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

GULF COAST BANK & TRUST COMPANY, on behalf of itself and all others similarly situated, Plaintiff, v. INTERCONTINENTAL HOTELS GROUP, PLC, INTER-CONTINENTAL HOTELS CORPORATION, and INTERCONTINENTAL HOTELS GROUP RESOURCES, INC., Defendants.	Civil Action No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Gulf Coast Bank & Trust Company (referred to as "Plaintiff") brings this action on behalf itself and all others similarly situated against Defendants InterContinental Hotels Group, PLC, Inter-Continental Hotels Corporation, and Intercontinental Hotels Group Resources, Inc. (hereinafter collectively referred to as "IHG" or "Defendants"), and states:

NATURE OF THE CASE

1. Plaintiff brings this class action on behalf of financial institutions that suffered, and continue to suffer, financial losses as a result of IHG's conscious failure to take adequate and reasonable measures to protect its point-of-sale ("POS") and computer systems. IHG's actions compromised highly sensitive and uniquely-identifiable Payment Card Data, including but not limited to names, credit and debit card numbers, expiration dates, card verification values ("CVVs"), and other credit and debit card information, damaging such payment cards and the uniquely-identifiable information stored thereon by making such payment cards and information effectively unusable and obsolete. As a result of this property damage, Plaintiff has incurred significant costs to create new payment cards (and new uniquely-identifiable data). Additionally, Plaintiff has suffered damages as a result of having to reimburse its customers for fraudulent charges on their payment card accounts, among other things.

2. Despite the growing threat of computer system intrusion, Defendants systematically failed to comply with industry standards and their statutory and common law duties to protect the Payment Card Data of its customers.

3. Defendants' systemic failure exposed its customers' highly sensitive Payment Card Data from approximately August 1, 2016 to December 29, 2016, and

allowed hackers to steal that data and misuse it for various purposes. The exposure of the Payment Card Data destroyed the usefulness of the payment cards and the information set forth thereon

4. Had Defendants put reasonable processes and procedures in place, they would have had a reasonable chance to prevent the breach. In fact, Defendants' data practices were so deficient that their customers' data was exposed for several months and Defendants failed to detect any issues.

5. The costs and financial harm caused by Defendants' negligent conduct is borne primarily by financial institutions, like Plaintiff, that issued the payment cards compromised and rendered useless in this data breach. These costs include, but are not limited to, expenses associated with cancelling and reissuing compromised cards, creating new uniquely-identifiable information, and reimbursing their customers and/or members for fraudulent charges.

6. Accordingly, Plaintiff, on behalf of itself and all others similarly situated, asserts claims for negligence, negligence *per se*, and declaratory and injunctive relief.

JURISDICTION AND VENUE

7. This Court has original jurisdiction of this Action pursuant to the Class Action Fairness Act, 28 U.S.C §1332 (d)(2). The matter in controversy, exclusive

of interest and costs, exceeds the sum or value of $5,000,000 and at least some members of the proposed Class have a different citizenship from Defendant. There are more than 100 putative class members.

8. This Court has personal jurisdiction over Defendant InterContinental Hotels Group, PLC because it maintains its U.S. headquarters in Atlanta, Georgia. Defendant InterContinental Hotels Group, PLC regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

9. This Court has personal jurisdiction over Defendant Inter-Continental Hotels Corporation because it maintains its headquarters in Atlanta, Georgia. Defendant Inter-Continental Hotels Corporation regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

10. This Court has personal jurisdiction over Defendant InterContinental Hotels Group Resources, Inc. because it maintains its headquarters in Atlanta, Georgia. Defendant InterContinental Hotels Group Resources, Inc. regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

11. Venue is proper under 28 U.S.C. § 1391 because Defendants reside in this District, regularly transact business in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

12. Plaintiff Gulf Coast Bank & Trust Company is a Louisiana-chartered bank with its headquarters located in New Orleans, Louisiana. As a result of the IHG Data Breach, Plaintiff Gulf Coast Bank & Trust Company has suffered, and continues to suffer, property damage and other injury, including *inter alia*, costs to replace payment cards and uniquely-identifiable information damaged and rendered useless in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

13. Defendant 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 Atlanta, Georgia.

14. Defendant Inter-Continental Hotels Corporation is a Delaware corporation with its headquarters located in Atlanta, Georgia. Inter-Continental Hotels Corporation is a fully owned subsidiary of Defendant InterContinental Hotels Group, PLC.

15. Defendant InterContinental Hotels Group Resources, Inc. is a Delaware corporation with its headquarters located in Atlanta, Georgia. InterContinental Hotels Group Resources, Inc. is a fully owned subsidiary of Defendant InterContinental Hotels Group, PLC.

FACTUAL BACKGROUND

16. It is well known that customer Payment Card Data is valuable and often targeted by hackers. Yet, despite the increasing (and highly publicized) occurrences of data breaches of retailers and hotels, IHG refused to adequately protect its computer systems from intrusion.

17. On December 28, 2016, news sources reported that a data breach had likely occurred at IHG.[1] The reports were based upon information from fraud experts at various financial institutions who noticed a pattern of fraud on customer credit and debit cards that had been used at IHG properties. When contacted by KrebsOnSecurity, IHG acknowledged that it had received similar reports and that it was conducting an investigation.

[1] *Holiday Inn Parent IHG Probes Breach Claims*, KREBS ON SECURITY (Dec. 28, 2016), https://krebsonsecurity.com/2016/12/holiday-inn-parent-ihg-probes-breach-claims/ (last visited January 26, 2018).

18. On or around this time, IHG issued a statement that it was "aware of a report of unauthorized charges occurring on some payment cards that were recently used at a small number of U.S.-based hotel locations."

19. On February 3, 2017 (more than *five weeks* after public news reports surfaced, and even longer since IHG was first made aware of the data breach), IHG publicly acknowledged that a data breach occurred. IHG assured the general public that only a dozen properties were impacted.[2]

20. On April 14, 2017, IHG issued a statement expanding the number of affected locations from a dozen to over 1,000 IHG-branded hotel locations.

21. The breach of Defendants' data systems occurred through Defendants' POS network, where hackers installed malware that allowed them to steal payment card data from remote locations as a card was swiped for payment.

22. The breach was made possible because Defendants disregarded the security of their POS network and the potential danger of a data breach, and failed to put in place reasonable systems and procedures to prevent the harm that their actions have caused.

[2] *IHG Notifies Guests of Payment Card Incident at 12 Properties in the Americas*,, (Feb. 03, 2017), http://www.prnewswire.com/news-releases/ihg-notifies-guests-of-payment-card-incident-at-12-properties-in-the-americas-300401996.html (last visited January 26, 2018).

23. Defendants knew the danger of not safeguarding their POS network as various high profile data breaches have occurred in the same way, including data breaches of Target, Home Depot, Wendy's, Trump Hotels, Hilton, and Mandarin Oriental. Indeed, IHG knew of the risk of a data breach of its own systems, especially since one of its own hotel chains, Kimpton Hotels, experienced a data breach in early 2016.

24. Despite this knowledge, Defendants acted unreasonably and failed to adequately and reasonably protect the data of their customers.

25. Defendants' failure is particularly egregious because various state and federal statutes obligate Defendants to act reasonably in protecting the data of their customers.

26. First, the payment card industry (MasterCard, VISA, Discover, and American Express), long before the beach of Defendants' data systems, issued Card Operating Regulations that: (1) are binding on Defendants; (2) required Defendants to protect cardholder data and prevent its unauthorized disclosure; (3) prohibited Defendants from storing such data, even in encrypted form, longer than necessary to process the transaction; and (4) mandated Defendants to comply with industry standards.

27. Second, the payment card industry set rules requiring all businesses, including Defendants, to upgrade to new card readers that accept EMV chips. EMV chip technology uses imbedded computer chips instead of magnetic stripes to store payment card data. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the hackers making it much more difficult for criminals to profit from what is stolen.

28. The set deadline for businesses to transition their systems from magnetic-stripe to EMV technology was October 1, 2015, a deadline Defendants, on information and belief, did not meet.

29. Under the Card Operating Regulations that are binding on Defendants, businesses accepting payment cards but not meeting the October 1, 2015 deadline agree to be liable for damages resulting from any data breaches.

30. Third, the Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Data Security Standard ("PCI DSS"). PCI DSS is the industry standard

governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.

31. PCI DSS 3.1, the version of the standards in effect at the time of the data breach, sets forth detailed and comprehensive requirements that must be followed to meet each of the following twelve "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

32. Among other things, PCI DSS required Defendants to: properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data on a need-to-know basis; establish a process to identify and timely fix security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and encrypt payment card data at the point of sale.

33. Fourth, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

34. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. 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 for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying 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.

35. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

36. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

37. Fifth, several states have enacted data breach statutes that require merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code § 1798.81.5(b) and Wash. Rev. Code § 19.255, or that otherwise impose data security obligations on merchants, such as Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64. States have also adopted unfair and deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. Moreover, most states have enacted statutes requiring merchants to provide notice if their data security systems are breached. These statutes, implicitly or explicitly, support the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

38. Defendants' failure to employ practices and procedures reasonably capable of securing the cardholder data of the customers of Plaintiff and the Class violated all of these statutory- and industry-imposed obligations and caused substantial damage to Plaintiff and Class members.

39. Indeed, the fact that cardholder data was left exposed for several months and the fact that Defendant continuously failed to detect this vulnerability demonstrates its complete lack of procedural and other safeguards with respect to its customers' data.

40. Plaintiff and Class members were required to act immediately to mitigate the massive fraudulent transactions being made on payment card accounts, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but Plaintiff and Class members are not. Financial institutions, like Plaintiff, bear primary responsibility for reimbursing members for fraudulent charges on the payment cards they issue.

41. As a result of the Defendants' data breach, the payment cards (and the uniquely-identifiable information contained thereon) created and issued by Plaintiff and Class members have been effectively destroyed and rendered useless. Plaintiff has been forced to create new uniquely-identifiable information and new payment cards, change or close accounts, notify customers that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect itself and its customers. Plaintiff also lost interest and transaction fees due to reduced card usage.

42. The financial damages suffered by Plaintiff and Class members are massive and continue to increase.

43. As a result of the data breach, Plaintiff and Class members suffered and continue to suffer losses related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as cancelling compromised cards and creating and mailing to customers new payment cards with new uniquely-identifiable data.

CLASS ALLEGATIONS

44. Plaintiff brings this action on behalf of itself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seeks certification of the following Class:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases from Defendants while malware was installed on its payment card systems.

45. Excluded from the Class are Defendants and its subsidiaries and affiliates; all employees of Defendants; all persons who make a timely election to be

excluded from the Class; government entities; and the judge to whom this case is assigned and his/her immediate family and his/her court staff.

46. **Numerosity**: All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

47. **Commonality and Predominance**: All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3)'s predominance requirement are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. Whether Defendants engaged in the misconduct alleged;

b. Whether Defendants owed a duty to Plaintiff and Class members and whether Defendants violated that duty;

c. Whether Plaintiff and Class members were injured and suffered damages or other ascertainable loss as a result of Defendants' conduct; and

d. Whether Plaintiff and Class members are entitled to relief and the measure of such relief.

48. **Typicality**: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having issued payment cards that were compromised in the data breach of Defendants' data systems. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendants' conduct.

49. **Adequacy**: All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representatives because it is a members of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to represent. Plaintiff is committed to pursuing this matter for the Class with the Class' collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type, and Plaintiff intends to prosecute this action vigorously. Plaintiff and its counsel will fairly and adequately protect the Class' interests.

50. **Superiority**: The superiority requirement of Fed. R. Civ. P. 23(b)(3) is satisfied. 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 Plaintiff and the other Class members are relatively small

compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' 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, economies of scale, and comprehensive supervision by a single court.

51. **Injunctive and Declaratory Relief**: All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CHOICE OF LAW

52. IHG's actions and omissions discussed herein were orchestrated and implemented at their corporate headquarters in Georgia and the tortious and deceptive actions complained of occurred in, and radiated from Georgia.

53. The key wrongdoing at issue in this litigation (IHG's failure to employ adequate data security measures) emanated from IHG's headquarters in Georgia.

54. IHG's principle executive offices, as well as POS system and IT personnel, operate out of, and are located at, IHG's headquarters in Georgia.

55. Georgia, which seeks to protect the rights and interests of Georgia and other U.S businesses against a company doing business in Georgia, has a greater interest in the claims of Plaintiff and Class members than any other state and is most intimately concerned with the outcome of this litigation.

56. Application of Georgia law to a nationwide Class, with respect to the claims asserted herein, is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiff and the nationwide Class.

57. The locations where Plaintiff was injured were fortuitous and IHG could not have foreseen where the injury would take place, as IHG did not know which financial institutions its customers used and the location of these institutions' headquarters, or principal places of business, at the time of the breach.

COUNT I
Negligence

58. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

59. Defendants owed a duty to Plaintiff and the Class to take reasonable care in cardholder data, and to timely notify Plaintiff in the case of a data breach. This duty arises from multiple sources.

60. Defendants have a common law duty to prevent the foreseeable risk of harm to others, including Plaintiff and the class. The duty to protect others against the risk of foreseeable criminal conduct has been recognized in situations in which the parties are in a special relationship, or where an actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk. *See* Restatement (Second) of Torts, § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard PII, Payment Card Data, and other sensitive information.

61. At common law, Defendants owed a duty to Plaintiff and the Class because it was foreseeable that Defendants' data systems and the cardholder data those data systems processed would be targeted by hackers. It also was foreseeable that such hackers would extract cardholder data from Defendants' systems and misuse that information to the detriment of Plaintiff and the Class, and that Plaintiff and the Class would be forced to mitigate such fraud or such potential fraud by cancelling and reissuing payment cards to their customers and reimbursing their customers for fraud losses.

62. Defendants' common law duty also arises from the special relationship that existed between Defendants and the Class. Plaintiff and the Class entrusted Defendants with the cardholder data contained on the payment cards Plaintiff and the Class issued to their customers. Defendants, as the holders and processors of that information, were the only parties who realistically could ensure that their data systems were sufficient to protect the data they were entrusted to hold.

63. In addition to the common law, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, further mandated Defendants to take reasonable measures to protect the cardholder data. Section 5 prohibits unfair practices in or affecting commerce, which requires and obligates Defendants to take reasonable measures to protect any cardholder data Defendants may hold or process. The FTC publications and data security breach orders described above further form the basis of Defendants' duty. In addition, individual states have enacted statutes based upon the FTCA that also created a duty.

64. Defendants are also obligated to perform their business operations in accordance with industry standards, including the PCI DSS, to which Defendants are bound. The industry standards create yet another source of obligations that mandate Defendants to exercise reasonable care with respect to Plaintiff and the Class.

65. Defendants, by their actions, have breached their duties to Plaintiff and the Class. Specifically, Defendants failed to act reasonably in protecting the cardholder data of the customer of Plaintiff and the Class, and did not have reasonably adequate systems, procedures and personnel in place to reasonably prevent the disclosure and theft of the cardholder data belonging to Plaintiff and the Class members.

66. Upon information and belief, the specific negligent acts and omissions committed by Defendants include, but are not limited to, some or all of the following:

a. failure to delete cardholder information after the time period necessary to authorize the transaction;

b. failure to employ systems to protect against malware;

c. failure to regularly update its antivirus software;

d. failure to maintain an adequate firewall;

e. failure to track and monitor access to their network and cardholder data;

f. failure to limit access to those with a valid purpose;

g. failure to encrypt cardholder data at the point-of-sale;

h. failure to transition to the use of EMV technology;

i. failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

j. failure to assign a unique ID to each individual with access to their systems;

k. failure to automate the assessment of technical controls and security configuration standards;

l. failure to adequately staff and fund their data security operation;

m. failure to use due care in hiring, promoting, and supervising those responsible for their data security operations;

n. failure to recognize red flags signaling that Defendants' systems were inadequate, and that as a result, the potential for a massive data breach was increasingly likely;

o. failure to recognize that hackers were stealing Customer Data from their network while the data breach was taking place; and

p. failure to disclose the data breach in a timely manner.

67. In connection with the conduct described above, Defendants acted wantonly, recklessly, and with complete disregard for the consequences.

68. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class have suffered and continue to suffer property damage and injury, including

but not limited to the effective destruction of the usefulness of the relevant payment cards and the uniquely-identifiable information contained thereon, as well as the costs associated with cancelling and reissuing payment cards (with new uniquely-identifiable data), changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage resulting from the breach.

COUNT II
Negligence *Per Se*

69. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

70. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, restaurants and other businesses such as Defendants of failing to use reasonable measures to protect cardholder data. The FTC publications and orders described above also form the basis of Defendants' duty.

71. Defendants violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect cardholder data and not complying

with applicable industry standards, including PCI DSS as described in detail previously in this complaint. Defendants' conduct was particularly unreasonable given the nature and amount of cardholder data it obtained and stored and the foreseeable consequences of a data breach at a national restaurant, including specifically the immense damages that would result to consumers and financial institutions.

72. Defendants' violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence *per se*.

73. Plaintiff and the Class members are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, Plaintiff and many Class members are credit unions, which are organized as cooperatives whose members are consumers.

74. Moreover, the harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty 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 suffered by Plaintiff and the Class members.

75. As a direct and proximate result of Defendants' negligence *per se*, the Plaintiff and the Class have suffered and continue to suffer property damage and injury, including but not limited to the effective destruction of the usefulness of the relevant payment cards and the uniquely-identifiable information contained thereon, as well as the costs associated with cancelling and reissuing payment cards (with new uniquely-identifiable data), changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage resulting from the breach.

COUNT III
Declaratory and Injunctive Relief

76. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

77. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

78. An actual controversy has arisen in the wake of the data breach at issue regarding Defendants' common law and other duties to act reasonably with respect to safeguarding the cardholder data of the customers of Plaintiff and the Class. Plaintiff alleges Defendants' actions in this respect were inadequate and unreasonable and Defendants deny such allegations. Additionally, Plaintiff continues to suffer injury as additional fraud and other illegal charges are being made on payment cards Plaintiff and the Class members have issued.

79. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed and continue to owe a legal duty to secure their customers' personal and financial information—specifically including information pertaining to credit and debit cards used by persons who made purchases at Defendants' properties—and to notify financial institutions of a data breach under the common law, Section 5 of the FTCA, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

b. Defendants breached this legal duty by failing to employ reasonable measure to secure their customers' personal and financial information;

c. Defendants' breach of their legal duty proximately caused the data breach; and

d. Banks, credit unions, and other institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Defendants' data breach are legally entitled to recover the costs they incurred from Defendants.

80. The Court also should issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to protect their customers' personal and financial information. Specifically, this injunction should, among other things, direct Defendants to:

a. utilize industry standard encryption to encrypt transmission of cardholder data at the point-of-sale and at all other times;

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

d. consistent with industry standards, engage third party auditors to test their systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test their systems for security vulnerabilities, consistent with industry standards;

g. comply with all PCI DSS standards pertaining to the security of their customers' personal and confidential information; and

h. install all upgrades recommended by manufacturers of security software and firewalls used by Defendants.

81. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Defendants' data systems. The risk of another such breach is real, immediate, and substantial. If another breach of Defendants' data systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Plaintiff will be forced to bring multiple lawsuits to rectify the same conduct.

82. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendants suffer another massive data breach, Plaintiff and the Class members will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable data security measures is relatively minimal and Defendants have a pre-existing legal obligation to employ such measures.

83. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and on behalf of the other members of the Class, respectfully requests that the Court:

a. Certify the Class and designating Plaintiff as the Class Representative and their counsel as Class Counsel;

b. Award Plaintiff and the proposed Class members damages with pre-judgment and post-judgment interest;

c. Enter a declaratory judgment in favor of Plaintiff and the Class as described above;

d. Grant Plaintiff and the Class the injunctive relief requested above;

e. Award attorneys' fees and costs; and

f. Award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial for all of the claims so triable.

Dated: January 26, 2017

s/ Charles H. Van Horn
Charles H. Van Horn
Georgia Bar No. 724710
BERMAN FINK VAN HORN P.C.
3475 Piedmont Road, NE Suite 1100
Atlanta, GA 30305
Telephone: (404) 261-7711
Facsimile: (404) 233-1943
cvanhorn@bfvlaw.com

Arthur M. Murray
Caroline T. White
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Telephone: (504) 525-8100
Facsimile: (504) 584-5249
amurray@murray-lawfirm.com
cthomas@murray-lawfirm.com

Gary F. Lynch
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 253-6307
Facsimile: (412) 322-9243
glynch@carlsonlynch.com

Attorneys for Plaintiff

JS44 (Rev. 6/2017 NDGA)

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

Gulf Coast Bank & Trust, on behalf of itself and all others similarly situated

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Orleans Parish, LA
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

Intercontinental Hotels Group, PLC, Inter-Continental Hotels Corporation, and Intercontinental Hotels Group Resources, Inc.

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Fulton, GA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

Charles H. Van Horn, Berman Fink Van Horn P.C.
3475 Piedmont Road N.E., Suite 1100
Atlanta, Georgia 30305
(404) 261-7711

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ☐ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☑ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☐ 2	☐ 2	CITIZEN OF ANOTHER STATE	☑ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. ORIGIN (PLACE AN "X "IN ONE BOX ONLY)

- ☑ 1 ORIGINAL PROCEEDING
- ☐ 2 REMOVED FROM STATE COURT
- ☐ 3 REMANDED FROM APPELLATE COURT
- ☐ 4 REINSTATED OR REOPENED
- ☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Negligence - Subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. 1332(d)

(IF COMPLEX, CHECK REASON BELOW)

- ☑ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☑ 4. Greater than normal volume of evidence.
- ☑ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☑ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☑ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☐ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☑ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** 5,000,000+

JURY DEMAND ☑ **YES** ☐ **NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE_____ **DOCKET NO.**_____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

- ☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

/s/ Charles H. Van Horn — 1/26/2018

SIGNATURE OF ATTORNEY OF RECORD **DATE**