IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

VICKIE VETTER, CYNTHIA DEESE, LEE SLAGLE, DALE SMITH, RHONDA STEVENS, NIKOLE JORDAN, CURTIS PAYNE, STACEY WOLLMAN, KAREN RAMBAT, CATHERINE CARLBERG, SCOTT DIAS, MARETTA LEITKA, ANTHONY MALFI, LAWRENCE PERLMUTTER, ANDREW ROSE, DAVID SPARKS, JOAN KNUDSON, ELLEN KOWITT, BURNEASE RAGIN, GRETCHEN EHLE, PATRICE MATTHEWS, KEVIN WALLS, TONEKIA SHOWELL, DOREEN WHELAN, ROBERT BLUESTONE, KAREN DAVIS, RONALD MICHAEL FESCHAK, DOROTHY ODIE, CAROL OSTAPCHUK, EDWARD SIPERSTEIN, MARIA WOOTEN, CURTIS CUMMINGS, JON GOLDBERG, LATAUSHA GRIFFIN, DANIELLE HAYES, VIRGINIA HOWELL, MONICA JOHNSON, BEVERLY RICKS, THERESA SYKES, FELICIA WALLACE, JEAN WASKIEWICZ, JULIE DUCHSHERER, BARBARA ERICKSON, BEVERLY LOUK, SHANE SOMERVILLE, KIANA BELCHER, KEVIN BERRY, PETER TAPLING, EDGAR VAYNSHTEYN, AMBER HELTON, JULIE YOUNG, JASON YOUNG, MARY JO JUREY, MICHAEL RAPP, MARLON GAINES, KUMAR RASHAD, SONJA SCOTT, KYLE JASKI, ANGELA SONNIER, MARJORIE WHEELER, DEBRA WHIDDON, LINDA WINSEY, RUTHANNE CARPENTER, MAY DESROCHERS, JEFFREY KEMP, MARK ROTONDI, KAREN RUSSELL, JERI HOLT-MINTER, RICHARD

Case No.

CLASS ACTION COMPLAINT

RYANS, MICHAEL BUNKER, DEBRA MICHAUD, MICHAEL BLICHER, GRAVES DE ARMOND, MICHAEL FREELAND, STEVE GAJEWSKI, ROBERT KAISER, SUSAN MCINTOSH, JOEL ROSSON, IRA WEINTRAUB, MELISSA WHITE, CHARLES WILLIAMS, GERALD WILLIAMS, DENNIS WOOLDRIDGE, SUSAN BEVERLEY, NATHAN FINNEY, EDWARD HANLEY, SHEILA HARRISON, OLIVIA MAY, JANLISA PARRIS, DARREL PARRIS, JOE TAYLOR, SHAUN YURTKURAN, HOLGER MEYER, YVETTE BUTLER, SHELIA CANIPE, DOROTHY DAVIS, MARK DUFFEY, LINDA KITE, RICK SABATH, DEBRA TALLEY, ERIC GAULT, CAROL BLOOD, KATHLEEN CHRISTENSEN, MICHELLE FEATHERSTONE, JACK MILAM, LUCY KARL, TAMIKA JACKSON, JUDY MILLS, CHRIS MORRIS, LISA FREDERICKSON, JOSEPH THRONEBERRY, EDWARD BAKER, TANESHA BORADGIAK, CRYSTAL CHAMBERS, LISA FRITZ, LAURENE GALLWAY, PHYLLIS HECKER, JEFFREY RAHN, ANNE SANTO, VINCENT SAVARESE, ANNE SAVARESE, CURTIS WEAVER, BRAD BARRINGER, ANGELA GRESH, CHALISE MORRIS, DAVID MOYER, DEIDRINELLE ROUSE, TAMIKA SIMMONDS, SUSAN MULLINS, SAMI DIFUNTORUM, STEVEN OWENS, CHERYL CASTOR, MICHAEL CASTOR, PRUDENCE CONCERT-WHITE, SHAWN SEELEY, MELISSA YURKANIN, RICARDO VAQUER, MARY ELLEN DAVEY, CHRISTOPHER PRATT, VANCE EDWARD EICHELBERGER, JUSTIN PALMER, DAVID SECRIST, JOHN GILLILAND, CHARLES HANSON,

AMANDA ARNOLD, DOUGLAS BLAKE, CARLA ENGLE, JANICE FRAZIER-SCOTT, BETSY GENTRY, JANET WENDER, RONZELLA WRIGHT-LOFTLY, DEANA CANNON, KENNETH DAVIS, SCOTT GIDEON, JERNARD GRIGGS, DONNA HUGHES, PATRICIA HUIZAR, SELMA RODRIGUEZ, BRUCE SANDERS, BEVERLY TOOKEY, JOHN WALLER, JONATHAN DODART, RUTH PATRICIA ROSADOS, RONALD KOTZ, DAVID MELENDEZ, ASIM PADH, MICHAEL RAIMONDI, JENINNE PITTS, CHRISTOPHER DAVIES, RIK LEWIS, CHRISTINA OLSEN, JOHN SIMMONS, JODY STEPHENS, GORDON THOMAS, JEFFREY OELHAFEN, BRENDA BURR, SARAH KORWAN, and KENT SPENCE, *individually and on behalf of all others similarly situated,*

Plaintiffs,

v.

MARRIOTT INTERNATIONAL, INC.,

Defendant.

Amy E. Keller
DiCello Levitt & Casey LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602

Andrew N. Friedman
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave NW
Suite 500
Washington, DC 20005

James J. Pizzirusso
Hausfeld LLP
1700 K Street, NW
Suite 650
Washington, DC 20006

Melissa H. Maxman
Cohen & Gresser LLP
2001 Pennsylvania Ave. NW
Suite 300
Washington, DC 20006

James Ulwick
KRAMON & GRAHAM PA
One South Street, Suite 2600
Baltimore, Maryland 21202

Plaintiffs' Counsel
Other Counsel Identified on Signature Pages

The individual consumer identified below (collectively, "Plaintiffs"), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Defendant Marriott International, Inc. (referred to herein as "Marriott" or "Defendant"), parent of Starwood Hotels & Resorts Worldwide, LLC (referred to herein as "Starwood"), for Starwood's failure to secure and safeguard its customers' personally identifiable information ("PII") such as passport information, customers' names, mailing addresses, and other personal information, as well as credit and debit card numbers and other payment card data ("PCD") (collectively, "Personal Information"). Starwood collected this information at the time customers registered on its website, checked-in to one of its hotels, used its Starwood Preferred Guest program (the "Loyalty Program"), or used it at one of its dining or retail operations within its hotels. Defendant knew this information presented a treasure trove of data to hackers, and should have used reasonable measures to protect it. Defendant also failed to provide timely, accurate, and adequate notice to Plaintiffs and other Class members (as defined below) that their data had been compromised in the breach, as well as precisely what types of information were taken. Plaintiffs suffered damages as a result of Defendant's misfeasance, and overpaid Defendant as they did not get the implicit data protection they expected when using Defendant's services.

INTRODUCTION

1. Marriott plays a central role in the modern travel industry as the world's largest hotel operator, with over 6,700 properties spanning over 130 countries and territories.

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

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

4. Marriott initially stated that the Data Breach impacted approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates.

5. Subsequently, Marriott revealed that after removing duplicates, the Data Breach impacted approximately 383 million guest records—making it the largest data loss in history. This includes over 5 million unencrypted passport numbers and 8.6 million credit and debit cards. Marriott has asserted it does not know who carried out the attack.

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

7. Marriott disregarded Plaintiffs' and Class Members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the Data Breach

from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Personal Information. On information and belief, Plaintiffs' and Class Members' Personal Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs' and Class Members' Personal Information was compromised and stolen. Plaintiffs therefore did not get the benefit of their bargain—implicit protection of their Personal Information when transacting with the Defendant. Moreover, this same Personal Information remains stored in Marriott's computer systems. Plaintiffs and Class Members have an interest in ensuring that their Personal Information is safe, and they are entitled to seek injunctive and other equitable relief, including independent oversight of Marriott's security systems.

JURISDICTION AND VENUE

8. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Marriott is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

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

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

10. Venue is proper in this District under 28 U.S.C. §§ 1391(a) through (d) because Marriott's principal place of business is located in this District and substantial parts of the events or omissions giving rise to the claims occurred in this District.

NAMED PLAINTIFFS

11. The Plaintiffs identified below bring this action on behalf of themselves and those similarly situated both across the United States and within their State or Territory of residence. As with the rest of the hundreds of millions of victims of the Marriott data breach, Marriott, through its actions described herein, leaked, disbursed, and furnished their valuable Personal Information to unknown cyber criminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

12. As used throughout this Complaint, "Personal Information" is defined as all information exposed by the Marriott data breach, including all or any part or combination of name, address, birth date, telephone number, email address, credit card number, or passport number.

ALABAMA

13. Plaintiff Cynthia Deese is a resident and citizen of the State of Alabama and a frequent user of the Defendant's Loyalty Program. Cynthia Deese provided her Personal Information to the Defendant on the assumption that Defendant would keep her Personal Information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her Personal Information, and notify her promptly in the event of a breach. Defendant provided her email notice that her Personal Information was compromised by the Data Breach. As a result of the Data Breach, Deese is taking measures that she otherwise

would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

14. Plaintiff Lee Slagle is a resident and citizen of the State of Alabama and a frequent user of the Defendant's Loyalty Program, having been a member for at least fifteen years. Lee Slagle provided his Personal Information to the Defendant on the assumption that Defendant would keep his Personal Information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his Personal Information, and notify him promptly in the event of a breach. Defendant provided him email notice that his Personal Information was compromised by the Data Breach. As a result of the Data Breach, Slagle is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

15. Plaintiff Dale Smith is a resident and citizen of the State of Alabama and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Dale Smith provided his Personal Information to the Defendant on the assumption that Defendant would keep his Personal Information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his Personal Information, and notify him promptly in the event of a breach. Defendant provided him email notice that his Personal Information was compromised by the Data Breach. As a result of the Data Breach, Smith is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

16. Plaintiff Rhonda Stevens is a resident and citizen of the State of Alabama and a frequent user of the Defendant's Loyalty Program, having been a member for at least seven years. Rhonda Stevens provided her Personal Information to the Defendant on the assumption that Defendant would keep her Personal Information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her Personal Information, and notify her promptly in the event of a breach. Defendant provided her email notice that her Personal Information was compromised by the Data Breach. As a result of the Data Breach, Stevens is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

ALASKA

17. Plaintiff Vickie Vetter is a resident and citizen of the State of Alaska and a frequent user of the Defendant's Loyalty Program, having been a member for at least eleven years. Vickie Vetter provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Vetter is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

ARIZONA

18. Plaintiff Karen Rambat is a resident and citizen of the State of Arizona and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years.

Karen Rambat provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Rambat is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

ARKANSAS

19. Plaintiff Nikole Jordan is a resident and citizen of the State of Arkansas and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Nikole Jordan provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Jordan is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

20. Plaintiff Curtis Payne is a resident and citizen of the State of Arkansas and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Curtis Payne provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Payne is taking measures that he otherwise would not

have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

21. Plaintiff Stacey Wollman is a resident and citizen of the State of Arkansas and a frequent user of the Defendant's Loyalty Program. Stacey Wollman provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Wollman is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

CALIFORNIA

22. Plaintiff Catherine Carlberg is a resident and citizen of the State of California and a frequent user of the Defendant's Loyalty Program, having been a member for at least four years. Catherine Carlberg provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Carlberg is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

23. Plaintiff Scott Dias is a resident and citizen of the State of California and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years.

Scott Dias provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Dias is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

24. Plaintiff Maretta Leitka is a resident and citizen of the State of California and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Maretta Leitka provided her to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Leitka is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

25. Plaintiff Anthony Malfi is a resident and citizen of the State of California and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Anthony Malfi provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Malfi is taking measures that he otherwise would not

have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

26. Plaintiff Lawrence Perlmutter is a resident and citizen of the State of California and a frequent user of the Defendant's Loyalty Program, having been a member for at least fifteen years. Lawrence Perlmutter provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Perlmutter is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

27. Plaintiff Andrew Rose is a resident and citizen of the State of California and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Andrew Rose provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Rose is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

28. Plaintiff David Sparks is a resident and citizen of the State of California and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years.

David Sparks provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Sparks is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

COLORADO

29. Plaintiff Joan Knudson is a resident and citizen of the State of Colorado and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Joan Knudson provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Knudson is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

30. Plaintiff Ellen Kowitt is a resident and citizen of the State of Colorado and a frequent user of the Defendant's Loyalty Program, having been a member for at least eighteen years. Ellen Kowitt provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Kowitt is taking measures that

she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Ms. Kowitt was also the victim of identity theft in January and February of 2018 as a result of the breach. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

CONNECTICUT

31. Plaintiff Burnease Ragin is a resident and citizen of the State of Connecticut and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Burnease Ragin provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Ragin is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

DELAWARE

32. Plaintiff Tonekia Showell is a resident and citizen of the State of Delaware and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Tonekia Showell provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Walls is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her

accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

33. Plaintiff Doreen Whelan is a resident and citizen of the State of Delaware and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Doreen Whelan provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Whelan is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

DISTRICT OF COLUMBIA

34. Plaintiff Gretchen Ehle is a resident and citizen of the District of Columbia and a frequent user of the Defendant's Loyalty Program, having been a member for at least seventeen years. Gretchen Ehle provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Ehle is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

35. Plaintiff Patrice Matthews is a resident and citizen of the District of Columbia and a frequent user of the Defendant's Loyalty Program, having been a member for at least fifteen years. Patrice Matthews provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Matthews is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

36. Plaintiff Kevin Walls is a resident and citizen of the District of Columbia and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Kevin Walls provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Walls is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

FLORIDA

37. Plaintiff Robert Bluestone is a resident and citizen of the State of Florida and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Robert Bluestone provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security

measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Bluestone is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

38. Plaintiff Karen Davis is a resident and citizen of the State of Florida and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Karen Davis provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Davis is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

39. Plaintiff Ronald Feschak is a resident and citizen of the State of Florida and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Ronald Feschak provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Feschak is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his

accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

40. Plaintiff Dorothy Odie is a resident and citizen of the State of Florida and a frequent user of the Defendant's Loyalty Program, having been a member for at least three years. Dorothy Odie provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Odie is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

41. Plaintiff Carol Ostapchuk is a resident and citizen of the State of Florida and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Carol Ostapchuk provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Ostapchuk is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

42. Plaintiff Edward Siperstein is a resident and citizen of the State of Florida and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty-

four years. Edward Siperstein provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Siperstein is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

43. Plaintiff Maria Wooten is a resident and citizen of the State of Florida and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Maria Wooten provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Wooten is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

GEORGIA

44. Plaintiff Curtis Cummings is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least fifteen years. Curtis Cummings provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was

compromised by the Data Breach. As a result of the Data Breach, Cummings is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

45. Plaintiff Jon Goldberg is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty-two years. Jon Goldberg provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Goldberg is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

46. Plaintiff Latausha Griffin is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least four years. Latausha Griffin provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Griffin is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her

accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

47. Plaintiff Danielle Hayes is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Danielle Hayes provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Hayes is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

48. Plaintiff Virginia Howell is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least eleven years. Virginia Howell provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Howell is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

49. Plaintiff Monica Johnson is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Monica Johnson provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Johnson is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

50. Plaintiff Beverly Ricks is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Beverly Ricks provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Ricks is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

51. Plaintiff Theresa Sykes is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Theresa Sykes provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure

that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Sykes is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

52. Plaintiff Felicia Wallace is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Felicia Wallace provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Wallace is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

53. Plaintiff Jean Waskiewicz is a resident and citizen of the State of Georgia and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Jean Waskiewicz provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Waskiewicz is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her

accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

HAWAII

54. Plaintiff Julie Duchscherer is a resident and citizen of the State of Hawaii and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Julie Duchscherer provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Duscherer is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

IDAHO

55. Plaintiff Shane Somerville is a resident and citizen of the State of Idaho and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Shane Sommerville provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Sommerville is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

ILLINOIS

56. Plaintiff Kiana Belcher is a resident and citizen of the State of Illinois and a frequent user of the Defendant's Loyalty Program, having been a member for at least eighteen years. Kiana Belcher provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Belcher is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

57. Plaintiff Kevin Berry is a resident and citizen of the State of Illinois and a frequent user of the Defendant's Loyalty Program, having been a member for at least eight years. Kevin Berry provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Berry is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

58. Plaintiff Peter Tapling is a resident and citizen of the State of Illinois and a frequent user of the Defendant's Loyalty Program, having been a member for at least thirty-one years. Peter Tapling provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security

measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Tapling is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

59. Plaintiff Edgar Vaynshteyn is a resident and citizen of the State of Illinois and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Edgar Vaynshteyn provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Vaynshteyn is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

INDIANA

60. Plaintiff Amber Helton is a resident and citizen of the State of Indiana and a frequent user of the Defendant's Loyalty Program, having been a member for at least three years. Amber Helton provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Helton is taking measures that she otherwise would not

have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

61. Plaintiff Jason Young is a resident and citizen of the State of Indiana and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Jason Young provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Young is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

62. Plaintiff Julie Young is a resident and citizen of the State of Indiana and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Julie Young provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Young is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

IOWA

63. Plaintiff Barbara Erickson is a resident and citizen of the State of Iowa and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Barbara Erickson provided her Personal Information to the Defendant on the assumption

Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Erickson is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

64. Plaintiff Beverly Louk is a resident and citizen of the State of Iowa and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Beverly Louk provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Louk is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

KANSAS

65. Plaintiff Mary Jo Jurey is a resident and citizen of the State of Kansas and a frequent user of the Defendant's Loyalty Program, having been a member for at least eleven years. Mary Jo Jurey provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Jurey is taking measures that

she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

66. Plaintiff Michael Rapp is a resident and citizen of the State of Kansas and a frequent user of the Defendant's Loyalty Program. Michael Rapp provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Rapp is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

KENTUCKY

67. Plaintiff Kumar Rashad is a resident and citizen of the Commonwealth of Kentucky and a frequent user of the Defendant's Loyalty Program. Kumar Rashad provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Rashad is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

68. Plaintiff Marlon Gaines is a resident and citizen of the Commonwealth of Kentucky and a frequent user of the Defendant's Loyalty Program. Marlon Gaines provided his

Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Gaines is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

69. Plaintiff Sonja Scott is a resident and citizen of the Commonwealth of Kentucky and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Sonja Scott provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Scott is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

LOUISIANA

70. Plaintiff Kyle Jaski is a resident and citizen of the State of Louisiana and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Kyle Jaski provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data

Breach. As a result of the Data Breach, Jaski is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

71. Plaintiff Angela Sonnier is a resident and citizen of the State of Louisiana and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Angela Sonnier provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Sonnier is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

72. Plaintiff Debra Whiddon is a resident and citizen of the State of Louisiana and a frequent user of the Defendant's Loyalty Program, having been a member for at least fourteen years. Debra Whiddon provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Whiddon is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

73. Plaintiff Marjorie Wheeler is a resident and citizen of the State of Louisiana and a frequent user of the Defendant's Loyalty Program. Marjorie Wheeler provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Wheeler is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

74. Plaintiff Linda Winsey is a resident and citizen of the State of Louisiana and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Linda Winsey provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Winsey is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

MAINE

75. Plaintiff Michael Bunker is a resident and citizen of the State of Maine and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Michael Bunker provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly

in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Bunker is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

76. Plaintiff Debra Michaud is a resident and citizen of the State of Maine and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Debra Michaud provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Michaud is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

MARYLAND

77. Plaintiff Jeri Holt-Minter is a resident and citizen of the State of Maryland and a frequent user of the Defendant's Loyalty Program, having been a member for at least eight years. Jeri Holt-Minter provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Holt-Minter is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her

accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

78. Plaintiff Richard Ryans is a resident and citizen of the State of Maryland and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Richard Ryans provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Ryans is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

MASSACHUSETTS

79. Plaintiff Ruthanne Carpenter is a resident and citizen of the Commonwealth of Massachusetts and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Ruthanne Carpenter provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Carpenter is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

80. Plaintiff May Desrochers is a resident and citizen of the Commonwealth of Massachusetts and a frequent user of the Defendant's Loyalty Program. May Desrochers provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Desrochers is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

81. Plaintiff Jeffrey Kemp is a resident and citizen of the Commonwealth of Massachusetts and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Jeffrey Kemp provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Kemp is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

82. Plaintiff Mark Rotondi is a resident and citizen of the Commonwealth of Massachusetts and a frequent user of the Defendant's Loyalty Program, having been a member for at least twelve years. Mark Rotondi provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate

security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Rotondi is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

83. Plaintiff Karen Russell is a resident and citizen of the Commonwealth of Massachusetts and a frequent user of the Defendant's Loyalty Program, having been a member for at least eight years. Karen Russell provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Russell is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

MICHIGAN

84. Plaintiff Michael Blicher is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Michael Blicher provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Blicher is taking measures that

he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

85. Plaintiff Graves De Armond is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Graves De Armond provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, De Armond is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

86. Plaintiff Michael Freeland is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Michael Freeland provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Freeland is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

87. Plaintiff Steve Gajewski is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Steve Gajewski provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Gajewski is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

88. Plaintiff Robert Kaiser is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least fifteen years. Robert Kaiser provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Kaiser is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

89. Plaintiff Susan McIntosh is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Susan McIntosh provided her Personal Information to the Defendant on the assumption

Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, McIntosh is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

90. Plaintiff Joel Rosson is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program. Joel Rosson provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Rosson is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

91. Plaintiff Ira Weintraub is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least four years. Ira Weintraub provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Weintraub is taking measures that he otherwise would

not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

92. Plaintiff Melissa White is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least three years. Melissa White provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, White is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

93. Plaintiff Charles Williams is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Charles Williams provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Williams is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

94. Plaintiff Gerald Williams is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Gerald Williams provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Williams is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

95. Plaintiff Dennis Wooldridge is a resident and citizen of the State of Michigan and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Dennis Wooldridge provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Wooldridge is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

MINNESOTA

96. Plaintiff Susan Beverley is a resident and citizen of the State of Minnesota and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty-seven years. Susan Beverley provided her Personal Information to the Defendant on the

assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Beverley is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

97. Plaintiff Nathan Finney is a resident and citizen of the State of Minnesota and a frequent user of the Defendant's Loyalty Program, having been a member for at least three years. Nathan Finney provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Finney is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

98. Plaintiff Edward Hanley is a resident and citizen of the State of Minnesota and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Edward Hanley provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Hanley is taking measures that

he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

99. Plaintiff Sheila Harrison is a resident and citizen of the State of Minnesota and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Sheila Harrison provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Harrison is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

MISSISSIPPI

100. Plaintiff Joe Taylor is a resident and citizen of the State of Mississippi and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Joe Taylor provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided his email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Taylor is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

101. Plaintiff Shawn Yurtkuran is a resident and citizen of the State of Mississippi and a frequent user of the Defendant's Loyalty Program. Shawn Yurtkuran provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Yurtkuran is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

MISSOURI

102. Plaintiff Olivia May is a resident and citizen of the State of Missouri and a frequent user of the Defendant's Loyalty Program. Olivia May provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, May is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

103. Plaintiff Darrel Parris is a resident and citizen of the State of Missouri and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Darrel Parris provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a

breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Parris is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

104. Plaintiff Janlisa Parris is a resident and citizen of the State of Missouri and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Janlisa provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Parris is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

MONTANA

105. Plaintiff Holger Meyer is a resident and citizen of the State of Montana and a frequent user of the Defendant's Loyalty Program, having been a member for at least nineteen years. Holger Meyer provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Meyer is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

NEBRASKA

106. Plaintiff Carol Blood is a resident and citizen of the State of Nebraska and a frequent user of the Defendant's Loyalty Program. Carol Blood provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Carol Blood is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

107. Plaintiff Kathleen Christensen is a resident and citizen of the State of Nebraska and a frequent user of the Defendant's Loyalty Program. Kathleen Christensen provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Kathleen Christensen is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

108. Plaintiff Michelle Featherstone is a resident and citizen of the State of Nebraska and a frequent user of the Defendant's Loyalty Program. Michelle Featherstone provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant

provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Michelle Featherstone is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

109. Plaintiff Jack Milam is a resident and citizen of the State of Nebraska and a frequent user of the Defendant's Loyalty Program. Jack Milam provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Jack Milam is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for

NEVADA

110. Plaintiff Lisa Frederickson is a resident and citizen of the State of Nevada and a frequent user of the Defendant's Loyalty Program, having been a member for at least four months. Lisa Frederickson provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Frederickson is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

111. Plaintiff Joseph Throneberry is a resident and citizen of the State of Nevada and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Joseph Throneberry provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Throneberry is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

NEW HAMPSHIRE

112. Plaintiff Lucy Karl is a resident and citizen of the State of New Hampshire and a frequent user of the Defendant's Loyalty Program, having been a member for at least four years. Lucy Karl provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Karl is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

NEW JERSEY

113. Plaintiff Tamika Jackson is a resident and citizen of the State of New Jersey and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Tamika Jackson provided her Personal Information to the Defendant on the assumption

Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Jackson is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

114. Plaintiff Judy Mills is a resident and citizen of the State of New Jersey and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Judy Mills provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Mills is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

NEW MEXICO

115. Plaintiff Kris "Chris" Morris is a resident and citizen of the State of New Mexico and a frequent user of the Defendant's Loyalty Program, having been a member for at least eleven years. Kris "Chris" Morris provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Morris is taking measures that

he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

NEW YORK

116. Plaintiff Edward Baker is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Edward Baker provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Baker is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

117. Plaintiff Tanesha Boradgiak is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Tanesha Boradgiak provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Boradgiak is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

118. Plaintiff Crystal Chambers is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program. Crystal Chambers provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Chambers is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

119. Plaintiff Lisa Fritz is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Lisa Fritz provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Fritz is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

120. Plaintiff Laurene Gallway is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Laurene Gallway provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly

in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Gallway is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

121. Plaintiff Phyllis Hecker is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Phyllis Hecker provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Hecker is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

122. Plaintiff Jeffrey Rahn is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least seven years. Jeffrey Rahn provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Rahn is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts

are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

123. Plaintiff Anne Santo is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Anne Santo provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Santo is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

124. Plaintiff Anne Savarese is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Anna Savarese provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Savarese is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

125. Plaintiff Vincent Savarese is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Vincent Savarese provided his Personal Information to the Defendant on the assumption

Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Savarese is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

126. Plaintiff Curtis Weaver is a resident and citizen of the State of New York and a frequent user of the Defendant's Loyalty Program, having been a member for at least eight months. Curtis Weaver provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Weaver is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

NORTH CAROLINA

127. Plaintiff Yvette Butler is a resident and citizen of the State of North Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Yvette Butler provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was

compromised by the Data Breach. As a result of the Data Breach, Butler is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

128. Plaintiff Shelia Canipe is a resident and citizen of the State of North Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Shelia Canipe provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Canipe is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

129. Plaintiff Dorothy Davis is a resident and citizen of the State of North Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Dorothy Davis provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Davis is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

130. Plaintiff Mark Duffey is a resident and citizen of the State of North Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Mark Duffey provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Duffey is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

131. Plaintiff Linda Kite is a resident and citizen of the State of North Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty-eight years. Linda Kite provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Kite is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

132. Plaintiff Rick Sabath is a resident and citizen of the State of North Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Rick Sabath provided his Personal Information to the Defendant on the assumption that

Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Sabath is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised.

133. Plaintiff Debra Talley is a resident and citizen of the State of North Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Debra Talley provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Talley is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

NORTH DAKOTA

134. Plaintiff Eric Gault is a resident and citizen of the State of North Dakota and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Eric Gault provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. As a result of the Data Breach, Gault is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

OHIO

135. Plaintiff Brad Barringer is a resident and citizen of the State of Ohio and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Brad Barringer provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Barringer is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

136. Plaintiff Angela Gresh is a resident and citizen of the State of Ohio and a frequent user of the Defendant's Loyalty Program, having been a member for at least fourteen years. Angela Gresh provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Gresh is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

137. Plaintiff Chalise Morris is a resident and citizen of the State of Ohio and a frequent user of the Defendant's Loyalty Program, having been a member for at least three years. Chalise Morris provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure

that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Morris is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

138. Plaintiff David Moyer is a resident and citizen of the State of Ohio and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. David Moyer provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Moyer is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

139. Plaintiff Deidrinelle Rouse is a resident and citizen of the State of Ohio and a frequent user of the Defendant's Loyalty Program, having been a member for at least twelve years. Deidrinelle Rouse provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Rouse is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her

accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

140. Plaintiff Tamika Simmonds is a resident and citizen of the State of Ohio and a frequent user of the Defendant's Loyalty Program, having been a member for at least four years. Tamika Simmonds provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Simmonds is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

OKLAHOMA

141. Plaintiff Susan Mullins is a resident and citizen of the State of Oklahoma and a frequent user of the Defendant's Loyalty Program, having been a member for at least eighteen years. Susan Mullins provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Mullins is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

OREGON

142. Plaintiff Sami Difuntorum is a resident and citizen of the State of Oregon and a frequent user of the Defendant's Loyalty Program, having been a member for at least fifteen years. Sami Difuntorum provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Difuntorum is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

143. Plaintiff Steven Owens is a resident and citizen of the State of Oregon and a frequent user of the Defendant's Loyalty Program. Steven Owens provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Owens is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

PENNSYLVANIA

144. Plaintiff Cheryl Castor is a resident and citizen of the Commonwealth of Pennsylvania and a frequent user of the Defendant's Loyalty Program, having been a member for at least fourteen years. Cheryl Castor provided her Personal Information to the Defendant on the

assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Castor is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

145. Plaintiff Michael Castor is a resident and citizen of the Commonwealth of Pennsylvania and a frequent user of the Defendant's Loyalty Program, having been a member for at least fourteen years. Michael Castor provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Castor is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

146. Plaintiff Prudence Concert-White is a resident and citizen of the Commonwealth of Pennsylvania and a frequent user of the Defendant's Loyalty Program. Prudence Concert-White provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach.

As a result of the Data Breach, Concert-White is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

147. Plaintiff Shawn Seeley is a resident and citizen of the Commonwealth of Pennsylvania and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty years. Shawn Seeley provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Seeley is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

148. Plaintiff Melissa Yurkanin is a resident and citizen of the Commonwealth of Pennsylvania and a frequent user of the Defendant's Loyalty Program, having been a member for at least six months. Melissa Yurkanin provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Yurkanin is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

PUERTO RICO

149. Plaintiff Ricardo Vaquer is a resident and citizen of the Territory of Puerto Rico and a frequent user of the Defendant's Loyalty Program, having been a member for at least three months. Ricardo Vaquer provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Vaquer is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

RHODE ISLAND

150. Plaintiff Mary Ellen Davey is a resident and citizen of the State of Rhode Island and a frequent user of the Defendant's Loyalty Program, having been a member for at least five years. Mary Ellen Davey provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Davey is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

151. Plaintiff Christopher Pratt is a resident and citizen of the State of Rhode Island and a frequent user of the Defendant's Loyalty Program, having been a member for at least two

years. Christopher Pratt provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Pratt is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

SOUTH CAROLINA

152. Plaintiff Vance Edward Eichelberger is a resident and citizen of the State of South Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Vance Edward Eichelberger provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Eichelberger is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

153. Plaintiff Justin Palmer is a resident and citizen of the State of South Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Justin Palmer provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a

breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Palmer is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

154. Plaintiff David Secrist is a resident and citizen of the State of South Carolina and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. David Secrist provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Secrist is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

SOUTH DAKOTA

155. Plaintiff John Gilliland is a resident and citizen of the State of South Dakota and a frequent user of the Defendant's Loyalty Program, having been a member for at least eight years. John Gilliland provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Gilliland is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

156. Plaintiff Charles Hanson is a resident and citizen of the State of South Dakota and a frequent user of the Defendant's Loyalty Program, having been a member for at least nineteen years. Charles Hanson provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Hanson is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

TENNESSEE

157. Plaintiff Amanda Arnold is a resident and citizen of the State of Tennessee and a frequent user of the Defendant's Loyalty Program, having been a member for at least seven years. Amanda Arnold provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Arnold is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

158. Plaintiff Douglas Blake is a resident and citizen of the State of Tennessee and a frequent user of the Defendant's Loyalty Program, having been a member for at least eight years. Douglas Blake provided his Personal Information to the Defendant on the assumption Defendant

would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Blake is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

159. Plaintiff Carla Engle is a resident and citizen of the State of Tennessee and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Carla Engle provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Engle is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

160. Plaintiff Janice Frazier-Scott is a resident and citizen of the State of Tennessee and a frequent user of the Defendant's Loyalty Program, having been a member for at least six months. Janice Frazier-Scott provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Frazier-Scott is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and

that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

161. Plaintiff Betsy Gentry is a resident and citizen of the State of Tennessee and a frequent user of the Defendant's Loyalty Program, having been a member for at least thirteen years. Betsy Gentry provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Gentry is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

162. Plaintiff Janet Wender is a resident and citizen of the State of Tennessee and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Janet Wender provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Wender is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

163. Plaintiff Ronzella Wright-Loftly is a resident and citizen of the State of Tennessee and a frequent user of the Defendant's Loyalty Program, having been a member for at least four

years. Ronzella Wright-Loftly provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Wright-Loftly is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

TEXAS

164. Plaintiff Deana Cannon is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least sixteen years. Deana Cannon provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Cannon is taking measures that her otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

165. Plaintiff Kenneth Davis is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least eighteen years. Kenneth Davis provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly

in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Davis is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

166. Plaintiff Scott Gideon is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Scott Gideon provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Gideon is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

167. Plaintiff Jernard Griggs is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Jernard Griggs provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Griggs is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

168. Plaintiff Donna Hughes is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least ten years. Donna Hughes provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Hughes is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

169. Plaintiff Patricia Huizar is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least eleven years. Patricia Huizar provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Huizar is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

170. Plaintiff Selma Rodriguez is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. Selma Rodriguez provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security

measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Rodriguez is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

171. Plaintiff Bruce Sanders is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least seven years. Bruce Sanders provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Sanders is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

172. Plaintiff Beverly Tookey is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least eighteen years. Beverly Tookey provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Tookey is taking measures that

she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

173. Plaintiff John Waller is a resident and citizen of the State of Texas and a frequent user of the Defendant's Loyalty Program, having been a member for at least twenty-two years. John Waller provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Waller is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

UTAH

174. Plaintiff Jonathan Dodart is a resident and citizen of the State of Utah and a frequent user of the Defendant's Loyalty Program, having been a member for at least three years. Jonathan Dodart provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Dodart is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

175. Plaintiff Ruth Patricia Rosados is a resident and citizen of the State of Utah and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year. Ruth Patricia Rosados provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Rosados is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

VERMONT

176. Plaintiff Jeninne Pitts is a resident and citizen of the State of Vermont and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Jeninne Pitts provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Pitts is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

VIRGINIA

177. Plaintiff Ronald Kotz is a resident and citizen of the Commonwealth of Virginia and a frequent user of the Defendant's Loyalty Program, having been a member for at least thirteen years. Ronald Kotz provided his Personal Information to the Defendant on the

assumption that Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Kotz is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

178. Plaintiff David Melendez is a resident and citizen of the Commonwealth of Virginia and a frequent user of the Defendant's Loyalty Program, having been a member for at least six years. David Melendez provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Melendez is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

179. Plaintiff Asim Padh is a resident and citizen of the Commonwealth of Virginia and a frequent user of the Defendant's Loyalty Program, having been a member for at least two years. Asim Padh provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was

compromised by the Data Breach. As a result of the Data Breach, Padh is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

VIRGIN ISLANDS

180. Plaintiff Michael Raimondi is a resident and citizen of the Virgin Islands and a frequent user of the Defendant's Loyalty Program, having been a member for at least eighteen years. Michael Raimondi provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Raimondi is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

WASHINGTON

181. Plaintiff Christopher Davies is a resident and citizen of the State of Washington and a frequent user of the Defendant's Loyalty Program, having been a member for at least seven years. Christopher Davies provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Davies is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts

are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

182. Plaintiff Rik Lewis is a resident and citizen of the State of Washington and a frequent user of the Defendant's Loyalty Program. Rik Lewis provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Lewis is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

183. Plaintiff Christina Olsen is a resident and citizen of the State of Washington and a frequent user of the Defendant's Loyalty Program, having been a member for at least fifteen years. Christina Olsen provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Olsen is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

184. Plaintiff John Simmons is a resident and citizen of the State of Washington and a frequent user of the Defendant's Loyalty Program, having been a member for at least one year.

John Simmons provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Simmons is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

185. Plaintiff Jody Stephens is a resident and citizen of the State of Washington and a frequent user of the Defendant's Loyalty Program, having been a member for at least nine years. Jody Stephens provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Stephens is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

186. Plaintiff Gordon Thomas is a resident and citizen of the State of Washington and a frequent user of the Defendant's Loyalty Program, having been a member for at least eighteen years. Gordon Thomas provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Thomas is taking measures

that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

WEST VIRGINIA

187. Plaintiff Brenda Burr is a resident and citizen of the State of West Virginia and a frequent user of the Defendant's Loyalty Program, having been a member for at least seven years. Brenda Burr provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Burr is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

188. Plaintiff Sarah Korwan is a resident and citizen of the State of West Virginia and a frequent user of the Defendant's Loyalty Program, having been a member for at least seventeen years. Sarah Korwan provided her Personal Information to the Defendant on the assumption Defendant would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. Defendant provided her email notice that her information was compromised by the Data Breach. As a result of the Data Breach, Korwan is taking measures that she otherwise would not have to take to ensure that her identity is not stolen and that her accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

WISCONSIN

189. Plaintiff Jeffrey Oelhafen is a resident and citizen of the State of Wisconsin and a frequent user of the Defendant's Loyalty Program, having been a member for at least eighteen years. Jeffrey Oelhafen provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Oelhafen is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

WYOMING

190. Plaintiff Kent Spence is a resident and citizen of the State of Wyoming and a frequent user of the Defendant's Loyalty Program. Kent Spence provided his Personal Information to the Defendant on the assumption Defendant would keep his information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Defendant provided him email notice that his information was compromised by the Data Breach. As a result of the Data Breach, Kent Spence is taking measures that he otherwise would not have to take to ensure that his identity is not stolen and that his accounts are not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

DEFENDANT AND ITS RELEVANT CORPORATE STRUCTURE

191. Defendant Marriott is a Delaware corporation, with its principal place of business in Bethesda, Maryland. Marriott is subject to the jurisdiction of this Court and may be served

with process through its registered agent, The Corporation Trust Incorporated, 2405 York Road, Suite 201, Lutherville-Timonium, Maryland 21093.

192. Marriott primarily derives its revenues from hotel and restaurant operations.

193. Starwood is now a wholly-owned subsidiary of Defendant Marriott.

STATEMENT OF FACTS

A. Marriott Gathers Massive Amounts of Personal Information From Its Guests.

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

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

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

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

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

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

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

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

[3] Tsang Article, *supra* n.1.

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

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

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

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

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

In more limited circumstances, we also may collect:

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

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

[4] Marriot Group Global Privacy Statement, https://www.marriott.com/about/privacy.mi (last accessed Nov. 30, 2018).

199. Marriott stores massive amounts of Personal Information on its servers and utilizes this Personal Information to maximize its profits through predictive marketing and other marketing techniques.

200. Consumers place value on data privacy and security, and they consider it when making decisions on where to stay for travel. Plaintiffs would not have stayed at the Starwood hotels nor would they have used their debit or credit cards to pay for their Starwood stays had they known that Marriott does not take all necessary precautions to secure the personal and financial data given to it by consumers. Alternatively, Plaintiffs would have paid less for their rooms than they did. Inherent in the price of every one of Marriott's hotel rooms is a portion for data security.

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

202. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

B. Defendant Takes Four Years to Discover the Data Breach and Delays Informing Impacted Customers.

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

[5] Incident Website, *supra* n.2.

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

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

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

207. Marriott has confirmed that hundreds of millions of guests who made a reservation at a Starwood property since 2014 may have been impacted.[9]

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

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

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

211. According to Gus Hosein, executive director of Privacy International, "It's astonishing how long it took them to discover they were breached. For four years, data was being pilfered out of the company and they didn't notice. They can say all they want that they take

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] Tsang Article, *supra* n.1.

[10] *Id.*

security seriously, but they don't if you can be hacked over a four-year period without noticing."[11]

212. Marriott has recently disclosed that after deduplication efforts, it now appears that approximately 383 million guest records were stolen, including 5.25 million unencrypted passport numbers, 20.3 million encrypted passport number, and 8.6 million credit and debit cards, making this the largest data breach in US history.[12] Marriott further concedes that it has no idea who carried out the breach.

213. Marriott could not answer why so many of its passport numbers were unencrypted. Asked how Marriott was handling the information now that it has merged Starwood's data into the Marriott reservations system — a merger that was just completed at the end of 2018 — Connie Kim, a company spokeswoman, said: "We are looking into our ability to move to universal encryption of passport numbers and will be working with our systems vendors to better understand their capabilities, as well as reviewing applicable national and local regulations."[13]

214. While Marriott has said it would pay for a new passport for anyone whose passport information, hacked from their systems, was found to be involved in a fraud, according to *The New York Times*, that was a "corporate sleight of hand," since it has provided no coverage for guests who wanted a new passport simply because their data had been taken.[14]

---

[11] *Id*.

[12] *Id.*

[12] *Id.*, *Marriott Concedes 5 Million Passport Numbers Lost to Hackers Were Not Encrypted*, The New York Times (Jan. 4, 2019), *available at* https://www.nytimes.com/2019/01/04/us/politics/marriott-hack-passports.html.

[13] *Id.*

[14] *Id.*

C. The Stolen Personal Information is Valuable to Hackers and Thieves.

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

216. In fact, in August of this year, the U.S. Department of Justice indicted members of an Eastern European cybercrime ring called Fin7, which targeted, *inter alia*, hotel chains.[15]

217. According to Richard Gold, head of security engineering at the cybersecurity firm Digital Shadows, "hotels are an attractive target for hackers because they hold a lot of sensitive information, including credit card and passport details, but often don't have security standards as tough as those of more regulated industries, like banking."[16]

218. Mr. Gold put this breach "among the largest of consumer data, on par with breaches at Yahoo and the credit-storing giant, Equifax."[17]

[15] Tang Article, *supra* n1.

[16] *Id*.

[17] *Id*.

219. Legitimate organizations and the criminal underground alike recognize the value of PII otherwise, they wouldn't aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[18] Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

220. Biographical data is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[19] PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of theft and unauthorized access have been the subject of many media reports. One form of identity theft, branded "synthetic identity theft," occurs when thieves create new identities by combining real and fake identifying information then using those identities to open new accounts. "This is where they'll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of a bionic person," said Adam Levin, Chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft, experts said: "It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person." In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

221. Unfortunately, and as alleged below, despite all this publicly available knowledge of the continued compromises of PII in the hands of third parties, such as hoteliers, Marriott's

[18] Verizon 2014 PCI Compliance Report, *available at* http://www.nocash.info.ro/wp-content/uploads/2014/02/ Verizon_pci-report-2014.pdf ("2014 Verizon Report"), at 54 (last visited Sept. 24, 2014).

[19] *Id.*

approach at maintaining the privacy of Plaintiffs' and Class Members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

D. Marriott Failed to Segregate PCD from PII.

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

223. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data."[20]

224. One PCI DSS requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code. "Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement."[21] However, segregation is recommended because, among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data."[22]

225. Illicitly obtained PII and PCD, sometimes aggregated from different data breaches, are sold on the black market, including on websites, as products at a set price.[23]

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

---

[20] PCI Security Standards Council, Payment Card Industry Data Security Standard 2.0 ("PCI Version 2") at 5.

[21] *Id*. at 10.

[22] *See* Verizon Report at 54.

[23] *See, e.g.*, Brian Krebs, *How Much Is Your Identity Worth?*, Krebs on Security (Nov. 8, 2011), https://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/.

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

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

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

230. In this regard, more than likely the software used in the attack was a variant of "BlackPOS," a malware strain designed to siphon data from cards when they are swiped at infected point-of-sale systems. Hackers previously utilized BlackPOS in other recent cyber-attacks, including breaches at Home Depot and Target. While many retailers, banks, and card companies have responded to these recent breaches by adopting technology and security practices that help make transactions and stored data more secure, Marriott has acknowledged that it did not do so.

231. According to a former senior executive at Starwood, his hypothesis is that the most probable cause of the breach was the technology platform deployed by Starwood under the name "Valhalla."[24] The Valhalla system was fully activated at Starwood in 2009. Following standard architectures, the Starwood system consisted of multiple databases and sub-systems.

[24] Israel del Rio, *I was a senior VP of technology at Starwood - here's my take on the guest data breach*, PhocusWire (Dec. 20, 2018), *available at*: https://www.phocuswire.com/Marriott-data-breach-ex-Starwood-perspective

Among the databases are the SPG System with its SPG members database, the actual reservation system where active bookings are kept, and a Data Warehouse used for analytical and marketing purposes.[25] Soon after Marriott took control of Starwood, the Starwood Data Warehouse began to migrate to Marriott as Marriott wanted access to the wealth of Starwood guest data as soon as possible for its own marketing purposes.[26]

232. According to the former Starwood senior executive, because the Data Warehouse contained the booking records for several prior years, (and it could contain nearly 400 million, and upwards to 500 million records), this is most likely the area from which the data was stolen. However, given that some of that data had already been migrated to Marriott, it is hard to say for certain whether the breach occurred in the Starwood system, the Marriott system, or in transit as a result of exposure during the Extract-Transform-Load process used during the migration. Because the Data Warehouse contains booking data going back several years, the Data Warehouse data could have been exposed recently and still show stolen records from 2014.[27]

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

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

234. The ramifications of Marriott's failure to keep Plaintiffs' and Class Members' data secure are severe and have already manifested themselves—as evidenced by the harm suffered by the named Plaintiffs in this lawsuit.

---

[25] *Id.*

[26] *Id.*

[27] *Id.*

235. The information Marriott compromised, including Plaintiffs' identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[28] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration date, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account [as occurred to Plaintiffs here], run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[29]

236. According to Javelin Strategy and Research, "1 in 4 [breach] notification recipients became a victim of identity fraud."[30] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

237. 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 or obtaining a driver's license or identification card in the victim's name but with another's picture. Some of this activity may not come to light for years. The IRS paid out $43.6 billion in potentially fraudulent returns in 2012, and the IRS identified more than 2.9

[28] FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf (last visited Sept. 24, 2014).
[29] FTC, Signs of Identity Theft, *available at* http://www.consumer.ftc.gov/articles/ 0271- signs-identity-theft (last visited Nov. 30, 2018).

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

million incidents of identity theft in 2013. The IRS has described identity theft as the number one tax scam for 2014.

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

239. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had Personal Information used for fraudulent purposes, 29% spent a month or more resolving problems."[31] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."[32]

F. Annual Monetary Losses From Identity Theft are in the Billions of Dollars.

240. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[33]

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information

[31] Victims of Identity Theft, 2012 at 10 (Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.
[32] *Id*. at 11.
[33] *See* 2013 Identity Fraud Report.

> 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.[34]

242. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

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

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

244. Further, the one year of free enrollment in Web Watcher offered by Marriott only applies to guests who live in the United States, Canada, and Britain and is not a credit monitoring service. Web Watcher merely "keeps an eye on internet sites where thieves swap and sell Personal Information and then alerts people if anyone is selling their information."[35]

245. Marriott appears to misapprehend how the sale of stolen data works. Many sales of stolen data occur on the Deep Web. The Deep Web is not Google. While the internet, as most people know it, contains at least 4.5 billion websites indexed by search engines, the Deep Web is

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

[35] Tsang Article, *supra* n.1

400 to 500 times larger, according to estimates, and is not indexed.[36] Web Watchers' service may detect some sales on the Deep Web, but cannot alone identify and prevent identity theft. Many sales are done in private through membership only forums and private chat services.

246. Moreover, data thieves are aware of the one-year expiration period associated with Marriott's offer. As explained herein, thieves will often wait years to purchase and use stolen data, waiting for the clock to run out on the offered monitoring services.[37]

247. Finally, the rollout of signup for the monitoring service confused many customers, who complained that the user interface was unclear.[38]

H. Plaintiffs and Class Members Suffered Damages.

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

249. Plaintiffs' and Class members' PII is private and sensitive in nature and was left inadequately protected by Marriott. Marriott did not obtain Plaintiffs' and Class Members'

[36] Mae Rice, *The Deep Web Is the 99% of the Internet You Can't Google*, Curiousity (May 22, 2018), *available at* https://curiosity.com/topics/the-deep-web-is-the-99-of-the-internet-you-cant-google-curiosity/.

[37] *See, e.g.*, Matt Tatham, *A Year After the Marriott Breach: Are You Protecting Your Data?* (Sept. 24, 2018), *available at* https://www.experian.com/blogs/ask-experian/a-year-after-the-Marriott-breach-are-you-protecting-your-data/.

[38] Tsang Article, *supra* n.1.

consent to disclose their PII to any other person as required by applicable law and industry standards.

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

251. Marriott's "deep[] regret [for] this incident" is no comfort to Plaintiffs and Class Members, though undoubtedly they agree that Marriott "fell short of what [its] guest deserve . . ."[39]

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

a. theft of their personal and financial information;

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

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

[39] *Id*.

d. the improper disclosure of their Personal Information;

e. loss of privacy;

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

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

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

i. deprivation of rights they possess under the various statutes.

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

CLASS ACTION ALLEGATIONS

254. Pursuant to Fed. R. Civ. P. 23 (a) and (b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> **All persons in the United States whose Personal Information was compromised in the Marriott Data Breach.**

255. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims brought

under either Maryland or Connecticut common law, as well as statutory claims under state data breach statutes and consumer protection statutes, on behalf of separate statewide subclasses for each State and Territory in the United States.

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

257. **Numerosity. Fed. R. Civ. P. 23(a)(1).** The members of the Classes are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, Marriott has acknowledged that information—including PII and PCD—of hundreds of millions of customers has been compromised. All members of the proposed Classes are readily ascertainable. Marriott has access to contact information for millions of members of the Classes, which can be used for providing notice to most Class members. Indeed, Marriott has already provided notice to the Class members who were likely impacted by the Data Breach.

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

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

b. Whether Marriott violated state data breach laws by failing to promptly notify class members their Personal Information had been compromised;

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

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

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

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

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

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

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

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

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

261. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2)**. The prosecution of separate actions by individual Class members would create a risk of

inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Marriott. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and otherwise impair their interests. Marriott has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

262. **Superiority of Class Action. Fed. R. Civ. P. 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through class actions will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action. Damages for any individual Class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Marriott's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

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

CHOICE OF LAW FOR NATIONWIDE CLAIMS

264. The state laws of one state will likely govern Plaintiffs' claims.

265. First, the principal place of business of Marriott, located in Bethesda, Maryland, is the "nerve center" of its business activities—the place where its high-level officers direct,

control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

266. Alternatively, the former principal place of business of Starwood, Stamford, Connecticut, was the center of operations of Starwood and its SPG Loyalty Program, in which much or all of the Personal Information that was compromised in the Data Breach was housed.

267. Both Maryland and Connecticut have significant interests in regulating the conduct of businesses operating within their borders. Those states, which seek to protect the rights and interests of residents and citizens of the United States against a company headquartered and doing business in those states, have a greater interest in the nationwide claims of Plaintiffs and Class members than any other state and are most intimately concerned with the claims and outcome of this litigation.

268. Marriott's response to the data breach at issue here, and corporate decisions surrounding such response, were made from and in Maryland.

269. Marriott's breaches of duty to Plaintiffs and Nationwide Class members emanated from both Connecticut and Maryland.

270. Additional factual analysis is necessary in order to determine which state's law should apply to the claims of the Class members. Accordingly, it would be inappropriate to determine choice of law at the pleadings stage of this case. Plaintiffs are therefore pleading nationwide claims based upon Maryland and Connecticut law in the alternative (or, under the law of the states of each Plaintiff).

271. Application of either Maryland or Connecticut law Class with respect to Plaintiffs' and Class members' claims after the completion of a factual inquiry would be neither

arbitrary nor fundamentally unfair because those states have significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Class.

272. Under choice of law principles, applicable to this action, the common law of one of the states—Maryland or Connecticut—would apply to the nationwide common law claims of all Class members by virtue of a choice of law provision in the Loyalty Program terms and conditions, or a substantive analysis concerning which state's laws should govern, given that the data compromised was part of the SPG database, which was previously not subject to those terms and conditions. Additionally, given Maryland's and Connecticut's significant interest in regulating the conduct of businesses operating within their borders, consumer protection laws may be applied to non-resident consumer plaintiffs upon completion of the factual analysis required for the choice of law determination.

273. To the extent the Court finds that the laws of each Class member's state apply to his or her injuries, Plaintiffs previously provided Marriott with notice sufficient to satisfy state statutory requirements, and sent correspondence to Marriott's counsel on January 8, 2019, providing the company with additional information on Plaintiffs' claim.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

1. Plaintiffs repeat and reallege Paragraphs 1-275, as if fully alleged herein.

2. Marriott owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized

persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing security systems to ensure that Plaintiffs' and Class members' Personal Information in Marriott's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system 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 security measures consistent with industry standards.

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

4. Defendant breached its duty to notify Plaintiffs and Class Members of the unauthorized access by failing to notify Plaintiffs and Class Members of the Data Breach until November 30, 2018. To date, although it has been months since the Data Breach was discovered, and four years since the Data Breach commenced, Defendant has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

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

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

7. Further, through Defendant's failure to provide timely and clear notification of the Data Breach to consumers, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data, bank accounts, and other accounts where PII or PCI could be used for fraudulent purposes.

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

9. Defendant's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive Personal Information violated its duty to protect that data and prevent its dissemination to third parties.

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

11. Marriott's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Marriott. Various FTC publications and data security breach orders further form the basis of Marriott's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty to use reasonable measures to protect Personal Information.

12. Defendant acknowledged the importance of keeping Personal Information secure, and stated that it sought "to use reasonable organizational, technical and administrative measures to protect Personal Data."[40] Despite acknowledging its responsibility to keep this information secure, Defendant improperly put the burden on Plaintiffs and Class Members to notify Defendant if they suspected that their Personal Information was not secure, when individuals would not have access to this information, and Defendant was in a superior position to know this information, and was in the exclusive possession of such information.[41]

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

14. Defendant's failure to take proper security measures to protect Plaintiffs' and Class Members' Personal Information has caused Plaintiffs and Class Members to suffer injury and damages. As described herein, the Plaintiffs received notice that their Personal Information was compromised, and now must take and have taken affirmative steps to ensure that their

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

[41] *Id*.

identity is not stolen and their financial information is not compromised. Furthermore, as a result of the Data Breach, Plaintiff did not get what Plaintiff bargained for.

15. Marriott also had a duty to safeguard the Personal Information of Plaintiffs and Class members and to promptly notify them of a breach because of state laws and statutes that require Marriott to reasonably safeguard sensitive Personal Information, as detailed herein.

16. 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, 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, replace their passports, and take other steps to mitigate or ameliorate the damages caused by Marriott's misconduct.

17. 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 Personal Information of Plaintiffs and Class members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiffs' and the Class members' Personal Information in Marriott's possession had been or was reasonably believed to have been, stolen or compromised.

18. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their Personal Information would not have been compromised.

19. As a direct and proximate result of Marriott's negligence, Plaintiffs and Class members have been injured as described herein, and are entitled to damages, including

compensatory, punitive, and nominal damages, in an amount to be proven at trial. Plaintiffs' and Class members' injuries include:

a. theft of their Personal Information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

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

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Marriott Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts, and replacing passports;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals;

i. damages to and diminution in value of their Personal Information entrusted, directly or indirectly, to Marriott with the mutual understanding that Marriott would safeguard Plaintiffs' and Class members' Personal Information against theft and not allow access and misuse of their Personal Information by others;

j. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Marriott's possession and is subject to further breaches so long as Marriott fails to undertake appropriate and adequate measures to protect Plaintiffs' Personal Information; and

k. overpayment of Defendant's services because Plaintiff and Class members did not get the implicit protection of their Personal Information that they bargained for.

COUNT 2

NEGLIGENCE *PER SE*

ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFFS AND THE STATEWIDE SUBCLASSES

20. Plaintiffs repeat and reallege Paragraphs 1-275, as if fully alleged herein.

21. Marriott owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing security systems to ensure that Plaintiffs' and Class members' Personal Information in Marriott's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system 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 security measures consistent with industry standards.

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

23. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Marriott had a duty to provide fair and adequate data security practices to safeguard Plaintiffs' and Class members' Personal Information.

24. Pursuant to state laws as alleged herein, Marriott had a duty to those respective states' Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class members' Personal Information.

25. Marriott breached its duties to the Plaintiffs and Class members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiffs' and Class members' Personal Information.

26. Marriott's failure to comply with applicable laws and regulations constitutes negligence *per se*.

27. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

28. The injury and harm suffered by Plaintiffs and the Class members was the reasonably foreseeable result of Marriott's breach of its duties. Marriott knew or should have known that it was failing to meet its duties, and that the breach would cause Plaintiffs and Class members to experience the foreseeable harms associated with exposure of their Personal Information.

29. As a direct and proximate result of Marriott's negligent conduct, Plaintiffs and Class members suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT 3

BREACH OF IMPLIED CONTRACT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

30. Plaintiffs repeat and reallege Paragraphs 1-275, as if fully alleged herein.

31. Marriott solicited and invited Plaintiffs and members of the Class to make reservations at Starwood properties. Plaintiffs and Class members accepted Marriott's offers and made such reservations with Marriott.

32. When Plaintiffs and Class members made reservations with Marriott, they were required to—and did—provide their Personal Information to Marriott. In so doing, Plaintiffs and

Class members entered into implied contracts with Marriott pursuant to which Marriott agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members if their data had been breached or compromised.

33. Each reservation by Plaintiffs and Class members was made pursuant to mutually agreed-upon implied contracts with Marriott under which Marriott agreed to safeguard and protect Plaintiffs' and Class members' Personal Information and to provide accurate and timely notice if such information was compromised, lost, or stolen.

34. Plaintiffs and Class members would not have provided their Personal Information to Marriott in the absence of such an implied contract.

35. Plaintiffs and Class members fully performed their obligations under the implied contracts with Marriott.

36. Marriott breached the implied contracts it made with the Plaintiffs and Class members by failing to safeguard or protect the Class members' Personal Information and by failing to provide accurate and timely notice when their Personal Information was compromised.

37. As a direct and proximate result of Marriott's breaches of the implied contracts between Marriott and Plaintiffs and Class members, Plaintiffs and the Class members sustained actual losses and damages as described herein, and paid more than they would have paid for Marriott's services.

COUNT 4

BREACH OF THE DUTY OF GOOD FAITH AND FAIR DEALING

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

38. Plaintiffs repeat and reallege Paragraphs 1-275, as if fully alleged herein.

39. Common law implies a covenant of good faith and fair dealing in every contract.

40. Plaintiffs and Class members contracted with Marriott by accepting Marriott's offers to stay at one or more Starwood hotels.

41. Plaintiffs and Class members performed all of the duties and obligations required under their agreements with Marriott.

42. Conditions required for Marriott's performance under its contracts with Plaintiffs' and Class members have occurred.

43. Marriott did not provide, unfairly interfered with, or frustrated the right of Plaintiffs and Class members to receive the full benefits under their agreements with Marriott.

44. Plaintiffs and Class members were damaged by Marriott's breach in that they paid for, but did not receive, the valuable security protections to which they were entitled under the contracts with Marriott, which would have made Marriott's services more valuable.

COUNT 5

BAILMENT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

45. Plaintiffs repeat and reallege Paragraphs 1-275, as if fully alleged herein.

46. Plaintiffs and Class members provided, or authorized disclosure of, their Personal Information to Marriott for the exclusive purpose of booking hotel reservations.

47. In providing their Personal Information to Marriott, Plaintiffs and Class Members intended and understood that Marriott would adequately safeguard that information.

48. Marriott accepted possession of Plaintiffs' and Class members' Personal Information for the purpose of making Marriott's services available to Plaintiffs and Class members.

49. By accepting possession of Plaintiffs' and Class members' Personal Information, Marriott understood that Plaintiffs and Class members expected Marriott to adequately safeguard that information. Accordingly, a bailment was established for the mutual benefit of the parties. During the bailment, Marriott owed a duty to Plaintiffs and Class members to exercise reasonable care, diligence, and prudence in protecting their Personal Information.

50. Marriott breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' Personal Information, resulting in the unauthorized access to and misuse of Plaintiffs' and Class members' information.

51. Marriott further breached its duty to safeguard Plaintiffs' and Class members' Personal Information by failing to timely and accurately discover the breach and by failing to timely and accurately notify Plaintiffs and Class members that their information had been compromised as a result of the Data Breach.

52. As a direct and proximate result of Marriott's breach of its duty, Plaintiffs and Class members suffered damages that were reasonably foreseeable to Marriott.

53. As a direct and proximate result of Marriott's breach of its duty, Plaintiffs' and Class members' Personal Information that they entrusted to Marriott during the bailment was damaged and its value diminished.

COUNT 6

MARYLAND PERSONAL INFORMATION PROTECTION ACT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Maryland Subclass

54. Plaintiffs repeat and reallege Paragraphs 1-275, as if fully alleged herein.

55. This count is subject to the Court's analysis under applicable choice of law principles.

56. Included in the terms and conditions of the Loyalty Program is a Choice of Law and Venue Provision that provides that Maryland law applies to the Loyalty Program. Whether that Choice of Law and Venue Provision applies to the Class is a question of fact inappropriate for resolution at the pleading stage.

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

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

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

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

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

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

63. Under Md. Comm. Code § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a

reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach."

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

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

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

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

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

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

COUNT 7

**MARYLAND CONSUMER PROTECTION ACT,
MD. COMM. CODE §§ 13-301, *ET SEQ.*
AND APPLICABLE STATE CONSUMER PROTECTION ACTS AND UNFAIR**

BUSINESS PRACTICES ACTS

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively on Behalf of Plaintiffs and the Statewide Subclasses

70. Plaintiffs repeat and reallege Paragraphs 1-275, as if fully alleged herein.

71. This count is subject to the Court's analysis under applicable choice of law principles.

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

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

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

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

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

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

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

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

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

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

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

d. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

80. Defendant engaged in these False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers by:;

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

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information , including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Data Breach;

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

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

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

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

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

83. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been required to implement and adopt reasonable data security measures to comply with its legal obligations. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and class members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

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

85. Defendant also violated other statutory claims as described herein, making its conduct unlawful.

86. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

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

COUNT 8

MARYLAND PERSONAL INFORMATION PROTECTION ACT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Maryland Subclass

88. Plaintiffs repeat and reallege Paragraphs 1-275, as if fully alleged herein.

89. Included in the terms and conditions of the Loyalty Program is a Choice of Law and Venue Provision that provides that Maryland law applies to the Loyalty Program. Whether that Choice of Law and Venue Provision applies to the Class is a question of fact inappropriate for resolution at the pleading stage. Accordingly, this count is subject to the Court's analysis under applicable choice of law principles.

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

91. Marriott is a business that owns or licenses computerized data that includes personal information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

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

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

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

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

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

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

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

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

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

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

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

COUNT 9

BREACH OF SECURITY REGARDING COMPUTERIZED DATA,

C.G.S.A. § 36a-701b

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Connecticut Subclass

103. The Connecticut Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nationwide Class, or in the alternative on behalf of the Connecticut Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

104. As discussed herein, this count is subject to the Court's analysis under applicable choice of law principles.

105. Marriott is a business that conducts business in Connecticut and owns, licenses, and maintains computerized data that includes personal information as covered by C.G.S.A. § 36a-701b(b). Marriott also maintains computerized data that includes personal information that it does not own as covered by C.G.S.A. § 36a-701b(c).

106. Plaintiff and Connecticut Subclass members' Personal Information includes that which is covered by C.G.S.A. § 36a-701b(a).

107. Marriott is required to accurately notify Plaintiff and Connecticut Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay, not to exceed ninety days after discovery of the breach under C.G.S.A. § 36a-701b(b).

108. Marriott is required to immediately notify Plaintiff and Connecticut Subclass members if it becomes aware of a breach of its data security system which may have compromised Personal Information that Marriott stores but that Plaintiff and Connecticut Class members own under C.G.S.A. § 36a-701b(c).

109. Because Marriott was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by C.G.S.A. §§ 36a-701b(b) and (c).

110. By failing to disclose the Marriott Data Breach in an accurate and timely manner, Marriott failed to comply with C.G.S.A. §§ 36a-701b(b) and (c). Pursuant to C.G.S.A. § 36a-701b(g), Marriott's failure to comply was an unfair trade practice under the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110a, *et seq.*

111. As a direct and proximate result of Marriott's violations of C.G.S.A. §§ 36a-701b(b) and (c), Plaintiff and Connecticut Subclass members suffered damages, as described above.

112. Plaintiff and Connecticut Subclass members seek relief under C.G.S.A. § 42-110g for the harm they suffered because of Marriott's violations of C.G.S.A. §§ 36a-701b(b) and (c), including actual damages and equitable relief.

COUNT 10

CONNECTICUT UNFAIR TRADE PRACTICES ACT,

C.G.S.A. § 42-110G

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Connecticut Subclass

113. The Connecticut Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nationwide Class, or in the alternative on behalf of the Connecticut Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

114. As discussed herein, this count is subject to the Court's analysis under applicable choice of law principles.

115. Marriott is a "person" as defined by C.G.S.A. § 42-110a(3).

116. Marriott is engaged in "trade" or "commerce" as those terms are defined by C.G.S.A. § 42-110a(4).

117. At the time of filing this Complaint, Plaintiff has sent notice to the Attorney General and Commissioner of Consumer Protection pursuant to C.G.S.A. § 42-110g(c). Plaintiff will provide a file-stamped copy of the Complaint to the Attorney General and Commissioner of Consumer Protection.

118. Marriott advertised, offered, or sold services in Connecticut, and engaged in trade or commerce directly or indirectly affecting the people of Connecticut.

119. Marriott engaged in deceptive acts and practices and unfair acts and practices in the conduct of trade or commerce, in violation of the C.G.S.A. § 42-110b, including:

a. Representing that services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

b. Representing that services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

120. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers.

121. Marriott intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

122. Had Marriott disclosed to Plaintiff and Class members that it misrepresented the security utilized on its networks, or otherwise had not omitted to Plaintiff and Class members that its systems were insecure, Marriott would not have been able to continue storing Plaintiff and Class members' Personal Information on its networks, and would have been forced to disclose the material information regarding security. Instead, Marriott and its predecessors allowed its servers to be hacked—undetected—over the course of four years, failed to discover that its servers were vulnerable through adequate due diligence and testing, and yet still continued to store customers' Personal Information in its databases.

123. Marriott's unlawful, deceptive, and unconscionable acts include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information.

124. Marriott's conduct is intentional, knowing, and malicious because it knew or was reckless in not knowing the value of consumers' personal information, that databases containing such information were targets for hackers, and yet still did nothing to appropriately segregate data or otherwise secure the database from hacking.

125. As a direct and proximate result of Marriott's deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from identity theft, fraudulent charges, and time and money spent on preventative and corrective measures.

126. Marriott's deceptive acts and practices caused substantial, ascertainable injury to Plaintiff and Class members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

127. Marriott's violations of Connecticut law were done with reckless indifference to the Plaintiff and the Class or was with an intentional or wanton violation of those rights.

128. Plaintiff requests damages in the amount to be determined at trial, including statutory and common law damages, attorneys' fees, and punitive damage.

CLAIMS ON BEHALF OF INDIVIDUAL STATE SUBCLASSES

129. Although Marriott has been on notice of its unlawful, unfair, and deceptive practices since at least the filing of the first lawsuit related to the Data Breach in November 2018, and additional notice may very well be an exercise in futility, Plaintiffs provided Marriott with additional notice pursuant to applicable state statutes on January 8, 2019. It is Plaintiffs' intent that, after the expiration of applicable statutory periods, if Marriott does not provide sufficient compensation or remediation, or otherwise cease its unlawful, unfair, and deceptive practices, Plaintiffs will amend their complaint to include additional state consumer protection statutes.

CLAIMS ON BEHALF OF THE ALASKA SUBCLASS

COUNT 11

PERSONAL INFORMATION PROTECTION ACT,

Alaska Stat. §§ 45.48.010, *et seq.*

130. The Alaska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

131. Marriott is a business that owns or licenses Personal Information as defined by Alaska Stat. § 45.48.090(7). As such a business, it is a Covered Person as defined in Alaska Stat. § 45.48.010(a).

132. Plaintiff and Alaska Subclass members' Personal Information includes that which is covered under Alaska Stat. § 45.48.010(a).

133. Marriott is required to accurately notify Plaintiff and Alaska Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Alaska Stat. § 45.48.010(b).

134. Marriott is similarly required to determine the scope of the breach and restore the reasonable integrity of the information system under Alaska Stat. § 45.48.010(b).

135. Because Marriott was aware of a breach of its security system, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Alaska Stat. § 45.48.010(b).

136. By failing to disclose the Marriott Data Breach in a timely and accurate manner Marriott violated Alaska Stat. § 45.48.010(b).

137. Pursuant to Alaska Stat. § 45.48.080(b), a violation of Alaska Stat. § 45.48.010(b) is an unfair or deceptive act or practice under the Alaska Consumer Protection Act.

138. As a direct and proximate result of Marriott's violations of Alaska Stat. § 45.48.010(b), Plaintiff and Alaska Subclass members suffered damages, as described above.

139. Plaintiff and Alaska Subclass members seek relief measured as the greater of (a) each unlawful act, (b) three times actual damages in an amount to be determined at trial, or (c) statutory damages in the amount of $500 for Plaintiff and each Alaska Subclass Member;

reasonable attorneys' fees; and any other just and proper relief available under Alaska Stat. § 45.48.080(b)(2) and Alaska Stat. § 45.50.531.

COUNT 12

ALASKA CONSUMER PROTECTION ACT,

Alaska Stat. §§ 45.50.471, *et seq.*

140. The Alaska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

141. Marriott advertised, offered, or sold goods or services in Alaska and engaged in trade or commerce directly or indirectly affecting the people of Alaska.

142. Alaska Subclass members are "consumers" as defined by Alaska Stat. § 45.50.561(4).

143. Marriott engaged in unfair or deceptive acts and practices in the conduct of trade or commerce, in violation Alaska Stat. § 45.50.471, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, when they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in any other conduct creating a likelihood of confusion or of misunderstanding and which misleads, deceives, or damages a buyer in connection with the sale or advertisements of its goods or services; and

e. Using or employing deception, fraud, false pretense, false promise, misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that others rely upon the concealment, suppression, or omission in connection with the sale or advertisement of its goods or services whether or not a person was in fact misled, deceived, or damaged.

144. Marriott's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Alaska Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Alaska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alaska Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

146. Marriott intended to mislead Plaintiff and Alaska Subclass members and induce them to rely on its misrepresentations and omissions.

147. Marriott acted intentionally, knowingly, and maliciously to violate Alaska's Consumer Protection Act, and recklessly disregarded Plaintiff and Alaska Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

148. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and Alaska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more than they would have paid for Marriott's services had they known of Defendant's inadequate security measures.

149. Plaintiff and the Alaska Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) three times their actual damages or (b) statutory damages in the amount of $500; punitive damages; reasonable attorneys' fees and costs; and any other relief that is necessary and proper. Plaintiff will amend this complaint to seek injunctive relief after providing adequate notice to Marriott.

CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS

COUNT 13

ARIZONA CONSUMER FRAUD ACT,

A.R.S. §§ 44-1521, *et seq.*

150. The Arizona Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arizona Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

151. Marriott is a "person" as defined by A.R.S. § 44-1521(6).

152. Marriott advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

153. Marriott engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arizona Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arizona Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arizona Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

155. Marriott intended to mislead Plaintiff and Arizona Subclass members and induce them to rely on its misrepresentations and omissions.

156. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

157. Marriott acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff and Arizona Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

158. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and Arizona Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

159. Plaintiff and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS

COUNT 14

ARKANSAS DECEPTIVE TRADE PRACTICES ACT,

A.C.A. §§ 4-88-101, *et seq.*

160. The Arkansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

161. Marriott is a "person" as defined by A.C.A. § 4-88-102(5).

162. Marriott's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

163. Marriott advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

164. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

165. Marriott engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services and as to goods being of a particular standard, quality, grade, style, or model;

b. Advertising goods or services with the intent not to sell them as advertised;

c. Employing consistent bait-and-switch advertising of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell, as evidenced by acts demonstrating an intent not to sell the advertised product or services;

d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of ignorance; and

e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

166. Marriott's unconscionable, false, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arkansas Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b), which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arkansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arkansas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b).

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

168. Marriott intended to mislead Plaintiff and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

169. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

170. Marriott acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Arkansas Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

171. As a direct and proximate result of Marriott's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass members' reliance thereon, Plaintiff and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their

Personal Information; and losses related to lack of benefit of the bargain for overpaying for Marriott's services.

172. Plaintiff and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 15

CALIFORNIA CUSTOMER RECORDS ACT,

Cal. Civ. Code §§ 1798.80, *et seq.*

173. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

174. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

175. Marriott is a business that owns, maintains, and licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass members.

176. Businesses that own or license computerized data that includes personal information are required to notify California residents when their personal information has been

acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

177. Marriott is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

178. Plaintiff and California Subclass members' personal information includes that which is covered by Cal. Civ. Code § 1798.82.

179. Because Marriott reasonably believed that Plaintiff's and California Subclass members' Personal Information was acquired by unauthorized persons during the Marriott Data Breach, Marriott had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

180. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Cal. Civ. Code § 1798.82.

181. As a direct and proximate result of Marriott's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

182. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 16

CALIFORNIA UNFAIR COMPETITION LAW,

Cal. Bus. & Prof. Code §§ 17200, *et seq.*

183. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

184. Marriott is a "person" as defined by Cal. Bus. & Prof. Code §17201.

185. Marriott violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

186. Marriott's "unfair" acts and practices include:

a. Marriott failed to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Marriott Data Breach. Marriott failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. For example, Marriott failed to patch the well-known Apache Struts vulnerability, which made it trivial for a hacker to penetrate Marriott's systems. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Personal Information has been compromised.

b. Marriott's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), and California's Consumer Records Act (Cal. Civ. Code § 1798.81.5).

c. Marriott's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Marriott's inadequate security, consumers could not have reasonably avoided the harms that Marriott caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

187. Marriott has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

188. Marriott's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*

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

190. As a direct and proximate result of Marriott's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, including the costs passed through to Marriott from their consumer credit transactions,

the premiums and/or price received by Marriott for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, loss of value of their Personal Information; and overpayment for Marriott's services.

191. Marriott acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

192. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Marriott's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 17

CALIFORNIA CONSUMER LEGAL REMEDIES ACT,

Cal. Civ. Code §§ 1750, *et seq.*

193. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

194. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

195. Marriott is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

196. Plaintiff and the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

197. Marriott's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

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

199. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations

had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

200. As a direct and proximate result of Marriott's violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and overpayment for Marriott's services.

201. Plaintiff and the California Subclass have provided notice of their claims for damages to Marriott, in compliance with California Civil Code § 1782(a), and will amend their complaint to include a demand for monetary relief and damages at the appropriate time.

CLAIMS ON BEHALF OF THE COLORADO SUBCLASS

COUNT 18

COLORADO SECURITY BREACH NOTIFICATION ACT,

Colo. Rev. Stat. §§ 6-1-716, *et seq.*

202. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

203. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

204. Plaintiff and Colorado Subclass members' Personal Information includes that which is covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

205. Marriott is required to accurately notify Plaintiff and Colorado Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

206. Because Marriott was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

207. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Colo. Rev. Stat. § 6-1-716(2).

208. As a direct and proximate result of Marriott's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered damages, as described above.

209. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

COUNT 19

COLORADO CONSUMER PROTECTION ACT,

Colo. Rev. Stat. §§ 6-1-101, *et seq.*

210. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

211. Marriott is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

212. Marriott engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

213. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Marriott or successors in interest to actual consumers.

214. Marriott engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Knowingly making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality, or grade, though Marriott knew or should have known that there were or another;

c. Advertising services with intent not to sell them as advertised; and

d. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

215. Marriott's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Colorado Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Colorado Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Colorado Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

217. Marriott intended to mislead Plaintiff and Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

218. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

219. Marriott acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

220. As a direct and proximate result of Marriott's deceptive trade practices, Colorado Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

221. Marriott's deceptive trade practices significantly impact the public, because hundreds of millions of individuals were impacted by Marriott's Data Breach—and a number of those individuals (including Plaintiff) are from Colorado.

222. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages (for Marriott's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS

COUNT 20

DELAWARE COMPUTER SECURITY BREACH ACT,

6 Del. Code Ann. §§ 12B-102, *et seq.*

223. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

224. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by 6 Del. Code Ann. § 12B-102(a).

225. Plaintiff and Delaware Subclass members' Personal Information includes that which is covered under 6 Del. Code Ann. § 12B-101(4).

226. Marriott is required to accurately notify Plaintiff and Delaware Subclass members if Marriott becomes aware of a breach of its data security system which is reasonably likely to result in the misuse of a Delaware resident's Personal Information, in the most expedient time possible and without unreasonable delay under 6 Del. Code Ann. § 12B-102(a).

227. Because Marriott was aware of a breach of its security system which is reasonably likely to result in misuse of Delaware residents' Personal Information, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by 6 Del. Code Ann. § 12B-102(a).

228. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated 6 Del. Code Ann. § 12B-102(a).

229. As a direct and proximate result of Marriott's violations of 6 Del. Code Ann. § 12B-102(a), Plaintiff and Delaware Subclass members suffered damages, as described above.

230. Plaintiff and Delaware Subclass members seek relief under 6 Del. Code Ann. § 12B-104, including actual damages and equitable relief.

COUNT 21

DELAWARE CONSUMER FRAUD ACT,

6 Del. Code §§ 2513*, et seq.*

231. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

232. Marriott is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

233. Marriott advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

234. Marriott used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Delaware Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Delaware Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Delaware Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100.

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

236. Marriott acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiff and Delaware Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

237. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

238. Marriott's unlawful trade practices were gross, oppressive, and aggravated, and Marriott breached the trust of Plaintiff and the Delaware Subclass members.

239. As a direct and proximate result of Marriott's unlawful acts and practices, Plaintiff and Delaware Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

240. Plaintiff and Delaware Subclass members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the

direct and natural consequences of Marriott's unlawful conduct; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE DISTRICT OF COLUMBIA SUBCLASS

COUNT 22

DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT, D.C. Code §§ 28-3851, *et seq.*

241. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

242. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by D.C. Code § 28-3852(a).

243. Plaintiff and District of Columbia Subclass members' Personal Information includes that which is covered under D.C. Code § 28-3851(3).

244. Marriott is required to accurately notify Plaintiff and District of Columbia Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

245. Because Marriott was aware of a breach of its security system, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

246. By failing to disclose the Marriott Data Breach in a timely and accurate manner Marriott violated D.C. Code § 28-3852(a).

247. As a direct and proximate result of Marriott's violations of D.C. Code § 28-3852(a), Plaintiff and District of Columbia Subclass members suffered damages, as described above.

248. Plaintiff and District of Columbia Subclass members seek relief under D.C. Code § 28-3853(a), including actual damages.

COUNT 23

DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT,

D.C. Code §§ 28-3904, *et seq.*

249. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

250. Marriott is a "person" as defined by D.C. Code § 28-3901(a)(1).

251. Marriott is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

252. Plaintiff and District of Columbia Subclass members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

253. Marriott advertised, offered, or sold goods or services in District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of District of Columbia.

254. Marriott engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, grade, style, or model, when they are of another;

c. Misrepresenting a material fact that has a tendency to mislead;

d. Failing to state a material fact where the failure is misleading;

e. Advertising or offering goods or services without the intent to sell them as advertised or offered; and

f. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

255. Marriott's unfair, unlawful, and deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and District of Columbia Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and District of Columbia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and District of Columbia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

257. Marriott intended to mislead Plaintiff and District of Columbia Subclass members and induce them to rely on its misrepresentations and omissions.

258. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and District of Columbia Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

259. Marriott acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiff and District of Columbia Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

260. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiff and District of Columbia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

261. Plaintiff and District of Columbia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive

damages, attorneys' fees and costs, the greater of treble damages or $1500 per violation, and any other relief that the Court deems proper.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 24

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,

Fla. Stat. §§ 501.201, *et seq.*

262. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

263. Plaintiff and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

264. Marriott advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

265. Marriott engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Florida Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Florida Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Florida Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

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

267. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in

its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

268. As a direct and proximate result of Marriott's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

269. Plaintiff and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS

COUNT 25

GEORGIA SECURITY BREACH NOTIFICATION ACT,

O.C.G.A. §§ 10-1-912, *et seq.*

270. The Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

271. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by O.C.G.A. § 10-1-912(a).

272. Plaintiff and Georgia Subclass members' Personal Information includes that which is covered under O.C.G.A. § 10-1-912(a).

273. Marriott is required to accurately notify Plaintiff and Georgia Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

274. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass members' Personal Information, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by O.C.G.A. § 10-1-912(a).

275. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated O.C.G.A. § 10-1-912(a).

276. As a direct and proximate result of Marriott's violations of O.C.G.A. § 10-1-912(a), Plaintiff and Georgia Subclass members suffered damages, as described above.

277. Plaintiff and Georgia Subclass members seek relief under O.C.G.A. § 10-1-912 including actual damages and injunctive relief.

CLAIMS ON BEHALF OF THE HAWAII SUBCLASS

COUNT 26

HAWAII SECURITY BREACH NOTIFICATION ACT,

Haw. Rev. Stat. §§ 487N-1, *et seq.*

278. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

279. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Haw. Rev. Stat. § 487N-2(a).

280. Plaintiff and Hawaii Subclass members' Personal Information includes that which is covered under Haw. Rev. Stat. § 487N-2(a).

281. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Haw. Rev. Stat. § 487N-2(a).

282. Marriott is required to accurately notify Plaintiff and Hawaii Subclass members if it becomes aware of a breach of its data security system without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

283. Because Marriott was aware of a breach of its security system, it had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

284. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Haw. Rev. Stat. § 487N-2(a).

285. As a direct and proximate result of Marriott's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass members suffered damages, as described above.

286. Plaintiff and Hawaii Subclass members seek relief under Haw. Rev. Stat. § 487N-3(b), including actual damages.

COUNT 27

HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT,

Haw. Rev. Stat. §§ 480-1, *et seq.*

287. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

288. Plaintiff and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

289. Plaintiffs, the Hawaii Subclass members, and Marriott are "persons" as defined by Haw. Rev. Stat. § 480-1.

290. Marriott advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

291. Marriott engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

293. Marriott intended to mislead Plaintiff and Hawaii Subclass members and induce them to rely on its misrepresentations and omissions.

294. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

295. Marriott acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii

Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

296. As a direct and proximate result of Marriott's deceptive acts and practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

297. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 28

HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT,

Haw. Rev. Stat. §§ 481A-3, *et seq.*

298. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

299. Plaintiff and Hawaii Subclass members are "persons" as defined by Haw. Rev. Stat. § 481A-2.

300. Marriott engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

301. Marriott's unfair and deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

303. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

304. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

305. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper.

CLAIMS ON BEHALF OF THE IDAHO SUBCLASS

COUNT 29

IDAHO CONSUMER PROTECTION ACT,

Idaho Code §§ 48-601, *et seq.*

306. The Idaho Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Idaho Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

307. Marriott is a "person" as defined by Idaho Code § 48-602(1).

308. Marriott's conduct as alleged herein pertained to "goods" and "services" as defined by Idaho Code § 48-602(6) and (7).

309. Marriott advertised, offered, or sold goods or services in Idaho and engaged in trade or commerce directly or indirectly affecting the people of Idaho.

310. Marriott engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

b. Representing that goods are of a particular standard, quality, or grade when they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other acts and practices that are otherwise misleading, false, or deceptive to consumers; and

e. Engaging in unconscionable methods, acts or practices in the conduct of trade or commerce.

311. Marriott's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Idaho Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Idaho Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Idaho Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

313. Marriott intended to mislead Plaintiff and Idaho Subclass members and induce them to rely on its misrepresentations and omissions. Marriott knew its representations and omissions were false.

314. Marriott acted intentionally, knowingly, and maliciously to violate Idaho's Consumer Protection Act, and recklessly disregarded Plaintiff and Idaho Subclass members'

rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

315. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable conduct, Plaintiff and Idaho Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

316. Plaintiff and Idaho Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, injunctive relief, costs, and attorneys' fees.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT 30

ILLINOIS PERSONAL INFORMATION PROTECTION ACT,

815 ILCS §§ 530/10(a), *et seq.*

317. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

318. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information, Marriott is a Data Collector as defined in 815 ILCS § 530/5.

319. Plaintiff and Illinois Subclass members' Personal Information includes that which is covered under 815 ILCS § 530/5.

320. As a Data Collector, Marriott is required to notify Plaintiff and Illinois Subclass members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 ILCS § 530/10(a).

321. By failing to disclose the Marriott Data Breach in the most expedient time possible and without unreasonable delay, Marriott violated 815 ILCS § 530/10(a).

322. Pursuant to 815 ILCS § 530/20, a violation of 815 ILCS § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

323. As a direct and proximate result of Marriott's violations of 815 ILCS § 530/10(a), Plaintiff and Illinois Subclass members suffered damages, as described above.

324. Plaintiff and Illinois Subclass members seek relief under 815 ILCS § 510/3 for the harm they suffered because of Marriott's willful violations of 815 ILCS § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT 31

ILLINOIS CONSUMER FRAUD ACT,

815 ILCS §§ 505, *et seq.*

325. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

326. Marriott is a "person" as defined by 815 ILCS §§ 505/1(c).

327. Plaintiff and Illinois Subclass members are "consumers" as defined by 815 ILCS §§ 505/1(e).

328. Marriott's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS § 505/1(f).

329. Marriott's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 ILCS § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a), which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a).

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

331. Marriott intended to mislead Plaintiff and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

332. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

333. Marriott acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

334. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

335. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 32

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT,

815 ILCS §§ 510/2, *et seq.*

336. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

337. Marriott is a "person" as defined by 815 ILCS §§ 510/1(5).

338. Marriott engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

339. Marriott's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a), which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a).

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

341. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

342. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

343. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT 33

PERSONAL INFORMATION SECURITY BREACH

PROTECTION LAW,

Iowa Code § 715C.2

344. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

345. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Iowa Code § 715C.2(1).

346. Plaintiff's and Iowa Subclass members' Personal Information including that which is covered under Iowa Code § 715C.2(1).

347. Marriott is required to accurately notify Plaintiff and Iowa Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

348. Because Marriott was aware of a breach of its security system, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1).

349. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Iowa Code § 715C.2(1).

350. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

351. As a direct and proximate result of Marriott's violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass members suffered damages, as described above.

352. Plaintiff and Iowa Subclass members seek relief under Iowa Code § 714.16(7), including actual damages and injunctive relief.

COUNT 34

PROTECTION OF CONSUMER INFORMATION,

Kan. Stat. Ann. §§ 50-7a02(a), *et seq.*

353. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

354. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

355. Plaintiff's and Kansas Subclass members' Personal Information including that which is covered under Kan. Stat. Ann. § 50-7a02(a).

356. Marriott is required to accurately notify Plaintiffs and Kansas Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

357. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass members' Personal Information, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

358. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Kan. Stat. Ann. § 50-7a02(a).

359. As a direct and proximate result of Marriott's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages, as described above.

360. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT 35

KANSAS CONSUMER PROTECTION ACT,

K.S.A. §§ 50-623, *et seq.*

361. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

362. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

363. Plaintiff and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

364. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

365. Marriott is a "supplier" as defined by K.S.A. § 50-624(l).

366. Marriott advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

367. Marriott engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kansas Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kansas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

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

369. Marriott intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

370. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in

business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

371. Marriott also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Marriott knew were substantially one-sided in favor of Marriott (see K.S.A. § 50-627(b)(5)).

372. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Personal Information in Marriott's possession.

373. The above unfair, deceptive, and unconscionable practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

374. Marriott acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

375. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

376. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT 36

KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT,

Ky. Rev. Stat. Ann. §§ 365.732, *et seq.*

377. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

378. Marriott is required to accurately notify Plaintiff and Kentucky Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have

caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

379. Marriott is a business that holds computerized data that includes Personal Information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

380. Plaintiff's and Kentucky Subclass members' Personal Information includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

381. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

382. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Ky. Rev. Stat. Ann. § 365.732(2).

383. As a direct and proximate result of Marriott's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass members suffered damages, as described above.

384. Plaintiff and Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

COUNT 37

KENTUCKY CONSUMER PROTECTION ACT,

Ky. Rev. Stat. §§ 367.110, *et seq.*

385. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

386. Marriott is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

387. Marriott advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

388. Marriott engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kentucky Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kentucky Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kentucky Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

390. Marriott intended to mislead Plaintiff and Kentucky Subclass members and induce them to rely on its misrepresentations and omissions.

391. Plaintiff and Kentucky Subclass members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Marriott's unlawful acts and practices.

392. The above unlawful acts and practices by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

393. Marriott acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

394. As a direct and proximate result of Marriott's unlawful acts and practices, Plaintiff and Kentucky Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

395. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS

COUNT 38

DATABASE SECURITY BREACH NOTIFICATION LAW,

La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.*

396. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

397. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

398. Plaintiff's and Louisiana Subclass members' Personal Information includes Personal Information as covered under La. Rev. Stat. Ann. § 51:3074(C).

399. Marriott is required to accurately notify Plaintiff and Louisiana Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

400. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, Marriott had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

401. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated La. Rev. Stat. Ann. § 51:3074(C).

402. As a direct and proximate result of Marriott's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages, as described above.

403. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

COUNT 39

LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,

La. Rev. Stat. Ann. §§ 51:1401, *et seq.*

404. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

405. Marriott, Plaintiff, and the Louisiana Subclass members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

406. Plaintiff and Louisiana Subclass members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

407. Marriott engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

408. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

409. Marriott participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Louisiana Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Louisiana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Louisiana Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

411. Marriott intended to mislead Plaintiff and Louisiana Subclass members and induce them to rely on its misrepresentations and omissions.

412. Marriott's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Louisiana

Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

413. Marriott acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

414. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

415. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of

value of their Personal Information; and paying more for Defendant's services than they would have.

416. Plaintiff and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Marriott's knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 40

MICHIGAN IDENTITY THEFT PROTECTION ACT,

Mich. Comp. Laws Ann. §§ 445.72, *et seq.*

417. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

418. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

419. Plaintiff's and Michigan Subclass members' Personal Information is covered under Mich. Comp. Laws Ann. § 445.72(1).

420. Marriott is required to accurately notify Plaintiff and Michigan Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

421. Because Marriott discovered a security breach and had notice of a security breach (where Personal Information was accessed or acquired by unauthorized persons), Marriott had an

obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

422. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Mich. Comp. Laws Ann. § 445.72(4).

423. As a direct and proximate result of Marriott's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass members suffered damages, as described above.

424. Plaintiff and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT 41

MICHIGAN CONSUMER PROTECTION ACT,

Mich. Comp. Laws Ann. §§ 445.903, *et seq.*

425. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

426. Marriott and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

427. Marriott advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

428. Marriott engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

429. Marriott's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Michigan Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Michigan Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Michigan Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

431. Marriott intended to mislead Plaintiff and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

432. Marriott acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass members'

rights. Previous data breaches put Marriott on notice that its security and privacy protections were inadequate.

433. As a direct and proximate result of Marriott's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

434. Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS

COUNT 42

MINNESOTA CONSUMER FRAUD ACT,

Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.*

435. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

436. Marriott, Plaintiff, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

437. Marriott's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

438. Marriott engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

439. Marriott engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Minnesota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

441. Marriott intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

442. Marriott's fraudulent, misleading, and deceptive practices affected the public interest, including millions of Minnesotans affected by the Marriott Data Breach.

443. As a direct and proximate result of Marriott's fraudulent, misleading, and deceptive practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

444. Plaintiff and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT 43

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT,

Minn. Stat. §§ 325D.43, *et seq.*

445. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

446. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Marriott violated Minn. Stat. § 325D.44, including the following provisions:

a. Representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);

b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);

c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and

d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

447. Marriott's deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Minnesota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

449. Marriott intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

450. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

451. Marriott acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Minnesota Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

452. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

453. Plaintiff and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT 44

MISSOURI MERCHANDISE PRACTICES ACT,

Mo. Rev. Stat. §§ 407.010, *et seq.*

454. The Missouri Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

455. Marriott is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

456. Marriott advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

457. Plaintiff and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

458. Marriott engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Missouri Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Missouri Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Missouri Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

460. Marriott intended to mislead Plaintiff and Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

461. Marriott acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass members'

rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

462. As a direct and proximate result of Marriott's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

463. Plaintiff and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

CLAIMS ON BEHALF OF THE MONTANA SUBCLASS

COUNT 45

COMPUTER SECURITY BREACH LAW,

Mont. Code Ann. §§ 30-14-1704(1), *et seq.*

464. The Montana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

465. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Mont. Code Ann. § 30-14-1704(4)(b). Marriott also maintains computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to Mont. Code Ann. § 30-14-1704(1) and (2).

466. Plaintiff's and Montana Subclass members' Personal Information includes that covered by Mont. Code Ann. § 30-14-1704(4)(b).

467. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Plaintiff and Montana Subclass members, pursuant to Mont. Code Ann. § 30-14-1704(2).

468. Marriott is required to accurately notify Plaintiff and Montana Subclass members if it discovers a security breach or receives notice of a security breach which may have compromised Personal Information which Marriott owns or licenses, without unreasonable delay under Mont. Code Ann. § 30-14-1704(1).

469. Because Marriott was aware of a Data Breach, Marriott had an obligation to disclose the Data Breach as mandated by Mont. Code Ann. § 30-14-1704(1) and (2).

470. Pursuant to Mont. Code Ann. § 30-14-1705, violations of Mont. Code Ann. § 30-14-1704 are unlawful practices under Mont. Code Ann. § 30-14-103, Montana's Consumer Protection Act.

471. As a direct and proximate result of Marriott's violations of Mont. Code Ann. § 30-14-1704(1) and (2), Plaintiff and Montana Subclass members suffered damages, as described above.

472. Plaintiff and Montana Subclass members seek relief under Mont. Code Ann. § 30-14-133, including actual damages and injunctive relief.

COUNT 46

MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, M.C.A. §§ 30-14-101, *et seq.*

473. The Montana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

474. Marriott is a "person" as defined by MCA § 30-14-102(6).

475. Plaintiff and Montana Subclass members are "consumers" as defined by MCA§ 30-14-102(1).

476. Marriott advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by MCA § 30-14-102(8).

477. Marriott engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation MCA § 30-14-103, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Montana Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Montana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Montana Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

479. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years.

Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

480. Marriott's acts described above are unfair and offend public policy; they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

481. Marriott acted intentionally, knowingly, and maliciously to violate Montana's Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiff and Montana Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

482. As a direct and proximate result of Marriott's unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiff and Montana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

483. Plaintiff and Montana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of

$500, treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS

COUNT 47

NEBRASKA CONSUMER PROTECTION ACT,

Neb. Rev. Stat. §§ 59-1601, *et seq.*

484. The Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

485. Marriott and Nebraska Subclass members are each a "person" as defined by Neb. Rev. Stat. § 59-1601(1).

486. Marriott advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

487. Marriott engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nebraska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

489. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of

value of their Personal Information; and paying more for Defendant's services than they would have.

490. Marriott's unfair and deceptive acts and practices complained of herein affected the public interest, including the large percentage of Nebraskans affected by the Marriott Data Breach.

491. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either (1) actual damages or (2) $1,000, civil penalties, and reasonable attorneys' fees and costs.

COUNT 48

NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT,

Neb. Rev. Stat. §§ 87-301, *et seq.*

492. The Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

493. Marriott and Nebraska Subclass members are "persons" as defined by Neb. Rev. Stat. § 87-301(19).

494. Marriott advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

495. Marriott engaged in deceptive trade practices in the course of its business, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including:

a. Represented that goods and services have characteristics, uses, benefits, or qualities that they do not have;

b. Represented that goods and services are of a particular standard, quality, or grade if they are of another; and

c. Advertised its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

496. Marriott's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nebraska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

498. Marriott intended to mislead Plaintiff and Nebraska Subclass members and induce them to rely on its misrepresentations and omissions.

499. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

500. Marriott acted intentionally, knowingly, and maliciously to violate Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nebraska Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

501. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent

activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

502. Marriott's deceptive trade practices complained of herein affected consumers at large, including the large percentage of Nebraskans affected by the Marriott Data Breach.

503. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEVADA SUBCLASS

COUNT 49

NEVADA DECEPTIVE TRADE PRACTICES ACT,

Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.*

504. The Nevada Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

505. Marriott advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

506. Marriott engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 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. § 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 they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);

c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat § 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. § 598.0923(A)(2); and

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

507. 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 Plaintiff and Nevada Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nevada Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nevada Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210.

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

509. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in

its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

510. Marriott acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

511. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Nevada Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

512. Plaintiff and Nevada Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS

COUNT 50

NOTICE OF SECURITY BREACH,

N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), *et seq.*

513. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

514. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

515. Plaintiff's and New Hampshire Subclass members' Personal Information includes that which is covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

516. Marriott is required to accurately notify Plaintiff and New Hampshire Subclass members if Marriott becomes aware of a breach of its data security system in which misuse of Personal Information has occurred or is reasonably likely to occur, as soon as possible under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

517. Because Marriott was aware of a security breach in which misuse of Personal Information has occurred or is reasonably likely to occur, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

518. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

519. As a direct and proximate result of Marriott's violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass members suffered damages, as described above.

520. Plaintiff and New Hampshire Subclass members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including actual damages and injunctive relief.

COUNT 51

NEW HAMPSHIRE CONSUMER PROTECTION ACT,

N.H.R.S.A. §§ 358-A, *et seq.*

521. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

522. Marriott is a "person" under the New Hampshire Consumer Protection.

523. Marriott advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H.R.S.A. § 358-A:1.

524. Marriott engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H.R.S.A. § 358-A:2, including:

a. Representing that its goods or services have characteristics, uses, or benefits that they do not have in violation of N.H.R.S.A. § 358-A:2.V;

b. Representing that its goods or services are of a particular standard or quality if they are of another in violation of N.H.R.S.A. § 358-A:2.VII; and

c. Advertising its goods or services with intent not to sell them as advertised in violation of N.H.R.S.A. § 358-A:2.IX.

525. Marriott's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Hampshire Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Hampshire Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Hampshire Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

527. Marriott acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiff and New Hampshire Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate. Marriott's acts and practices went beyond the realm of strictly private transactions.

528. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and New Hampshire Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

529. Plaintiff and New Hampshire Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 52

NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT,

N.J. Stat. Ann. §§ 56:8-163, *et seq.*

530. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

531. Marriott is a business that compiles or maintains computerized records that include Personal Information on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

532. Plaintiff's and New Jersey Subclass members' Personal Information includes that which is covered under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

533. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person."

534. Because Marriott discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Marriott had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

535. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated N.J. Stat. Ann. § 56:8-163(b).

536. As a direct and proximate result of Marriott's violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass members suffered the damages described above.

537. Plaintiff and New Jersey Subclass members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT 53

NEW JERSEY CONSUMER FRAUD ACT,

N.J. Stat. Ann. §§ 56:8-1, *et seq.*

538. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

539. Marriott is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

540. Marriott sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

541. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, *et seq.*, prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

542. Marriott's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Jersey Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Jersey Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

544. Marriott intended to mislead Plaintiff and New Jersey Subclass members and induce them to rely on its misrepresentations and omissions.

545. Marriott acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff and New Jersey Subclass members'

rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

546. As a direct and proximate result of Marriott's unconscionable and deceptive practices, Plaintiff and New Jersey Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

547. Plaintiff and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS

COUNT 54

NEW MEXICO UNFAIR PRACTICES ACT,

N.M. Stat. Ann. §§ 57-12-2, *et seq.*

548. The New Mexico Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

549. Marriott is a "person" as meant by N.M. Stat. Ann. § 57-12-2.

550. Marriott was engaged in "trade" and "commerce" as defined by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

551. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

552. Marriott engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following:

a. Knowingly representing that its goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. § 57-12-2(D)(5);

b. Knowingly representing that its goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. § 57-12-2(D)(7);

c. Knowingly using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive in violation of N.M. Stat. Ann. § 57-12-2(D)(14);

d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff's and the New Mexico Subclass' detriment in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and

e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).

553. Marriott's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Mexico Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Mexico Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and mandating reasonable data security, N.M. Stat. § 57-12C-4;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Mexico Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and mandating reasonable data security, N.M. Stat. § 57-12C-4.

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

555. Marriott intended to mislead Plaintiff and New Mexico Subclass members and induce them to rely on its misrepresentations and omissions.

556. Marriott acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass members'

rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

557. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

558. Plaintiff and New Mexico Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 55

INFORMATION SECURITY BREACH AND NOTIFICATION ACT,

N.Y. Gen. Bus. Law § 899-aa

559. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

560. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a). Marriott also maintains

computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

561. Plaintiff's and New York Subclass members' Personal Information includes that which is covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

562. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Plaintiff and New York Subclass members, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

563. Marriott is required to accurately notify Plaintiff and New York Subclass members if it discovers a security breach or receives notice of a security breach which may have compromised Personal Information which Marriott owns or licenses, in the most expedient time possible and without unreasonable delay under N.Y. Gen. Bus. Law § 899-aa(2).

564. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

565. As a direct and proximate result of Marriott's violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiff and New York Subclass members suffered damages, as described above.

566. Plaintiff and New York Subclass members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

COUNT 56

NEW YORK GENERAL BUSINESS LAW,

N.Y. Gen. Bus. Law §§ 349, *et seq.*

567. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

568. Marriott engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New York Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New York Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

570. Marriott acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

571. As a direct and proximate result of Marriott's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

572. Marriott's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Marriott Data Breach.

573. The above deceptive and unlawful practices and acts by Marriott caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

574. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT 57

NORTH CAROLINA IDENTITY THEFT PROTECTION ACT,

N.C. Gen. Stat. §§ 75-60, *et seq.*

575. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

576. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

577. Plaintiff and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

578. Marriott is required to accurately notify Plaintiff and North Carolina Subclass members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

579. Plaintiff's and North Carolina Subclass members' Personal Information includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

580. Because Marriott discovered a security breach and had notice of a security breach (where Personal Information was accessed or acquired by unauthorized persons), Marriott had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

581. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated N.C. Gen. Stat. § 75-65.

582. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

583. As a direct and proximate result of Marriott's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass members suffered damages, as described above.

584. Plaintiff and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

COUNT 58

NORTH CAROLINA UNFAIR TRADE PRACTICES ACT,

N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.*

585. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

586. Marriott advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

587. Marriott engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Carolina Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and North Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Carolina Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

589. Marriott intended to mislead Plaintiff and North Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

590. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

591. Marriott acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

592. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

593. Marriott's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

594. Plaintiff and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NORTH DAKOTA SUBCLASS

COUNT 59

NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION,

N.D. Cent. Code §§ 51-30-02, *et seq.*

595. The North Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

596. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.D. Cent. Code § 51-30-01(4). Marriott also maintains computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to N.D. Cent. Code §§ 51-30-02 and 03.

597. Plaintiff's and North Dakota Subclass members' Personal Information includes that which is covered by N.D. Cent. Code § 51-30-01(4).

598. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Plaintiff and North Dakota Subclass members, pursuant to N.D. Cent. Code § 51-30-03.

599. Marriott is required to accurately notify Plaintiff and North Dakota Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Marriott owns or licenses, in the most expedient time possible and without unreasonable delay under N.D. Cent. Code § 51-30-02.

600. Because Marriott was aware of a security breach, Marriott had an obligation to disclose the Data Breach as mandated by N.D. Cent. Code §§ 51-30-02 and 51-30-03.

601. Pursuant to N.D. Cent. Code § 51-30-07, violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03 are unlawful sales or advertising practices which violate chapter 51-15 of the North Dakota Century Code.

602. As a direct and proximate result of Marriott's violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03, Plaintiff and North Dakota Subclass members suffered damages, as described above.

603. Plaintiff and North Dakota Subclass members seek relief under N.D. Cent. Code §§ 51-15-01 *et seq.*, including actual damages and injunctive relief.

COUNT 60

NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT,

N.D. Cent. Code §§ 51-15-01, *et seq.*

604. The North Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

605. Marriott, Plaintiff, and each member of the North Dakota Subclass is a "person," as defined by N.D. Cent. Code § 51-15-01(4).

606. Marriott sells and advertises "merchandise," as defined by N.D. Cent. Code § 51-15-01(3) and (5).

607. Marriott advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

608. Marriott engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code § 51-15-01, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Dakota Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and North Dakota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Dakota Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

610. Marriott's above-described acts and practices caused substantial injury to Plaintiff and North Dakota Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

611. Marriott intended to mislead Plaintiff and North Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

612. Marriott acted intentionally, knowingly, and maliciously to violate North Dakota's Unlawful Sales or Advertising Law, and recklessly disregarded Plaintiff and North Dakota Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

613. As a direct and proximate result of Marriott's deceptive, unconscionable, and substantially injurious practices, Plaintiff and North Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

614. Plaintiff and North Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 61

OHIO CONSUMER SALES PRACTICES ACT,

Ohio Rev. Code §§ 1345.01, *et seq.*

615. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

616. Plaintiff and Ohio Subclass members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

617. Marriott was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

618. Marriott advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

619. Marriott engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including:

a. Marriott represented that its goods, services, and intangibles had performance characteristics, uses, and benefits that it did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and

b. Marriott represented that its goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

620. Marriott engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Ohio Subclass to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and

b. Requiring Plaintiff and the Ohio Subclass to enter into a consumer transaction on terms that Marriott knew were substantially one-sided in favor of Marriott (Ohio Rev. Code Ann. § 1345.03(B)(5)).

621. Marriott's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

622. The Data Breach, which occurred over the course of four years, demonstrates that Marriott did not meet the minimum threshold requirements for implementation of data security practices. As discussed herein, Marriott did not maintain programs that protected the security and confidentiality of its customers' Personal Information, protected against anticipated threats

or hazards to the security or integrity of that Personal Information, protected against unauthorized access to and acquisition of the Personal Information that is likely to result in the material risk of identity theft or other fraud to the individual to whom the information relates. Accordingly, Marriott is entitled to no affirmative defense regarding the design and maintenance of any cybersecurity programs.

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

624. Marriott intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

625. Marriott acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

626. Marriott's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the millions of Ohioans affected by the Marriott Data Breach.

627. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable acts and practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud

and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

628. Plaintiff and the Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

COUNT 62

OHIO DECEPTIVE TRADE PRACTICES ACT,

Ohio Rev. Code §§ 4165.01, *et seq.*

629. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

630. Marriott, Plaintiff, and Ohio Subclass members are a "person," as defined by Ohio Rev. Code § 4165.01(D).

631. Marriott advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

632. Marriott engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);

b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and

c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

633. Marriott's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to

protect Plaintiff and Ohio Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

635. Marriott intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

636. The Data Breach, which occurred over the course of four years, demonstrates that Marriott did not meet the minimum threshold requirements for implementation of data security practices. As discussed herein, Marriott did not maintain programs that protected the security and confidentiality of its customers' Personal Information, protected against anticipated threats

or hazards to the security or integrity of that Personal Information, protected against unauthorized access to and acquisition of the Personal Information that is likely to result in the material risk of identity theft or other fraud to the individual to whom the information relates. Accordingly, Marriott is entitled to no affirmative defense regarding the design and maintenance of any cybersecurity programs

637. Marriott acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

638. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

639. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

COUNT 63

OKLAHOMA CONSUMER PROTECTION ACT,

Okla. Stat. Tit. 15, §§ 751, *et seq.*

640. The Oklahoma Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

641. Marriott is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

642. Marriott's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

643. Marriott, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

a. Making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5);

b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7);

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8);

d. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and

e. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

644. Marriott's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oklahoma Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oklahoma Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oklahoma Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

646. Marriott intended to mislead Plaintiff and Oklahoma Subclass members and induce them to rely on its misrepresentations and omissions.

647. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in

business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

648. The above unlawful practices and acts by Marriott were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Oklahoma Subclass members.

649. Marriott acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

650. As a direct and proximate result of Marriott's unlawful practices, Plaintiff and Oklahoma Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

651. Plaintiff and Oklahoma Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OREGON SUBCLASS

COUNT 64

OREGON CONSUMER IDENTITY THEFT PROTECTION ACT,

Or. Rev. Stat. §§ 646A.604(1), *et seq.*

652. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

653. Marriott is a business that maintains records which contain Personal Information, within the meaning of Or. Rev. Stat. § 646A.622(1), about Plaintiff and Oregon Subclass members.

654. Pursuant to Or. Rev. Stat. § 646A.622(1), a business "that maintains records which contain Personal Information" of an Oregon resident "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

655. Marriott violated Or. Rev. Stat. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiff's and Oregon Subclass members' Personal Information.

656. Marriott is a business that owns, maintains, or otherwise possesses data that includes consumers Personal Information as defined by Or. Rev. Stat. § 646A.604(1).

657. Plaintiff's and Oregon Subclass members' Personal Information includes Personal Information as covered under Or. Rev. Stat. § 646A.604(1).

658. Marriott is required to accurately notify Plaintiff and Oregon Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. § 646A.604(1).

659. Because Marriott discovered a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Or. Rev. Stat. § 646A.604(1).

660. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Or. Rev. Stat. § 646A.604(1).

661. Pursuant to Or. Rev. Stat. § 646A.604(9), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

662. As a direct and proximate result of Marriott's violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass members suffered damages, as described above.

663. Plaintiff and Oregon Subclass members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

COUNT 65

OREGON UNLAWFUL TRADE PRACTICES ACT,

Or. Rev. Stat. §§ 646.608, *et seq.*

664. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

665. Marriott is a "person," as defined by Or. Rev. Stat. § 646.605(4).

666. Marriott engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

667. Marriott sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

668. Marriott advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

669. Marriott engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

b. Representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

c. Advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and

d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

670. Marriott's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oregon Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oregon Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oregon Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*

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

672. Marriott intended to mislead Plaintiff and Oregon Subclass members and induce them to rely on its misrepresentations and omissions.

673. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

674. Marriott acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

675. As a direct and proximate result of Marriott's unlawful practices, Plaintiff and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

676. Plaintiff and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 66

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,

73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*

677. The Pennsylvania Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

678. Marriott is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

679. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

680. Marriott Pennsylvania engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

681. Marriott's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Pennsylvania Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Pennsylvania Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Pennsylvania Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

683. Marriott intended to mislead Plaintiff and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

684. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

685. Marriott acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

686. As a direct and proximate result of Marriott's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass' reliance on them, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

687. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100

(whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE PUERTO RICO SUBCLASS

COUNT 67

CITIZEN INFORMATION ON DATA BANKS SECURITY ACT,

P.R. Laws Ann. tit. 10, §§ 4051, *et seq.*

688. Plaintiffs, on behalf of the Puerto Rico Subclass, repeat and allege Paragraphs 1-275, as if fully alleged herein.

689. Marriott is the owner and custodian of databases that include Personal Information as defined by P.R. Laws Ann. tit. 10, § 4051(a), and is therefore subject to. P.R. Laws Ann. tit. 10, § 4052.

690. Plaintiff's and Puerto Rico Subclass members' Personal Information (e.g., Social Security numbers) includes personal identifying information as covered under P.R. Laws Ann. tit. 10, § 4051(a).

691. Marriott is required to accurately notify Plaintiff and Puerto Rico Subclass members following discovery or notification of a breach of its data security system as expeditiously as possible under P.R. Laws Ann. tit. 10, § 4052.

692. Because Marriott discovered a breach of its data security system, Marriott had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by P.R. Laws Ann. tit. 10, § 4052.

693. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated P.R. Laws Ann. tit. 10, § 4052.

694. As a direct and proximate result of Marriott's violations of P.R. Laws Ann. tit. 10, § 4052, Plaintiff and Puerto Rico Subclass members suffered damages, as described above.

695. Plaintiff and Puerto Rico Subclass members seek relief under P.R. Laws Ann. tit. 10, § 4055, including actual damages and injunctive relief.

CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS

COUNT 68

RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT,

R.I. Gen. Laws §§ 6-13.1, *et seq.*

696. The Rhode Island Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Rhode Island Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

697. Plaintiff and Rhode Island Subclass members are each a "person," as defined by R.I. Gen. Laws § 6-13.1-1(3).

698. Plaintiff and Rhode Island Subclass members purchased goods and services for personal, family, or household purposes.

699. Marriott advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

700. Marriott engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-52(6)(v));

b. Representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-52(6)(vii));

c. Advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-52(6)(ix));

d. Engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-52(6)(xii));

e. Engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-52(6)(xiii)); and

f. Using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-52(6)(xiv)).

701. Marriott's unfair and deceptive acts include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Rhode Island Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Rhode Island Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Rhode Island Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2.

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

703. Marriott intended to mislead Plaintiff and Rhode Island Subclass members and induce them to rely on its misrepresentations and omissions.

704. Marriott acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Rhode Island Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

705. As a direct and proximate result of Marriott's unfair and deceptive acts, Plaintiff and Rhode Island Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

706. Plaintiff and Rhode Island Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $200 per Subclass Member (whichever is greater), punitive damages, injunctive relief, other equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS

COUNT 69

SOUTH CAROLINA DATA BREACH SECURITY ACT,

S.C. Code Ann. §§ 39-1-90, *et seq.*

707. The South Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

708. Marriott is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

709. Plaintiff's and South Carolina Subclass members' Personal Information includes that which is covered under S.C. Code Ann. § 39-1-90(D)(3).

710. Marriott is required to accurately notify Plaintiff and South Carolina Subclass members following discovery or notification of a breach of its data security system if Personal Information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

711. Because Marriott discovered a breach of its data security system in which Personal Information that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Marriott had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

712. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated S.C. Code Ann. § 39-1-90(A).

713. As a direct and proximate result of Marriott's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and South Carolina Subclass members suffered damages, as described above.

714. Plaintiff and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

COUNT 70

SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT,

S.C. Code Ann. §§ 39-5-10, *et seq.*

715. The South Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

716. Marriott is a "person," as defined by S.C. Code Ann. § 39-5-10(a).

717. South Carolina's Unfair Trade Practices Act (SC UTPA) prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

718. Marriott advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

719. Marriott engaged in unfair and deceptive acts and practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and South Carolina Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and South Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and South Carolina Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

720. Marriott's acts and practices had, and continue to have, the tendency or capacity to deceive.

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

722. Marriott intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

723. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

724. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiff and the South Carolina Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to the Personal Information in Marriott's possession, and place trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Carolina Subclass that contradicted these representations.

725. Marriott's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Marriott's acts and practices offend established public policies that seek to protect consumers' Personal Information and ensure that entities entrusted with Personal Information use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45, and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, *et seq.*

726. Marriott's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of Marriott's long history of inadequate data security and previous data breaches; the sensitivity and extensivity of Personal Information in its possession; ; and its duty of trustworthiness and care as an entrusted steward of data.

727. Marriott's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition. Such acts or practices impact the public at large, including the millions South Carolinians impacted by the Marriott Data Breach.

728. Marriott's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Marriott's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

729. Marriott's violations present a continuing risk to Plaintiff and South Carolina Subclass members as well as to the general public.

730. Marriott intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

731. Marriott acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and South Carolina Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct, and would deter Marriott and others from committing similar conduct in the future.

732. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiff and South Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

733. Plaintiff and South Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE SOUTH DAKOTA SUBCLASS

COUNT 71

SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT,

S.D. Codified Laws §§ 37-24-1, *et seq.*

734. The South Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Dakota Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

735. Marriott is a "person," as defined by S.D. Codified Laws § 37-24-1(8).

736. Marriott advertises and sells "merchandise," as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

737. Marriott advertised, offered, or sold goods or services in South Dakota and engaged in trade or commerce directly or indirectly affecting the people of South Dakota, as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

738. Marriott knowingly engaged in deceptive acts or practices, misrepresentation, concealment, suppression, or omission of material facts in connection with the sale and advertisement of goods or services, in violation of S.D. Codified Laws § 37-24-6, including:

d. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and South Dakota Subclass members' Personal Information, which was a direct and proximate cause of the Marriott Data Breach;

e. 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 Marriott Data Breach;

f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

g. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and South Dakota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

h. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

i. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and South Dakota Subclass members' Personal Information; and

a. 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 Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

739. Marriott intended to mislead Plaintiff and South Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

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

741. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

742. Marriott had a duty to disclose the above facts because such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the South Dakota Subclass, and Marriott, because consumers are unable to fully protect their interests with regard to their data, and have placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Dakota Subclass that contradicted these representations.

743. As a direct and proximate result of Marriott's deceptive acts or practices, misrepresentations, and concealment, suppression, and/or omission of material facts, Plaintiff and South Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

744. Marriott's violations present a continuing risk to Plaintiff and South Dakota Subclass members as well as to the general public.

745. Plaintiff and South Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 72

TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT,

Tenn. Code Ann. §§ 47-18-2107, *et seq.*

746. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

747. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

748. Plaintiff's and Tennessee Subclass members' Personal Information includes that which is covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

749. Marriott is required to accurately notify Plaintiff and Tennessee Subclass members following discovery or notification of a breach of its data security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an

unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

750. Because Marriott discovered a breach of its security system in which Personal Information was acquired by an unauthorized person, Marriott had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

751. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Tenn. Code Ann. § 47-18-2107(b).

752. As a direct and proximate result of Marriott's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

753. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

COUNT 73

TENNESSEE CONSUMER PROTECTION ACT,

Tenn. Code Ann. §§ 47-18-101, *et seq.*

754. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

755. Marriott is a "person," as defined by Tenn. Code § 47-18-103(13).

756. Plaintiff and Tennessee Subclass members are "consumers," as meant by Tenn. Code § 47-18-103(2).

757. Marriott advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

758. Marriott advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And Marriott's acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

759. Marriott's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Tennessee Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Tennessee Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Tennessee Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Tennessee Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Tennessee Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

760. Marriott intended to mislead Plaintiff and Tennessee Subclass members and induce them to rely on its misrepresentations and omissions.

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

762. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

763. Marriott had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Tennessee Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Tennessee Subclass that contradicted these representations.

764. Marriott's "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

765. The injury to consumers was and is substantial because it was non-trivial and non-speculative, and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

766. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

767. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

768. By misrepresenting and omitting material facts about its data security and failing to comply with its common law and statutory duties pertaining to data security (including its duties under the FTC Act), Marriott violated the following provisions of Tenn. Code § 47-18-104(b):

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve.

769. Marriott acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiff and Tennessee Subclass members'

rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

770. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiff and Tennessee Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

771. Marriott's violations present a continuing risk to Plaintiff and Tennessee Subclass members as well as to the general public.

772. Plaintiff and Tennessee Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

CLAIMS ON BEHALF OF THE UTAH SUBCLASS

COUNT 74

UTAH CONSUMER SALES PRACTICES ACT,

Utah Code §§ 13-11-1, *et seq.*

773. The Utah Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Utah Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

774. Marriott is a "person," as defined by Utah Code § 13-11-1(5).

775. Marriott is a "supplier," as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces "consumer transactions," as defined by Utah Code § 13-11-1(2).

776. Marriott engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Utah Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Utah Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Utah Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201.

777. Marriott intended to mislead Plaintiff and Utah Subclass members and induce them to rely on its misrepresentations and omissions.

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

779. Had Marriott disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

780. Marriott had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Utah Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Utah Subclass that contradicted these representations.

781. Marriott intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

a. Indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not;

b. Indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;

c. Indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not;

d. Indicating that the subject of a consumer transaction will be supplied in greater quantity (e.g. more data security) than the supplier intends.

782. Marriott engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. Marriott's acts and practices unjustly imposed hardship on Plaintiff and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity; and lost value of their Personal Information. The deficiencies in Marriott's data security, and the material misrepresentations and omissions concerning those deficiencies, led to unfair surprise to Plaintiff and the Utah Subclass when the Data Breach occurred.

783. As a direct and proximate result of Marriott's unconscionable and deceptive acts or practices, Plaintiffs and Utah Subclass members have suffered and will continue to suffer

injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

784. Marriott's violations present a continuing risk to Plaintiff and Utah Subclass members as well as to the general public.

785. Plaintiff and Utah Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of $2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, *et seq.*; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VERMONT SUBCLASS

COUNT 75

VERMONT CONSUMER FRAUD ACT,

Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.*

786. The Vermont Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Vermont Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

787. Plaintiff and Vermont Subclass members are "consumers," as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

788. Marriott's conduct as alleged herein related to "goods" or "services" for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

789. Marriott is a "seller," as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

790. Marriott advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

791. Marriott engaged in unfair and deceptive acts or practices, in violation of Vt. Stat. tit. 9, § 2453(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Vermont Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Vermont Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Vermont Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

792. Marriott intended to mislead Plaintiff and Vermont Subclass members and induce them to rely on its misrepresentations and omissions.

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

794. Marriott had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Vermont Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Vermont Subclass that contradicted these representations.

795. Marriott's acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

796. The injury to consumers was and is substantial because it was non-trivial and non-speculative; and involved a concrete monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

797. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of

consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

798. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

799. Marriott is presumed, as a matter of law under Vt. Stat. Ann. tit. 9, § 2457, to have intentionally violated the Vermont Consumer Protection Act because it failed to sell goods or services in the manner and of the nature advertised or offered.

800. Marriott acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Fraud Act, and recklessly disregarded Plaintiff and Vermont Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

801. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiff and Vermont Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

802. Marriott's violations present a continuing risk to Plaintiff and Vermont Subclass members as well as to the general public.

803. Plaintiff and Vermont Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, actual damages, disgorgement of profits, treble damages, punitive/exemplary damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS

COUNT 76

VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT,

Va. Code. Ann. §§ 18.2-186.6, *et seq.*

804. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

805. Marriott is required to accurately notify Plaintiff and Virginia Subclass members following discovery or notification of a breach of its data security system if unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

806. Marriott is an entity that owns or licenses computerized data that includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(B).

807. Plaintiff's and Virginia Subclass members' Personal Information includes Personal Information as covered under Va. Code Ann. § 18.2-186.6(A).

808. Because Marriott discovered a breach of its security system in which unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and

acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

809. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Va. Code Ann. § 18.2-186.6(B).

810. As a direct and proximate result of Marriott's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass members suffered damages, as described above.

811. Plaintiff and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

COUNT 77

VIRGINIA CONSUMER PROTECTION ACT,

Va. Code Ann. §§ 59.1-196, *et seq.*

812. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

813. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

814. Marriott is a "person" as defined by Va. Code Ann. § 59.1-198.

815. Marriott is a "supplier," as defined by Va. Code Ann. § 59.1-198.

816. Marriott engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198.

Marriott advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

817. Marriott engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virginia Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virginia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virginia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

818. Marriott intended to mislead Plaintiff and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

819. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Virginia Subclass members, about the adequacy of Marriott's computer and data security and the quality of the Marriott brand.

820. Had Marriott disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott and its predecessors maintained customer Personal Information in its databases, where it was insecure, and subject to attack over the course of four years. Customers including Plaintiff and Subclass members would not have provided Marriott with their Personal Information had they known that Marriott was misrepresenting the security of, and omitting the flaws in, its databases. Marriott could not have continued to book hotel reservations had it disclosed the truth about its lax security. Additionally, Plaintiff and Class members would not have paid as much as they did for Defendant's services had they known that Defendant would not keep their information secure. Accordingly, Plaintiff and Class members did not receive the benefit of their bargain.

821. Marriott had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virginia Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virginia Subclass that contradicted these representations.

822. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

823. Marriott acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish Marriott for its wrongdoing, and warn or deter others from engaging in similar conduct.

824. As a direct and proximate result of Marriott's deceptive acts or practices, Plaintiff and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

825. Marriott's violations present a continuing risk to Plaintiff and Virginia Subclass members as well as to the general public.

826. Plaintiff and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VIRGIN ISLANDS SUBCLASS

COUNT 78

IDENTITY THEFT PREVENTION ACT,

V.I. Code tit. 14 §§ 2208, *et seq.*

827. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-275, as if fully alleged herein.

828. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by V.I Code tit. 14 § 2201(a). Marriott also maintains computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to V.I Code tit. 14 §§ 2208(a) and (b).

829. Virgin Islands Subclass members' Personal Information (*e.g.* Social Security numbers) includes Personal Information covered by V.I Code tit. 14 § 2201(a).

830. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Virgin Islands Subclass members, pursuant to V.I Code tit. 14 § 2208(b).

831. Marriott is required to accurately notify Virgin Islands Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised

Personal Information which Marriott owns or licenses, in the most expedient time possible and without unreasonable delay under V.I Code tit. 14 § 2208(a).

832. Because Marriott was aware of a security breach, Marriott had an obligation to disclose the data breach as mandated by V.I Code tit. 14 § 2208.

833. As a direct and proximate result of Marriott's violations of V.I Code tit. 14 §§ 2208(a) and (b), Virgin Islands Subclass members suffered damages, as described above.

834. Virgin Islands Subclass members seek relief under V.I Code tit. 14 §§ 2211(a) and (b), including actual damages, and injunctive relief.

COUNT 79

VIRGIN ISLANDS CONSUMER FRAUD

AND DECEPTIVE BUSINESS PRACTICES ACT,

V.I. Code tit. 12A, §§ 301, *et seq.*

835. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-275, as if fully alleged herein.

836. Marriott is a "person," as defined by V.I. Code tit. 12A, § 303(h).

837. Plaintiff and Virgin Islands Subclass members are "consumers," as defined by V.I. Code tit. 12A, § 303(d).

838. Marriott advertised, offered, or sold goods or services in the Virgin Islands and engaged in trade or commerce directly or indirectly affecting the people of the Virgin Islands.

839. Marriott engaged in unfair and deceptive acts and practices, in violation of V.I. Code tit. 12A, § 304, including: failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virgin Islands Subclass members' Personal Information, which was a direct and proximate cause of the Marriott Data Breach; failing to

identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Marriott Data Breach; failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott Data Breach; misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virgin Islands Subclass members' Personal Information, including by implementing and maintaining reasonable security measures; misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virgin Islands Subclass members' Personal Information; and 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 Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

840. Marriott's acts and practices were "unfair" under V.I. Code tit. 12A, § 304 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

841. The injury to consumers from Marriott's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity. The injury to

consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

842. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

843. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

844. Marriott's acts and practices were "deceptive" under V.I. Code tit. 12A, §§ 303 & 304 because Marriott made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

845. Marriott intended to mislead Plaintiff and Virgin Island Subclass members and induce them to rely on its misrepresentations and omissions.

846. Marriott's representations and omissions were material because they were likely to unfairly influence or deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

847. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virgin Islands Subclass—and Marriott, because

consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its: possession of exclusive knowledge regarding the security of the data in its systems; active concealment of the state of its security; and/or incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

848. Marriott acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiff and Virgin Islands Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate. Marriott intentionally hid the inadequacies in its data security, callously disregarding the rights of consumers.

849. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

850. Marriott's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

851. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory, consequential, treble, punitive, and

equitable damages under V.I. Code tit. 12A, § 331; injunctive relief; and reasonable attorneys' fees and costs.

COUNT 80

VIRGIN ISLANDS CONSUMER PROTECTION LAW,

V.I. Code tit. 12A, §§101, *et seq.*

852. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-275, as if fully alleged herein.

853. Marriott is a "merchant," as defined by V.I. Code tit. 12A, § 102(e).

854. Plaintiff and Virgin Islands Subclass members are "consumers," as defined by V.I. Code tit. 12A, § 102(d).

855. Marriott sells and offers for sale "consumer goods" and "consumer services," as defined by V.I. Code tit. 12A, § 102(c).

856. Marriott engaged in deceptive acts and practices, in violation of V.I. Code tit. 12A, § 101, including: failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virgin Islands Subclass members' Personal Information, which was a direct and proximate cause of the Marriott Data Breach; failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Marriott Data Breach; failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virgin Islands Subclass members' Personal Information, including by implementing and maintaining

reasonable security measures; misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virgin Islands Subclass members' Personal Information; and 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 Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

857. Marriott's acts and practices were "deceptive trade practices" under V.I. Code tit. 12A, § 102(a) because Marriott: represented that goods or services have sponsorship, approval, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have; or that goods or services are of particular standard, quality, grade, style or model, if they are of another; used exaggeration, innuendo or ambiguity as to a material fact or failure to state a material fact if such use deceives or tends to deceive; offered goods or services with intent not to sell them as offered; and stated that a consumer transaction involves consumer rights, remedies or obligations that it does not involve.

858. Marriott's acts and practices were also "deceptive" under V.I. Code tit. 12A, § 101 because Marriott made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

859. Marriott intended to mislead Plaintiff and Virgin Islands Subclass members and induce them to rely on its misrepresentations and omissions.

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

861. Marriott acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Protection Law, and recklessly disregarded Plaintiff and Virgin Island Subclass members' rights. Marriott's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

862. As a direct and proximate result of Marriott's deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

863. Marriott's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

864. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory relief; injunctive relief; the greater of actual damages or $500 per violation; compensatory, consequential, treble, and punitive damages; disgorgement; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT 81

WASHINGTON DATA BREACH NOTICE ACT,

Wash. Rev. Code §§ 19.255.010, *et seq.*

865. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

866. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Wash. Rev. Code § 19.255.010(1).

867. Plaintiff's and Washington Subclass members' Personal Information includes Personal Information as covered under Wash. Rev. Code § 19.255.010(5).

868. Marriott is required to accurately notify Plaintiff and Washington Subclass members following discovery or notification of the breach of its data security system if Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

869. Because Marriott discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

870. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Wash. Rev. Code § 19.255.010(1).

871. As a direct and proximate result of Marriott's violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Washington Subclass members suffered damages, as described above.

872. Plaintiff and Washington Subclass members seek relief under Wash. Rev. Code §§ 19.255.010(13)(a) and 19.255.010(13)(b), including actual damages and injunctive relief.

COUNT 82

WASHINGTON CONSUMER PROTECTION ACT,

Wash. Rev. Code Ann. §§ 19.86.020, *et seq.*

873. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

874. Marriott is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

875. Marriott advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

876. Marriott engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Washington Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Washington Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Washington Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

878. Marriott acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

879. Marriott's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the millions of Washingtonians affected by the Marriott Data Breach.

880. As a direct and proximate result of Marriott's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

881. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS

COUNT 83

NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION, Wis. Stat. §§ 134.98(2), *et seq.*

882. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

883. Marriott is a business that maintains or licenses Personal Information as defined by Wis. Stat. § 134.98(2).

884. Plaintiff's and Wisconsin Subclass members' Personal Information include that which is covered under Wis. Stat. § 134.98(1)(b).

885. Marriott is required to accurately notify Plaintiff and Wisconsin Subclass members if it knows that Personal Information in its possession has been acquired by a person

whom it has not authorized to acquire the Personal Information within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

886. Because Marriott knew that Personal Information in its possession had been acquired by a person whom it has not authorized to acquire the Personal Information, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

887. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Wis. Stat. § 134.98(2).

888. As a direct and proximate result of Marriott's violations of Wis. Stat. § 134.98(3)(a), Plaintiff and Wisconsin Subclass members suffered damages, as described above.

889. Plaintiff and Wisconsin Subclass members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

COUNT 84

WISCONSIN DECEPTIVE TRADE PRACTICES ACT,

Wis. Stat. § 100.18

890. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

891. Marriott is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

892. Plaintiff and Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

893. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Marriott to members of the public for sale, use, or distribution, Marriott made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

894. Marriott also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

895. Marriott's deceptive acts, practices, plans, and schemes include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Wisconsin Subclass members' Personal Information, which was a direct and proximate cause of the Marriott 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 Marriott Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Marriott Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Wisconsin Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Wisconsin Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

896. Marriott intended to mislead Plaintiff and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

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

898. Marriott had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between

consumers—including Plaintiff and the Wisconsin Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

899. Marriott's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

900. Marriott acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

901. As a direct and proximate result of Marriott's deceptive acts or practices, Plaintiff and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Personal Information; and paying more for Defendant's services than they would have.

902. Marriott had an ongoing duty to all Marriott customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

903. Plaintiff and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

CLAIMS ON BEHALF OF THE WYOMING SUBCLASS

COUNT 85

COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS,

Wyo. Stat. Ann. §§ 40-12-502(a), *et seq.*

904. The Wyoming Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wyoming Subclass, repeats and alleges Paragraphs 1-275, as if fully alleged herein.

905. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Wyo. Stat. Ann. § 40-12-502(a).

906. Plaintiff's and Wyoming Subclass members' Personal Information includes that which is covered under Wyo. Stat. Ann. § 40-12-502(a).

907. Marriott is required to accurately notify Plaintiff and Wyoming Subclass members when it becomes aware of a breach of its data security system if the misuse of personal identifying information has occurred or is reasonably likely to occur, in the most expedient time possible and without unreasonable delay under Wyo. Stat. Ann. § 40-12-502(a).

908. Because Marriott was aware of a breach of its data security system in which the misuse of personal identifying information has occurred or is reasonably likely to occur, Marriott had an obligation to disclose the Marriott Data Breach in a timely and accurate fashion as mandated by Wyo. Stat. Ann. § 40-12-502(a).

909. By failing to disclose the Marriott Data Breach in a timely and accurate manner, Marriott violated Wyo. Stat. Ann. § 40-12-502(a).

910. As a direct and proximate result of Marriott's violations of Wyo. Stat. Ann. § 40-12-502(a), Plaintiff and Wyoming Subclass members suffered damages, as described above.

911. Plaintiff and Marriott Subclass members seek relief under Wyo. Stat. Ann. § 40-12-502(f), including actual damages and equitable relief.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Marriott, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint the undersigned as Plaintiffs' Co-Lead Counsel;
2. That the Court grant permanent injunctive relief to prohibit Marriott from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. That the Court award Plaintiffs and Class and Subclass members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;
4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Marriott as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

7. That the Court award pre- and post-judgment interest at the maximum legal rate; and

8. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: January 9, 2019

Respectfully submitted,

/s/ James P. Ulwick
James P. Ulwick (Fed. Bar No. 00536)
KRAMON & GRAHAM PA
One South Street, Suite 2600
Baltimore, Maryland 21202
Telephone: (410) 752-6030
Facsimile: (410) 539-1269
julwick@kg-law.com

Melissa H. Maxman (Fed. Bar No. 86838)
Erica Lai (to file *pro hac vice)*
COHEN & GRESSER LLP
2001 Pennsylvania Avenue, NW, Suite 300
Washington, DC 20006
Telephone: (202) 851-2071
mmaxman@cohengresser.com
elai@cohengresser.com

Andrew N. Friedman (Fed. Bar No. 14421)
Douglas J. MacNamara (to file *pro hac vice)*
Sally Handmaker Guido (to file *pro hac vice)*
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW, Suite 500
Washington, D.C. 20005
Telephone: (202) 408-4600
afriedman@cohenmilstein.com
dmcnamara@cohenmilstein.com
sguido@cohenmilstein.com

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

James J. Pizzirusso (to file *pro hac vice)*
Steven Nathan (to file *pro hac vice)*
Megan E. Jones (Fed. Bar No. 15671)
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, D.C. 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeld.com
snathan@hausfeld.com
mjones@hausfeld.com

Counsel for Plaintiffs and the Putative Class Members