing and safeguarding Class Members' PII.

CHOICE OF LAW FOR NATIONWIDE CLAIMS

88. The state laws of one state should govern Plaintiffs' and Class Members' claims.

89. First, the principal place of business of Marriott, located in Bethesda, Maryland, is the "nerve center" of its business activities—the place where its executive-level and similarly-responsible officers, directors, and other high-level employees direct, control, and coordinate the corporation's activities, including Marriott's data and cyber security functions and major policy, financial, and legal decisions.

90. Maryland has a significant interest in regulating the conduct of businesses operating within its borders. Maryland, which seeks to protect the rights and interest of residents and citizens

of the United States against a company headquartered and doing business in Maryland, has a greater interest in the nationwide claims of Plaintiffs and Class Members than any other state and is most intimately concerned with the claims and outcome of this litigation.

91. Upon information and belief, Marriott's response to the Data Breach, and the decisions and responses thereto, were made from and in Maryland.

92. Upon information and belief, Marriott's breaches of duty to Plaintiffs and Class Members emanated from Maryland.

93. Application of Maryland law to Plaintiffs' and Class Members' claims would be neither arbitrary nor fundamentally unfair because Maryland has a significant interest in the claims of Plaintiffs and Class Members.

94. Under choice of law principles applicable to this litigation, the common law of Maryland would apply to the nationwide common law claims of all class members given Maryland's significant interest in regulating the conduct of businesses—Marriott included—operating within its borders. Thus, consumer protection laws may be applied to non-resident consumers across the United States.

CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

First Claim for Relief
Negligence
(On behalf of Plaintiffs and the Nationwide Class)

95. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 94 as though fully stated herein.

96. Marriott owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. More specifically, this duty included, among

other things: (a) designing, maintaining, and testing Marriott's data security systems to ensure that Plaintiffs' and Class Members' PII in Marriott's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its data systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data and cyber security measures consistent with industry standards.

97. Marriott knew that the PII belonging to Plaintiffs and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Marriott also knew of the serious harms that could happen if the PII of Plaintiffs and the Class was wrongfully disclosed, that disclosure was not fixed, or Plaintiffs and the Class were not told about the disclosure in a timely manner.

98. By being entrusted by Plaintiffs and the Class to safeguard their PII, Marriott had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up for and paid for Marriott's services and agreed to provide their PII with the understanding that Marriott 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. Marriott did not.

99. Marriott had a common law duty to prevent foreseeable harm to its consumers. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Marriott knew that it was more likely than not Plaintiffs and other Class Members would be harmed.

100. Marriott is morally culpable, given the prominence of security breaches in the hospitality industry and its own recent massive breach which demonstrated Marriott's wholly inadequate cyber security measures and safeguards.

101. Marriott breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to Plaintiffs' and the other Class member's PII.

102. Marriott breached the duties it owed to Plaintiffs and Class Members described above and thus was negligent. Marriott breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose in a timely fashion that Plaintiffs' and Class Members' PII in Marriott's possession had been or was reasonably believed to have been, stolen or compromised.

103. Marriott's failure to comply with industry and federal regulations further evidences Marriott's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class Members' PII.

104. Marriott's breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Marriott to acknowledge and correct serious and ongoing data and cyber security problems.

105. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiffs and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized

persons. Marriott's negligence was a direct and legal cause of the theft of the PII of Plaintiffs and the Class and all resulting damages.

106. Marriott also had a duty to safeguard the PII of Plaintiffs and Class Members and to promptly notify them of a breach because of laws and regulations that require Marriott to reasonably safeguard PII, as detailed herein.

107. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or lock their credit profiles, cancel current passports and obtain new passports, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Marriott's misconduct.

108. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of Marriott's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII. Marriott knew its systems and technologies for processing and securing the PII of Plaintiffs and the Class had numerous security vulnerabilities.

109. As a result of this misconduct by Marriott, the PII of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. Plaintiffs and the Class have also suffered consequential out of pocket losses for

procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Second Claim for Relief
Negligence *Per Se*
(On behalf of Plaintiffs and the Nationwide Class)

110. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 94 as though fully stated herein.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Marriott, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Marriott's duty in this regard.

112. Marriott violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Marriott's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach at a hospitality chain as large as Marriott, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

113. Marriott's violation of Section 5 of the FTC Act constitutes negligence *per se*.

114. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

115. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data and cyber security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

116. As a direct and proximate result of Marriott's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

117. Additionally, as a direct and proximate result of Marriot's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Marriott's possession and is subject to further unauthorized disclosures so long as Marriott fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

Third Claim for Relief
Breach of Contract
(On behalf of Plaintiffs and the Nationwide Class)

118. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 94 as though fully stated herein.

119. At all times during Plaintiffs' and Class Members' interactions with Marriott, Marriott was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to Marriott.

120. Marriott's Privacy Statement is an agreement between Marriott and individuals who provided their PII to Marriott, including Plaintiffs and Class Members

121. Marriott's Privacy Statement states that it applies to consumers and those who choose to stay at Marriott properties, and details how Marriott will both protect and use the PII provided by consumers for Marriott's use.

122. The Privacy Policy provides detailed information about what types of PII will be used and for which "legitimate business purposes," as well as when it will be sold or shared with third parties, and finally that Marriott seeks "to use reasonable organizational, technical and administrative measures to protect consumers PII."

123. Plaintiffs and Class Members on the one hand, and Marriott on the other, formed a contract when Plaintiffs and Class Members provided PII to Marriott subject to the Privacy Policy.

124. Plaintiffs and Class Members provided their PII to Marriott when they, among other things, used Marriott's services, enrolled in Marriott's loyalty and rewards programs, purchased products and services from Marriott, and/or booked reservations at a Marriott Property via offline and online channels. Consequently, Plaintiffs and Class Members who transacted with Marriott manifested their willingness to enter into a bargain with Marriott and intention to assent to the terms of the Privacy Statement by providing their PII to Marriott.

125. Plaintiffs and Class Members fully performed their obligations under the contract with Marriott.

126. Conversely, Marriott, in collecting Plaintiffs' and Class Members' PII, manifested its intent to adhere to its obligations under the Privacy Statement, including using "reasonable organizational, technical and administrative measures to protect [its consumers'] Personal Data."

127. Marriott breached its agreements with Plaintiffs and Class Members by failing to protect their PII. Specifically, Marriott: (1) failed to use reasonable organizational, technical,

procedural, and administrative measures to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of their agreements.

128. As a direct and proximate result of these breaches of contract, Plaintiffs and Class Members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

Fourth Claim for Relief
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

129. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 94 as though fully stated herein.

130. Plaintiffs and Class Members also entered into an implied contract with Marriott when they obtained services from Marriott, or otherwise provided PII to Marriott.

131. As part of these transactions, Marriott agreed to safeguard and protect the PII of Plaintiffs and Class Members.

132. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Marriott's data and cyber security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class Members believed that Marriott would use part of the monies paid to Marriott under the implied contracts to fund adequate and reasonable data and cyber security practices.

133. Plaintiffs and Class Members would not have provided and entrusted their PII to Marriott or would have paid less for Marriott's services in the absence of the implied contract or implied terms between them and Marriott. The safeguarding of the PII of Plaintiffs and Class Members was critical to realize the intent of the parties.

134. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Marriott.

135. Marriott breached its implied contracts with Plaintiffs and Class Members to protect their PII when it: (1) failed to have security protocols and measures in place to protect that information; and (2) disclosed that information to unauthorized third parties.

136. As a direct and proximate result of Marriott's breaches of implied contract, Plaintiffs and Class Members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

Fifth Claim for Relief
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

137. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 94 as through fully stated herein.

138. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII conferred upon, collected by, and maintained by Marriott and that was stolen in the Data Breach.

139. Marriott benefited from receiving Plaintiffs' and Class Members' PII by its ability to retain and use that information for its own benefit. Marriott understood this benefit.

140. Marriott also understood and appreciated that Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Marriott maintaining the privacy and confidentiality of that PII.

141. But for Marriott's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and untrusted with Marriott. Indeed, if Marriott had informed Plaintiffs and Class Members that Marriott's data and cyber security

measures were inadequate, Marriott would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

142. As a result of Marriott's wrongful conduct, Marriott has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Marriott continues to benefit and profit from its retention and use of the PII while its value to Plaintiffs and Class Members has been diminished.

143. Marriott's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Amended Complaint, including compiling, using, and retaining Plaintiffs' and Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

144. Under the common law doctrine of unjust enrichment, it is inequitable for Marriott to be permitted to retain the benefits it received, and still receives, without justification, from Plaintiffs and Class Members in an unfair and unconscionable manner. Marriott's retention of such benefits under the circumstances makes it inequitable, constituting unjust enrichment.

145. The benefit conferred upon, received, and enjoyed by Marriott was not conferred officiously or gratuitously, and it would be inequitable and unjust for Marriott to retain that benefit.

146. Marriott is therefore liable to Plaintiffs and Class Members for restitution in the amount of the benefit. Conferred on Marriott as a result of its wrongful conduct, including specifically the value to Marriott of the PII that was stolen in the Data Breach and the profits Marriott is receiving from the use of that PII.

Sixth Claim for Relief
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

147. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 94 as though fully stated herein.

148. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. This Court has broad authority to restrain acts, such as those alleged herein, which are tortious and violate the terms of the laws described above and herein.

149. An actual controversy has arisen in the wake of the Data Breach regarding present and prospective common law and other duties to reasonably safeguard Marriott's consumers' PII and whether Marriott is currently maintaining data and cyber security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise the PII they shared with Marriott. Plaintiffs allege that Marriott's data and cyber security measures remain inadequate, and that Plaintiffs and Class Members continue to suffer injury as a result of the Data Breach. Plaintiffs and Class Members remain at imminent risk that further compromises of their PII provided to Marriott will occur in the future.

150. Pursuant to the Court's authority under the Declaratory Judgment Act, the Court should enter a judgment declaring, *inter alia*, the following:

a. Marriott continues to owe a legal duty to secure consumers' PII;

b. Marriott continues to owe a legal duty to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and respective state statutes;

c. Marriott continues to breach these legal duties by failing to employ reasonable measures to secure consumers' PII.

151. The Court should also issue corresponding prospective injunctive relief requiring Marriott to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

152. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack any adequate legal remedy, should another data breach occur due to Marriott's insufficient practices. As described above, a subsequent data breach is real, immediate, and substantial, as Marriott remains a rich target for hackers and other malicious actors. If another data breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

153. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Marriott if an injunction is issued. Among other things, Plaintiffs would be subjected to fraud, identity theft, and other harms should another data breach occur. The cost to Marriott of complying with such an injunction is relatively minimal, and Marriott has pre-existing legal obligations to employ such measures.

154. Issuance of the requested injunction will not disserve the public interest. Instead, such an injunction would *benefit* the public by mitigating and preventing another data breach, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and other consumers whose PII would be further compromised.

Seventh Claim for Relief
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

155. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 94 as though fully stated herein.

156. At all times during Plaintiffs' and Class Members' interactions with Marriott, Marriott was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to Marriott.

157. As alleged herein and above, Marriott's relationship with Plaintiffs and Class Members was governed by expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

158. Plaintiffs and Class Members provided their respective PII to Marriott with the explicit and implicit understandings that Marriott would protect and not permit the PII to be disseminated to any unauthorized parties.

159. Plaintiffs and Class Members also provided their respective PII to Marriott with the explicit and implicit understanding that Marriott would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

160. Marriott voluntarily received in confidence Plaintiffs' and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

161. Due to Marriott's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII was disclosed and misappropriated

to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

162. As a direct and proximate cause of Marriott's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

163. But for Marriott's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Marriott's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

164. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Marriott's unauthorized disclosure of Plaintiffs' and Class Members' PII. Marriott knew its computer systems and cyber security practices for accepting and securing Plaintiffs' and Class Members' PII had numerous security vulnerabilities because Marriott failed to observe industry standard information security practices.

165. As a direct and proximate result of Marriott's breaches of confidence, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

166. As a direct and proximate result of Marriott's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

Eighth Claim for Relief
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.* (Unlawful Business Practices)
(On Behalf of Mr. Lopez and the California Subclass)

167. Mr. Lopez repeats, realleges, and re-incorporates by reference the allegations contained in paragraphs 1 through 87 as though fully stated herein.

168. Marriott violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Subclass.

169. Marriott engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Mr. Lopez's and California Subclass Members' PII with knowledge that the information would not be adequately protected; and by storing Mr. Lopez's and California Subclass Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Marriott to take reasonable methods of safeguarding the PII of Mr. Lopez and the California Subclass Members.

170. In addition, Marriott engaged in unlawful acts and practices by failing to disclose the Breach to California Subclass Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

171. As a direct and proximate result of Marriott's unlawful practices and acts, Mr. Lopez and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Marriott for the services, the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

172. Marriott knew or should have known that its computer systems and data and cyber security practices were inadequate to safeguard California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Marriott's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Mr. Lopez and the members of the California Subclass.

173. Mr. Lopez and California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Mr. Lopez and California Subclass Members of money or property that Marriott may have acquired by means of Marriott's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Marriott because of Marriott's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Ninth Claim for Relief
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.* (Unfair Business Practices)
(On Behalf of Mr. Lopez and the California Subclass)

174. Mr. Lopez repeats, realleges, and re-incorporates by reference the allegations contained in paragraphs 1 through 87 as though fully stated herein.

175. Marriott engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Mr. Lopez's and California Subclass Members' PII with knowledge that the information

would not be adequately protected; and by storing Mr. Lopez's and California Subclass Members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Mr. Lopez and California Subclass Members. These unfair acts and practices were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Mr. Lopez and the California Subclass Members outweighed their utility, if any.

176. Marriott engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Mr. Lopez's and California Subclass Members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Mr. Lopez and California Subclass Members. These unfair acts and practices were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Mr. Lopez and the California Subclass Members outweighed their utility, if any.

177. As a direct and proximate result of Marriott's acts of unfair practices, Mr. Lopez and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Marriott for the services, the loss of Mr. Lopez's and California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

178. Marriott knew or should have known that Marriott's computer systems and data and cyber security practices were inadequate to safeguard Mr. Lopez's and California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Marriott's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful,

and/or wanton and reckless with respect to the rights of Mr. Lopez and members of the California Subclass.

179. Mr. Lopez and California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Mr. Lopez and California Subclass Members of money or property that Marriott may have acquired by means of Marriott's unfair business practices, restitutionary disgorgement of all profits accruing to Marriott because of Marriott's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Tenth Claim for Relief
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq.* (§ 1798.150(a))
(On Behalf of Mr. Lopez and the California Subclass)

180. Mr. Lopez repeats, realleges, and re-incorporates by reference the allegations contained in paragraphs 1 through 87 as though fully stated herein.

181. Marriott violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Mr. Lopez's and California Subclass Members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Marriott's violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Mr. Lopez and California Subclass Members.

182. As a direct and proximate result of Marriott's acts, Mr. Lopez's and the California Subclass Members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Marriott's violation of the duties described above and herein.

183. As a direct and proximate result of Marriott's acts, Mr. Lopez and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Marriott for the services, the loss of Mr. Lopez's and California Class Members'

legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

184. Marriott knew or should have known that Marriott's computer systems and data and cyber security practices were inadequate to safeguard Mr. Lopez's and California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Marriott failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Mr. Lopez and the California Class Members.

185. Marriott is a company that is organized or operated for the profit or financial benefit of its owners, with annual gross revenues over $25 million. Marriott collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

186. Mr. Lopez and California Subclass Members seek relief under § 1798.150(a), including, but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5).

187. Mr. Lopez and the California Subclass Members reserve the right to amend this Complaint as of right to seek statutory damages and relief under. Cal. Civ. Code § 1798.100.

Eleventh Claim for Relief
Violation of Nevada Deceptive Trade Practices Act
Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.*
(On Behalf of Ms. Springmeyer and the Nevada Subclass)

188. Ms. Springmeyer repeats, realleges, and re-incorporates by reference the allegations contained in paragraphs 1 through 36, and 42 through 87 as through fully stated herein.

189. Marriott advertised, offered, or sold goods or services from Maryland to Nevada and engaged in trade or commerce directly or indirectly affected the people of Nevada.

190. Marriott engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. Ann. §§ 598.0915 and 598.0923, including:

a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. Ann. § 598.0915(5);

b. Representing that goods or services for sale are of a particular standard, quality, or grade when Marriott knew or should have known that those are of another standard, quality, or grade in violation of Nev. Rev. State. Ann. § 598.0915(7);

c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat. Ann. § 598.0915(9);

d. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. Ann. § 598.0923(A)(2); and

e. Violating state and federal laws relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

191. Marriott's deceptive trade practices in the course of its business or occupation include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Ms. Springmeyer's and Nevada Subclass Members' PII, 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 Ms. Springmeyer and Nevada Subclass Members' PII, including duties imposed by the FTC Act and Nevada's data security statute, Nev. Rev. Stat. Ann. § 603A.210, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Ms. Springmeyer's and Nevada Subclass Members' PII, 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 Ms. Springmeyer's and Nevada Subclass Members' PII, including duties imposed by the FTC Act and Nevada's data security statute, Nev. Rev. Stat. Ann. § 603A.210;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Ms. Springmeyer's and Nevada Subclass Members' PII; 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 Ms. Springmeyer's and Nevada Subclass Members' PII, including duties imposed by the FTC Act and Nevada's data security statute, Nev. Rev. Stat. Ann. § 603A.210.

192. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data and cyber security and ability to protect the confidentiality of consumers' PII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class Members, respectfully request this Court enter an Order:

a. An Order certifying this case as a class action;

b. An Order appointing Plaintiffs as class representatives;

c. An Order appointing undersigned counsel as class counsel;

d. A mandatory injunction directing Marriott to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

e. An award of damages, at a minimum, nominal damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims so triable.

Dated: June 29, 2020.

/s/ *John A. Yanchunis*
John A. Yanchunis, Esq. (*Pro Hac Vice*)

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis (Admitted *Pro Hac Vice*)
jyanchunis@ForThePeople.com
Jean S. Martin (Admitted *Pro Hac Vice*)
jeanmartin@ForThePeople.com
Ryan J. McGee (Admitted *Pro Hac Vice*)
rmcgee@ForThePeople.com

201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813/223-5505
813/223-5402 (fax)

LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Karen Hanson Riebel (Admitted *Pro Hac Vice*)
khriebel@locklaw.com
Kate M. Baxter-Kauf (Admitted *Pro Hac Vice*)
kmbaxter-kauf@locklaw.com
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981

MURPHY, FALCON & MURPHY, P.A.
William H. Murphy III, Esq. (Bar No. 30126)
hassan.murphy@murphyfalcon.com
One South Street, 23rd Floor
Baltimore, MD 21202
Telephone: (410) 951-8744
Facsimile: (410) 539-6599

GLANCY, PRONGAY & MURRAY
Brian Murray (*Pro Hac Vice* Forthcoming)
BMurray@GlancyLaw.com
230 Park Avenue, Suite 530
New York, NY 10169
Telephone: (212) 682-5340
Facsimile: (212) 884-0988

TOSTRUD LAW GROUP, P.C.
Jon A. Tostrud (*Pro Hac Vice* Forthcoming)
jtostrud@tostrudlaw.com
Anthony M. Carter (*Pro Hac Vice* Forthcoming)
acarter@tostrudlaw.com
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600
Facsimile: (310) 278-2640

Attorney for Plaintiffs and the Class