IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

DAVID ORR, HENRY CHAMBERLAIN, ANGELA MICKEL, and JENNIFER GRADY individually and on behalf of all others similarly situated, Plaintiffs, v. INTERCONTINENTAL HOTELS GROUP, PLC, INTER-CONTINENTAL HOTELS CORPORATION, and INTERCONTINENTAL HOTELS GROUP RESOURCES, INC., Defendants.	Civil Action No.: 1:17-cv-01622-MHC **CLASS ACTION** **JURY TRIAL DEMANDED**

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs David Orr, Henry Chamberlain, Angela Mickel, and Jennifer Grady ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, and as permitted by Fed. R. Civ. P. 15, hereby bring this Second Amended Class Action Complaint against defendants InterContinental Hotels Group, PLC, Inter-Continental Hotels Corporation, and InterContinental Hotels Group Resources, Inc. (collectively, "Defendants" or "IHG").

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against IHG for its failure to secure and safeguard its customers' personal financial data—credit and debit card information including cardholder name, card number, expiration date, and internal verification code ("Private Information").

2. Based on reports of patterns of unauthorized card use from payment card networks, in December 2016, IHG began investigating a possible security breach affecting some of its locations.

3. On April 14, 2017, IHG sent a letter to Plaintiffs informing them that its investigation "identified signs of the operation of malware designed to access payment card information" at IHG hotels between September 29, 2016, and December 29, 2016 ("Security Breach"). This malware was designed to search for cardholder names, card numbers, expiration dates, and internal verification codes read from the magnetic stripe of payment cards as they were routed through the server of an affected hotel.

4. On information and belief, Plaintiffs' and Class members' Private Information was stolen by hackers when Plaintiffs and Class members used their credit and debit cards at the affected IHG branded hotels during this period. The Security Breach affected at least 1,000 IHG properties.

5. IHG's security failures enabled the hackers to steal Plaintiffs' and Class members' Private Information from within IHG's hotels and subsequently make unauthorized purchases on their credit and debit cards. The failures also put Plaintiffs' and Class members' financial information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiffs and Class members attributable to responding, identifying, and correcting damages that were reasonably foreseeable as a result of IHG's willful and negligent conduct. The hackers continue to use the information they obtained as a result of IHG's inadequate security to exploit and injure Plaintiffs and Class members across the United States.

6. The Security Breach was caused and enabled by IHG's knowing violation of its obligations to abide by best practices and industry standards concerning the security of payment systems. IHG failed to comply with security standards and allowed its customers' financial information to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

7. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class, assert claims for breach of implied contract, negligence, and unjust enrichment, and seek injunctive relief, monetary damages, statutory damages, and

all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

8. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

9. The Court has personal jurisdiction over InterContinental Hotels Group, PLC, because InterContinental Hotels Group, PLC maintains its U.S. headquarters in Dunwoody, Georgia. InterContinental Hotels Group, PLC has significant continuous and pervasive contacts with the State of Georgia.

10. The Court has personal jurisdiction over Inter-Continental Hotels Corporation because Inter-Continental Hotels Corporation maintains its headquarters in Dunwoody, Georgia. Inter-Continental Hotels Corporation has significant continuous and pervasive contacts with the State of Georgia.

11. The Court has personal jurisdiction over InterContinental Hotels Group Resources, Inc. because InterContinental Hotels Group Resources, Inc. maintains its headquarters in Dunwoody, Georgia. InterContinental Hotels Group Resources has significant continuous and pervasive contacts with the State of

Georgia.

12. Venue is proper in this District under 28 U.S.C. §§ 1391 (b)(1), 1391(b)(2), and 1391(d), because a substantial part of the events and omissions giving rise to the claims emanated from activities within this District and InterContinental Hotels Group, PLC, Inter-Continental Hotels Corporation, and InterContinental Hotels Group Resources, Inc. conduct substantial business in this District.

III. PARTIES

Plaintiff Orr

13. David Orr resides in Flowood, Mississippi, and is a citizen of the State of Mississippi. Orr stayed at an affected IHG Holiday Inn in Biloxi, Mississippi from October 14–15, 2016. Orr used his debit card to pay for the stay and had his Private Information exposed as a result of IHG's inadequate security.

14. As a result of the Security Breach, Orr spent time inspecting his debit card statements for fraudulent activity. Orr had to wait seven days for delivery of a new debit card to replace his compromised one. Orr has also suffered from the deprivation of the value of his Private Information and the lost benefit of the bargain.

Plaintiff Chamberlain

15. Henry Chamberlain resides in Kansas City, Kansas, and is a citizen of the State of Kansas. In October of 2016, Chamberlain paid for a hotel stay at an affected IHG Holiday Inn Express in Sevierville, Tennessee. Chamberlain used his debit card to pay for the stay and had his Private Information exposed as a result of IHG's inadequate security.

16. As a result of the Security Breach, Chamberlain experienced fraud on his debit account, resulting in out-of-pocket losses over $3,000. Chamberlain also spent time inspecting his debit card statements for fraudulent activity and making phone calls. Chamberlain has suffered from the deprivation of the value of his Private Information and the lost benefit of the bargain.

Plaintiff Mickel

17. Angela Mickel resides in Newport News, Virginia, and is a citizen of the State of Virginia. Mickel used her prepaid PayPal MasterCard in connection with several stays at affected IHG properties, including a Holiday Inn Express in Hyattsville, Maryland on September 30, 2016, and November 29-30, 2016, a stay at a Holiday Inn in Williamsburg, Virginia on October 25, 2016, and November 1, 2016, a stay at Holiday Inn Express in Largo, Maryland on December 1, 2016, and a stay at a Holiday Inn Express in Greenbelt, Maryland on December 8, 2016.

18. On February 4, 2017, as a result of the Security Breach, Mickel had two fraudulent charges made to her PayPal card. Mickel had to wait seven days for delivery of a new debit card to replace her compromised one. To date, PayPal has refused to accept the charges as fraudulent or reverse them. Mickel spent time inspecting her account for fraudulent activity and making phone calls. Mickel has suffered from the deprivation of the value of her Private Information and the lost benefit of the bargain.

Plaintiff Grady

19. Jennifer Grady resides in Indianapolis, Indiana, and is a citizen of the State of Indiana. Grady used her Discover credit card to reserve rooms at IHG hotels and her Forum Credit Union debit card for actual payment upon checking in.

20. After five hotel stays at affected IHG properties during the period of September 2016 to January 2017, Grady discovered fraud on her debit card on or around January 11, 2017. As a direct result of the fraud, she incurred insufficient funds charges, exceeding $300. Some of these charges remain unreimbursed. Grady also spent time inspecting her debit card statements for fraudulent activity and making phone calls. Grady has suffered from the deprivation of the value of her Private Information and the lost benefit of the bargain.

Defendants

21. InterContinental Hotels Group, PLC is a British company headquartered in Denham, UK. It is a multinational hotel company with over 5,000 hotels worldwide. InterContinental Hotels Group, PLC's brands include Holiday Inn Express, Holiday Inn, Candlewood Suites, Staybridge Suites, Crowne Plaza, Hotel Indigo, and Holiday Inn Resort. InterContinental Hotels Group, PLC's headquarters for the Americas is located in Dunwoody, Georgia.

22. Inter-Continental Hotels Corporation is a Delaware corporation headquartered in Dunwoody, Georgia and is a fully owned subsidiary of InterContinental Hotels Group, PLC.

23. InterContinental Hotels Group Resources, Inc., is a Delaware corporation headquartered in Georgia and is a fully owned subsidiary of InterContinental Hotels Group, PLC.

IV. FACTUAL BACKGROUND

24. IHG uses a payment system to process its customers' credit and debit card payments. In the years preceding IHG's announcement of the Security Breach, several hotel chains caused press releases to be published alerting the public of security breaches at their properties, including Kimpton Hotels, Trump Hotels, Hilton, Mandarin Oriental, White Lodging, Starwood Hotels, and Hyatt.

IHG knew or should have known that its customers' card data was squarely within the crosshairs of hackers. Despite this, IHG failed to take adequate steps to secure the payment systems used in its hotels.

The IHG Security Breach

25. In December of 2016, IHG stated that it was made aware of a pattern of unauthorized charges occurring on payment cards that were used at a "small number of U.S.-based hotel locations," and began an investigation. On February 3, 2017, IHG announced that a security breach affected 12 of its locations. In April of 2017, IHG expanded the number of affected locations to over 1,000 locations and finally issued a data breach notification letter to affected customers.

26. According to IHG, properties that had implemented IHG's point-to-point encrypted Secure Payment Solution prior to September 29, 2016, were not affected by the Security Breach and are not among the over 1,000 locations affected.

27. IHG hotels must adhere to the Payment Card Industry Data Security Standards ("PCI DSS") promulgated by the Payment Card Industry Security Standards Council. These requirements apply to any entity storing, processing, or transmitting cardholder data. Under PCI DSS, IHG was required to protect cardholder data, not store cardholder data beyond the time necessary to authorize a

transaction, implement strong access control measures, regularly monitor and test its network, and ensure maintenance of information security policies. IHG failed to take adequate steps to prevent the installation of malware on its payment system, failed to recognize existing vulnerabilities in its payment system, and failed to detect the Security Breach.

28. Despite IHG's awareness of its data security obligations, IHG's treatment of Private Information entrusted to it by its customers fell far short of satisfying IHG's legal duties and obligations, and included violations of the PCI DSS. IHG failed to ensure that access to its data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

29. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of

reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[1]

30. In 2016, the Federal Trade Commission ("FTC") updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[2] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

31. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to

[1] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 10, 2017).
[2] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 10, 2017).

sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[3]

32. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

33. In this case, IHG was at all times fully aware of its obligation to protect the Private Information of IHG's customers because of its participation in payment card processing networks. IHG was also aware of the significant repercussions if it failed to do so because IHG collected payment card data from tens of thousands of customers daily at its hotels and IHG knew that this data, if hacked, would result in injury to consumers, including Plaintiffs and Class members.

[3] FTC, *Start With Security*, *supra* note 38.

34. As a result of IHG's failure to adhere to industry and government standards for the security of card data, Private Information of thousands of IHG guests, including Plaintiffs, was compromised over a time period spanning several months.

Security Breaches Lead to Identity Theft

35. According the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[4]

36. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[5] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[6]

---

[4] See *Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited May 3, 2017).

[5] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited May 3, 2017).

[6] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official

37. Private Information—which includes Plaintiffs' and Class members' names combined with their credit or debit card information that were stolen in the Security Breach at issue in this action—is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[7] As a result of recent large scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers and other Private Information directly on various Internet websites, making the information publicly available.

38. In fact, "[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud."[8]

The Monetary Value of Privacy Protections and Private Information

39. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman

---

State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

[7] Companies, in fact, also recognize Private Information as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PERSONAL INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

[8] *One in Four that Receive Data Breach Letters Affected By Identity Theft*, available at http://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/ (last visited May 3, 2017).

> [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[9]

40. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[10]

41. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[11]

42. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And,

---

[9] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at ttps://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited May 3, 2017).

[10] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited May 3, 2017).

[11] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited May 3, 2017).

by making the transaction transparent, consumers will make a profit from their Private Information.[12] This business has created a new market for the sale and purchase of this valuable data.[13]

43. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[14]

44. The value of Plaintiffs' and Class members' Private Information on the black market is substantial. Credit card numbers range in cost from $1.50 to $90 per card number.[15] By way of the Security Breach, IHG has deprived Plaintiffs and Class members of the substantial value of their Private Information.

45. Given these facts, any company that transacts business with consumers and then compromises the privacy of consumers' Private Information has thus

[12] Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited May 3, 2017).

[13] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited May 3, 2017).

[14] See Department of Justice, *Victims of Identity Theft, 2014*, at 6 (2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited May 3, 2017).

[15] *The Cyber Black Market: What's Your Bank Login Worth*, available at https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/ (last visited May 3, 2017).

deprived that consumer of the full monetary value of the consumer's transaction with the company.

Damages Sustained by Plaintiffs and Class Members

46. A portion of the services purchased from IHG by Plaintiffs and the other Class members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of Private Information, including their credit and debit card information. On information and belief, the cost to IHG of collecting and safeguarding Private Information is built into the price of all of its services. Because Plaintiffs and the other Class members were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the other Class members incurred actual monetary damages in that they overpaid for their hotel stays.

47. Plaintiffs and other members of the Class have suffered additional injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Private Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market—for which they are entitled to compensation.

48. Plaintiffs and the other Class members suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend to monitor their financial accounts as a result of the Security Breach. Such damages also include the time and costs of obtaining replacement credit and debit cards.

49. Acknowledging the damage to Plaintiffs and Class members, IHG is instructing customers who used their card at affected locations to take certain cautionary steps. Credit and debit card users should review their accounts for unauthorized transactions and notify their banks immediately if they discover any unauthorized purchases or cash advances. Plaintiffs and the other Class members now face a greater risk of identity theft.

V. CLASS ACTION ALLEGATIONS

50. Plaintiffs bring all counts, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class defined as:

> All persons who used their credit, debit, or prepaid debit card at a hotel and time period identified by IHG as being affected by the security breach that occurred from September 29, 2016, to and including December 29, 2016, including all persons who received a letter from IHG describing the exposure of their payment card information in this breach.

Excluded from the Class are Defendants and their affiliates, parents, subsidiaries,

employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

51. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

52. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number in the thousands. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from IHG's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, or publication.

53. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether IHG failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and

Class members' Private Information;

b. Whether IHG properly implemented its purported security measures to protect Plaintiffs' and Class members' Private Information from unauthorized capture, dissemination, and misuse;

c. Whether IHG took reasonable measures to determine the extent of the Security Breach after it first learned of same;

d. Whether IHG's conduct constitutes breach of an implied contract;

e. Whether IHG willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Private Information;

f. Whether IHG was negligent in failing to properly secure and protect Plaintiffs' and Class members' Private Information;

g. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

54. IHG engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other Class members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

55. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other

things, all Class members were comparably injured through IHG's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to IHG that are unique to Plaintiffs.

56. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

57. **Insufficiency of Separate Actions—Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated consumers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for IHG. The Class thus satisfies

the requirements of Fed. R. Civ. P. 23(b)(1).

58. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against IHG, so it would be impracticable for Class members to individually seek redress for IHG's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS

COUNT I
Breach of Implied Contract
(Against All Defendants)

59. Plaintiffs incorporate the preceding paragraphs as if fully set forth

herein.

60. IHG's customers who intended to make payments at IHG hotels with debit or credit cards were required to provide their credit or debit cards.

61. In providing such financial data, Plaintiffs and the other members of the Class entered into an implied contract with IHG, whereby IHG became obligated to reasonably safeguard Plaintiffs' and the other Class members' Personal Information.

62. Under the implied contract, IHG was obligated to not only safeguard the Personal Information, but also to provide Plaintiffs and the other Class members with prompt, adequate notice of any security breach or unauthorized access of said information.

63. IHG breached the implied contract with Plaintiffs and the other members of the Class by failing to take reasonable measures to safeguard their Personal Information.

64. IHG also breached its implied contract with Plaintiffs and the other Class members by failing to provide prompt, adequate notice of the Security Breach and unauthorized access of their Personal Information by hackers.

65. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) improper disclosure of their

Personal Information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Security Breach; (iii) the value of their time spent mitigating the increased risk of identity theft and/or identity fraud; (iv) the increased risk of identity theft; and (v) deprivation of the value of their Personal Information, for which there is a well-established national and international market—for which they are entitled to compensation. At the very least, Plaintiffs and the other Class members are entitled to nominal damages.

COUNT II
Negligence
(Against All Defendants)

66. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

67. IHG owes numerous duties to Plaintiffs and the other members of the Class. These duties include:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Personal Information in its possession;

b. to protect Personal Information in its possession using reasonable and adequate security procedures that are compliant with the PCI-DSS

standards and with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and the other members of the Class of the Security Breach.

68. IHG knew or should have known the risks of collecting and storing Personal Information and the importance of maintaining secure payment systems. IHG knew of the many breaches that targeted other hotel chains in the months before the Security Breach.

69. IHG knew or should have known that its payment systems did not adequately safeguard Plaintiffs' and the other Class members' Personal Information.

70. IHG breached the duties it owes to Plaintiffs and Class members in several ways, including:

a. by failing to implement adequate security systems, protocols and practices sufficient to protect customer Personal Information and thereby creating a foreseeable risk of harm;

b. by failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the data breach; and

c. by failing to timely and accurately disclose to customers that their Personal Information had been improperly acquired or accessed.

71. But for IHG's wrongful and negligent breach of the duties it owed to Plaintiffs and the other Class members, their Personal Information would not have been compromised.

72. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of IHG's negligent conduct.

COUNT III
Unjust Enrichment
(Against All Defendants)

73. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

74. Plaintiffs and the other Class members conferred a monetary benefit on IHG. Specifically, Plaintiffs and the other Class members paid for services provided by IHG and provided IHG with payment information. In exchange, Plaintiffs and the other Class members were entitled to have IHG protect their Personal Information with adequate data security.

75. IHG knew that Plaintiffs and the other Class members conferred a benefit on IHG. IHG profited from Plaintiffs' and the other Class members' purchases and used their Personal Information for business purposes.

76. IHG failed to secure Plaintiffs' and the other Class members' Personal Information and therefore did not provide full compensation for the benefit the Plaintiffs and the other Class members provided. Further, IHG failed to secure the Plaintiffs' and the other Class members' Personal Information and therefore did not provide full compensation for the benefit the Plaintiffs and the other Class members provided. IHG inequitably acquired the Personal Information because it failed to disclose its inadequate security practices.

77. If Plaintiffs and the other Class members knew that IHG would not secure their Personal Information using adequate security, they would not have stayed at IHG hotels.

78. Plaintiffs and the other Class members have no adequate remedy at law.

79. Under the circumstances, it would be unjust for IHG to be permitted to retain any of the benefits that Plaintiffs and the other Class members conferred on it.

80. IHG should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and the other Class members proceeds that it unjustly received from them. In the alternative, IHG should be compelled to refund the amounts that Plaintiffs and the other Class members

overpaid.

COUNT IV
Negligence Per Se
(Against All Defendants)

81. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

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

83. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information their hotels obtained and stored, and the foreseeable consequences of a data breach at a hotel chain as large as IHG, including, specifically, the damages that would result to Plaintiffs and Class members.

84. IHG's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

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

87. As a direct and proximate result of IHG's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and forgone cash back rewards, damages from lost time and effort to mitigate the actual and potential impact of the Security Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the

far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

VII. DEMAND FOR JURY TRIAL

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

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against IHG, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs David Orr, Henry Chamberlain, Angela Mickel, and Jennifer Grady as Class Representatives, and appointing Ben Barnow of Barnow and Associates, P.C. as Lead Counsel for the Class;

B. Ordering IHG to pay actual damages to Plaintiffs and the other members of the Class;

C. Ordering IHG to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

D. Ordering IHG to pay attorneys' fees and litigation costs to Plaintiffs;

E. Ordering IHG to pay both pre- and post-judgment interest on any amounts awarded; and

F. Ordering such other and further relief as may be just and proper.

Date: August 4, 2017 Respectfully submitted,

David Orr, Henry Chamberlain, Angela Mickel, and Jennifer Grady, individually and on behalf of all others similarly situated,

/s/ David J. Worley
David J. Worley
Georgia Bar No. 776665
James M. Evangelista
Georgia Bar No. 707807
EVANGELISTA WORLEY, LLC
8100 A. Roswell Road
Suite 100
Atlanta, GA 30350
Tel: (404) 205-8400
david@ewlawllc.com
jim@ewlawllc.com

Of Counsel:

Ben Barnow
Illinois Bar No. 0118265
(*Pro hac vice*)
Erich P. Schork
Illinois Bar No. 6291153
(*Pro hac vice)*
Anthony L. Parkhill
Illinois Bar No. 6317680
(*Pro hac vice)*
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000
Fax: (312) 641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
aparkhill@barnowlaw.com

Brian K. Herrington
(*Pro hac vice*)
Mississippi Bar No. 10204
HERRINGTON LAW, PA
1520 N. State St.
Jackson, MS 39202
Tel: (601) 208-0013
brian@herringtonlawpa.com

Ranse M. Partin
CONLEY GRIGGS PARTIN LLP
4200 Northside Parkway NW
Building One, Suite 300
Atlanta, GA 30327
Tel: (404) 809-2591
Fax: (404) 467-1166
ranse@conleygriggs.com

John Yanchunis*
Florida Bar Number 324681
Marisa Glassman*
Florida Bar Number 111991
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@forthepeople.com
mglassman@forthepeople.com

Jean Sutton Martin*
North Carolina Bar Number 25703
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road, Suite 225
Wilmington, North Carolina

Telephone: (910) 292-6676
jean@jsmlawoffice.com

Christopher D. Jennings*
Arkansas Bar Number 2006306
JOHNSON VINES PLLC
2226 Cottondale Lane, Suite 210
Little Rock, Arkansas 72202
Telephone: (501) 372-1300
Facsimilie: (888) 505-0909
cjennings@johnsonvines.com

Steven W. Teppler*
Florida Bar Number 14787
ABBOTT LAW GROUP, P.A.
2929 Plummer Cove Road
Jacksonville, FL 32223
Telephone: (904) 292-1111
Facsimile: (904) 292-1220
steppler@abbottlawpa.com

* *pro hac vice* application forthcoming

CERTIFICATE OF SERVICE

I hereby certify that on this date I electronically filed the foregoing **SECOND AMENDED CLASS ACTION COMPLAINT** with the Clerk of Court using the CM/ECF system which will automatically send email notification of such filing to the attorneys of record.

Dated: August 4, 2017

/s/ David J. Worley
David J. Worley