UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

HARRY BELL
30 Capitol St.
Charleston, WV 25301

and

EDWARD CLAFFY
626 W. Jackson Boulevard, Suite 500
Chicago, Illinois 60661,

Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

MARRIOTT INTERNATIONAL, INC., (a Montgomery County, Maryland Resident)
10400 Fernwood Road
Bethesda, Maryland 20817

Defendant

CASE NO.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

(1) Negligence
(2) Negligence *Per Se*
(3) Breach of Confidence
(4) Deceptive & Unfair Trade Practices

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

SUMMARY OF THE CASE

1. Marriott is one of the largest hotel chains in the World. Upon information and belief, approximately 500 million people have stayed at Marriott and Marriott-owned properties since 2014.

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 information, including their names, birthdates, addresses, locations, email addresses, and payment card information. Additionally, for international travel (to Canada, Europe, and the like), Marriott requires guests to provide their passport information, including passport numbers. This passport information, along with the aforementioned personal information, is collectively referred to herein as "PII."

3. This case involves the data breach Marriott announced on November 30, 2018, wherein the PII of up to 500 million guests was exposed due to a flaw in Marriott's reservation system and database systems dating back to 2014, which allowed hackers and other nefarious actors to take over guests' accounts and siphon off PII for unsavory and illegal purposes.

4. This Class Action Complaint is filed on behalf of all persons in the United States, described more fully in the following sections, whose PII was compromised in the data breach.

JURISDICTION AND VENUE

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

6. Venue is proper under 28 U.S.C. § 1391(c) because Defendant is a corporation that does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or

emanated from this District, including the decisions made by Marriott's governance and management personnel that led to the breach. Further, Marriott's terms of service governing users in the United States provides for Maryland venue for all claims arising out of Plaintiffs' relationship with Marriott.

PARTIES

A. Plaintiffs

7. Plaintiff Harry Bell ("Bell") is a resident and citizen of West Virginia. Plaintiff Bell has stayed at Marriott properties and hotels for decades, entrusting Marriott with aggregating PII for this time period. On or about November 30, 2018, Plaintiff Bell reviewed news accounts, as well as a notification from Marriott indicating that his account and PII may have been compromised in the data breach. In addition to the damages detailed herein, the data breach has caused Plaintiff Bell to be at substantial risk for further identity theft.

8. Plaintiff Edward Claffy ("Claffy") is a resident and citizen of Illinois. Plaintiff Claffy has stayed at Marriott properties and hotels for at least the last eight years, entrusting Marriott with and aggregating PII for this time period. On or about November 30, 2018, Plaintiff Claffy received a notice from Marriott informing him that his account and PII may have been compromised in the data breach. In addition to the damages detailed herein, the data breach has caused Plaintiff Claffy to be at substantial risk for further identity theft.

9. Plaintiffs have taken great steps to protect their PII, including shredding documents containing PII, not transmitting their PII via un-encrypted means, regularly monitoring their credit reports, and entrusting their PII only to entities that represent they follow industry-standard guidelines for the protection and storage of PII. Plaintiffs travel internationally and provided their passport information to the Defendant.

B. Defendant

10. Defendant Marriott, Inc., is a corporation with its principal executive offices located at 10400 Fernwood Rd, Bethesda, Maryland 20817 (Montgomery County). Marriott's securities trade on the NASDAQ under the ticker symbol "MAR."

FACTUAL BACKGROUND

A. Marriott's Data Collection Practices

11. In 2017, Marriott produced a report of brand-wide revenue totaling more than $1.32 billion for the third fiscal quarter ending September 30, 2018.

12. Marriott is an American multinational, diversified hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities, and is considered the largest hotel chain in the world, with more than 6,500 properties in 127 countries and territories globally, accommodating over 1.2 million rooms.

13. Upon information and belief, Marriott collects, stores, and maintains the PII of all guests who stay at Marriott properties.

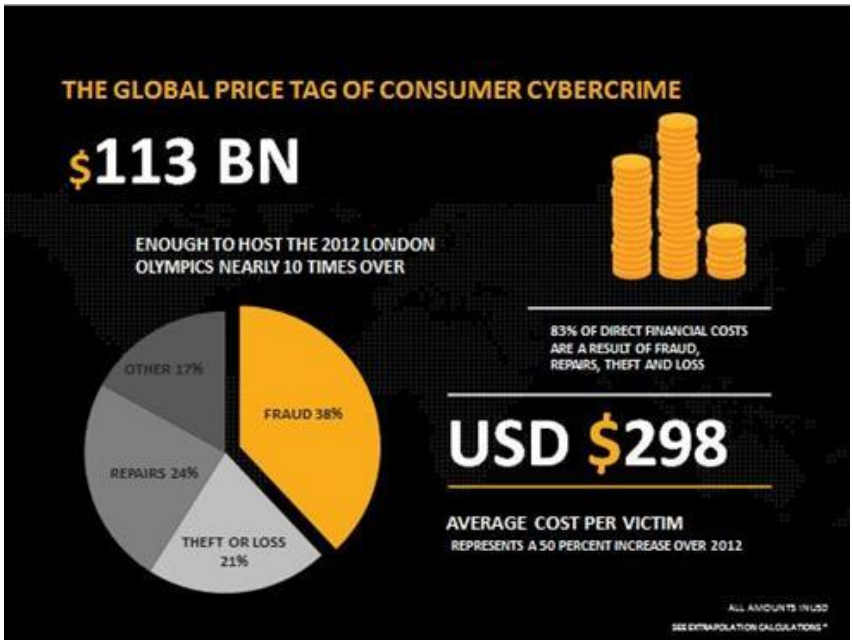
B. PII is Very Valuable on the Black Market

14. The types of information compromised in the Data Breach are highly valuable to identity thieves. The names, email addresses, recovery email accounts, telephone numbers, payment card information, passport information, and other valuable PII can all be used to gain access to a variety of existing accounts and websites.

15. 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.[1]

16. To put it into context, as demonstrated in the chart below, 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. That number will no doubt increase exponentially after the PII of over 50 million users was leaked in the September 2018 Data Breach.



17. 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

[1] The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007), http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

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

18. 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.[2] Websites appear and disappear quickly, making it a very dynamic environment.

19. 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.

C. Marriott's Inadequate Data Security Allows the Massive Breach of 500 Million Guest Accounts

20. On November 30, 2018, Marriott announced a previously unreported attack on its network, that exposed the PII of 500 million users (the "Data Breach").[3]

21. Marriott claims it discovered the vulnerability on September 8, 2018, "from an internal security tool regarding an attempt to access the Starwood guest reservation database," and "quickly engaged leading security experts to help determine what occurred."[4]

[2] 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.
[3] Kroll, *Starwood Guest Reservation Database Security Incident*, https://answers.kroll.com/
[4] *Id.*

22. During Marriott's investigation (again, beginning September 8, 2018), Marriott learned that nefarious actors had access to the guest reservation database since 2014—unfettered and allegedly undetected access for four years.[5]

23. Of the 500 million guests who could have been affected by the Data Breach, approximately 327 million of the affected guests include some combination of their name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation dates, communication preferences, and other PII.[6] For "some" of these affected guests, additional information, such as payment card numbers and payment card expiration dates, also included as PII.[7]

24. Despite Marriott's use of AES-128 encryption methods, the payment card numbers and payment card expiration dates may have been compromised, because the encryption method requires two components for decryption, and both may have been taken.[8]

25. For the remaining approximately 173 million of the affected guests, the information was limited to name, mailing address, email address, and "other information," that Marriott has not expanded upon or provided more details, leaving consumers without full knowledge of the extent of the breach of their information.[9]

26. Marriott, however, did not know the origin of or identify the hackers. In fact, Marriott has not fully assessed the scope of the attack, despite discovering the attack on September 8, 2018, and engaging "leading security experts."[10]

[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*

27. Unfortunately, despite numerous lapses in the hospitality industries, Marriott still lacks the safeguards and protections for users' PII, and that information remains at risk today and into the future, until Marriott is compelled to secure the PII stored on millions of United States citizens.

D. Marriott Failed to Comply With FTC Requirements

28. 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 security practices. According to the FTC, the need for data security should be factored into all business decision-making.[11]

29. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[12] The guidelines note businesses should protect the personal customer 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.

[11] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 18, 2018).

[12] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 18, 2018).

30. 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.[13]

31. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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 Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

32. 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.

33. In this case, Marriott was at all times fully aware of its obligation to protect the personal and financial data of Marriott's guests and customers because of its participation in the storage of PII, storage of payment card information, and interactions with payment card processing networks. Marriott was also aware of the significant repercussions if it failed to do so because Marriott collected payment card data from hundreds of millions of guests and customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiffs and Class members.

[13] FTC, *Start With Security*, *supra* note 11.

34. Despite understanding the consequences of inadequate data security, Marriott failed to take appropriate protective measures to protect and secure guests' and customer's PII, including Plaintiffs and Class members.

35. Despite understanding the consequences of inadequate data security, Marriott operated computer network systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; failed to detect intrusions dating back as far as 2014; and, failed to take other measures necessary to protect its data network.

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

36. Without detailed disclosure to Marriott's guests and customers, consumers, including Plaintiffs and Class members, were unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their PII for months, or even years, without being able to take necessary precautions to prevent imminent harm.

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

38. 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.[14]

39. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying

[14] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf, (last visited July 26, 2018).
[15] 17 C.F.R § 248.201 (2013).

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[16]

40. 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 drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[17]

41. 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.

42. Analysis of a 2016 survey of 5,028 consumers found "The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[18]

---

[16] *Id.*

[17] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

[18] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new , February 1, 2017.

43. As a result of Marriott's delay in notifying consumers of the Data Breach—nearly three months following the discovery—the risk of fraud for Plaintiffs and Class members has been driven even higher.

44. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[19]

45. 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.[20]

46. 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 unauthorized transactions at roughly US $215 per cardholder incurring these charges,[21] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

[19] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).
[20] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).
[21] 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/** (last visited July 26, 2018).

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

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

F. Plaintiffs and Class Members Suffered Damages

49. 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.

50. 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 law, including Marriott's failure to establish and implement appropriate administrative, technical,

[22] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

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.

51. 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 security, despite the growing number of data intrusions and several years of well-publicized data breaches.

52. 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 customers' confidential PII.

53. 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 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.

54. 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. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and misused via the sale of Plaintiffs' and Class members' information on the Internet's black market;

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. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. 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, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit

monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

55. While Plaintiffs' and Class members' PII have been stolen, 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.

G. Marriott's Offer of Credit Monitoring is Inadequate

56. 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.

57. 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.

58. 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.

CLASS ACTION ALLEGATIONS

59. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs, individually and on behalf of all others similarly situated, brings this lawsuit on behalf of themselves and as a class action on behalf of the following class:

> All persons in the United States who provided PII (including payment card information) to Marriott and whose PII was accessed, compromised, or stolen from Marriott in the Data Breach.

60. Excluded from the Class are Defendant and any entities in which any Defendant or its subsidiaries or affiliates have a controlling interest, and Defendant'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.

61. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. Plaintiffs reasonably believes that Class members number hundreds of millions of people or more in the aggregate and well over 1,000 in the smallest of the classes. The names and addresses of Class members are identifiable through documents maintained by Defendant.

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

i. Whether Defendant represented to the Class that it would safeguard Class members' PII;

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

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

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

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

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

63. 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.

64. **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 Defendant. 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. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

65. **Adequacy of Representation:** Plaintiffs is an adequate representative of the classes because their interests do not conflict with the interests of the other Class members he seeks to represent; he has 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.

66. **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 Defendant, making it impracticable for Class members to individually seek redress for Defendant'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.

67. Further, Defendant 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.

68. 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) Defendant knew about any security vulnerabilities that led to the Data Breach before it was announced to the public and whether Defendant failed to timely notify the public of those vulnerabilities and the Data Breach;

c. Whether Defendant'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 Defendant's services;

d. Whether Defendant 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 Defendant concealed crucial information about its inadequate data security measures from Plaintiffs and the Class;

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

g. Whether Defendant 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 Defendant 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 Defendant failed to provide timely notice of the Data Breach in violation of state consumer protection laws, including Md. Code Com. Law § 14-3501, *et seq.*;

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

k. Whether Defendant 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.

CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

First Claim for Relief
Negligence

69. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 68 as though fully stated herein.

70. Defendant 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. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the PII of Plaintiffs' and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

71. Defendant knew that the PII of Plaintiffs and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant 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.

72. By being entrusted by Plaintiffs and the Class to safeguard their PII, Defendant had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up for and paid for Defendant's services and agreed to provide their PII with the understanding that Defendant 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, Defendant did not. Defendant is morally culpable, given the prominence of security breaches in the hospitality industry, and especially given the admission that this data vulnerability dates back to 2014, demonstrating Defendant's wholly inadequate safeguards, and refusal to notify Plaintiffs and the Class of breaches or security vulnerabilities.

73. Defendant 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.

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

75. Defendant'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 Defendant to acknowledge and correct serious and ongoing data security problems again, as evidenced by this vulnerability existing since 2014.

76. But for Defendant'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. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiffs and the Class and all resulting damages.

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

78. As a result of this misconduct by Defendant, 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.

79. Defendant's misconduct as alleged herein is malice or oppression, in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the Class to cruel and unjust hardship in conscious disregard of their rights.

Second Claim for Relief
Negligence *Per Se*

80. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 79 as though fully stated herein.

81. 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.

82. 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 (approximately 500 million unique guests and consumers), 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.

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

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

85. 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 security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

86. 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; Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; 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.

87. 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 Confidence

88. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 87 as though fully stated herein.

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

90. As alleged herein and above, Defendant'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.

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

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

93. Defendant 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.

94. Due to Defendant'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' Customer Data was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

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

96. But for Defendant'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. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

97. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiffs' and Class Members' PII had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices, including Defendant's inability to detect the Data Breach as far back as 2014.

98. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; 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

99. As a direct and proximate result of Defendant'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.

Fourth Cause of Action
Violation of Maryland's Consumer Protection Act
Maryland Code Ann., Com. Law § 13-101 *et seq.*

100. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 99 as though fully stated herein.

101. This Count is brought pursuant to the Maryland Consumer Protection Act, Md. Code Ann., Com. Law ("CL") § 13-101 *et seq.*

102. Plaintiffs are consumers for the purposes of Maryland's Consumer Protection Act.

103. Defendant is merchant for the purposes of Maryland's Consumer Protection Act. Marriott was, at all times relevant herein, engaged in soliciting "consumer services" as that term is defined in CL § 13-101(d) by soliciting an ongoing service, credit reporting and data aggregation of Plaintiffs' personal information, to consumers in Maryland for primarily personal use within the meanings specified in the Act.

104. Marriott is also a "person" as that term is defined by CL § 13-101(h), as Marriott was, at all times relevant herein, a legal or commercial entity.

105. Defendant, by failing to inform consumers (including Plaintiffs and the Class Members) of Defendant's unsecure, uncompliant, and otherwise insufficient data and information security practices, advertised, sold, serviced, and otherwise induced those consumers (including Plaintiffs and Class Members) to purchase goods and services from Defendant.

106. By failing to inform consumers (including Plaintiffs and the Class Members) of its unsecure, uncompliant, and otherwise insufficient data and information security practices, Defendants falsely represented the security of their data and information security practices to safeguard the PII Defendant collected on consumers (including Plaintiffs and the Class Members).

107. Additionally, Maryland law requires notification of data breaches upon identification. Defendant identified the Data Breach as early as September 2018, but only identified consumers on November 30, 2018, thus placing those consumers at risk for the months in between the discovery and notification of the Data Breach.

108. Defendant's failures constitute false, misleading, and misrepresentations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) concerning the security of their networks and aggregation of PII.

109. In addition, the facts upon which consumers (including Plaintiffs and Class Members) relied were material facts, the veracity of which was not true (e.g., protection of PII), and consumers (including Plaintiffs and Class Members) relied on those false facts to their detriment.

110. Defendant employed these false representations to promote the sale of a consumer good or service, which Plaintiffs and the Class Members purchased.

111. As a direct and proximate result of Defendant'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.

PRAYER FOR RELIEF

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

(a) Certifying the United States Class, and appointing Plaintiffs as Class Representatives;

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

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

(d) Awarding Plaintiffs and the Class members 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) Requiring Defendant to provide appropriate credit monitoring services to Plaintiffs and the other class members;

(h) Awarding Plaintiffs and the Class members punitive damages;

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

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 30, 2018

Respectfully Submitted,

/s/ William H. Murphy III

William H. Murphy III, Esq. (Bar No. 30126)
Jessica H. Meeder, Esq. (Bar No. 17986)
MURPHY, FALCON & MURPHY, P.A.
One South Street, 23rd Floor
Baltimore, MD 21202
Telephone: (410) 951-8744
Facsimile: (410) 539-6599
hassan.murphy@murphyfalcon.com
jessica.meeder@murphyfalcon.com

John A. Yanchunis (Pro Hac Vice Forthcoming)
Ryan J. McGee (Pro Hac Vice Forthcoming)
Jonathan B. Cohen (Pro Hac Vice Forthcoming)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813/223-5505

813/223-5402 (fax)
jyanchunis@ForThePeople.com
rmcgee@ForThePeople.com
jcohen@ForThePeople.com

Attorneys for Plaintiffs and the Class