

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

TERESA J. McGARRY, on behalf of
herself and all others similarly situated,

Plaintiff,

v.

DELTA AIR LINES, INC., and
[24]7.AI,

Defendants.

CIVIL ACTION FILE

NO. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

COMPLAINT

1. Plaintiff Teresa J. McGarry brings this action individually and on behalf of all others similarly situated (the “Class” as more fully defined below) against Delta, and [24]7.ai to recover monetary damages, injunctive relief, and other remedies for violations of state statutes and the common law. Plaintiff alleges the following on information and belief, except that Plaintiff’s allegations as to her own actions are based on personal knowledge.

I. INTRODUCTION

2. This action arises from a data breach involving Delta Air Lines, Inc. (“Delta”) customers whose sensitive personal identification and payment card

information was hacked and accessed for a period of weeks in September and October 2017. According to Delta, Delta and its third-party vendor, [24]7.ai, who, along with Delta collected customers' personal identification and financial information ("Personal Information" or "PII") to make travel bookings, suffered a malware attack which allowed customer information to be accessed by hackers. Delta and [24]7.ai's conduct following the breach only compounded the injury to Plaintiff and the Class. Despite the hack occurring six months prior, Delta customers were not notified of the breach of their sensitive information until April 2018. Their PII was available to hackers for six months without their knowledge. Data thieves had of use customers' PII during this time while Delta customers were totally unaware.

II. PARTIES

3. Plaintiff Teresa J. McGarry ("Plaintiff") is a resident of Florida and booked airline tickets on the Delta website during the time of the breach. Plaintiff received a letter from Delta notifying her of the breach. **See Exhibit A, Letter from Delta to Plaintiff dated April 11, 2018.**

4. Defendant Delta Air Lines, Inc. ("Delta") is a major American airline. Delta is a Delaware limited liability company with a principal place of business at

1030 Delta Boulevard, Atlanta, Georgia 30320. Delta maintains and operates a website where customers can book tickets for airline travel online.

5. Defendant [24]7.ai is a California corporation with its headquarters at 2001 Logic Drive, San Jose, CA 95124. [24]7.ai provides online chat services for Delta and other companies.

III. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over the state law claims asserted here pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from the Defendant and, upon the original filing of this complaint, members of the putative Plaintiff class resided in states around the country; there are more than 100 putative class members; and the amount in controversy exceeds \$5 million.

7. The Court also has personal jurisdiction over the Parties because Defendant Delta is headquartered in Atlanta, GA and conducts a major part of its national operations with regular and continuous business activity in Georgia.

8. Venue is appropriate because, among other things: Delta's principal place of business is located in the District, substantial parts of the events or omissions giving rise to the claim occurred in the District. A substantial part of Plaintiffs' personal and financial information and activities that Delta collected,

obtained, maintained, and allowed to be accessed without authorization during the data breach, occurred in or was found in the District. And, a significant part of the risk of harm that Plaintiff and the Class now face through Delta's wrongful conduct is present in this District. Venue is also proper in the Atlanta Division because Delta is located within the geographical boundaries of this division.

9. Venue is further appropriate pursuant to 28 U.S.C. § 1391 because Defendants conduct a large amount of their business in this District, and Defendants have substantial relationships in this District.

IV. ALLEGATIONS

10. On April 5th Delta announced that its computer systems had been breached and customer information had been accessed. Delta estimated that hundreds of thousands of customers were affected. The type of information that was stolen was credit card information, names and addresses. The breach occurred from September 26 to October 12, 2017. Plaintiff made an online reservation with Delta during the time of the breach. Plaintiff, and hundreds of thousands of other customers, had their credit card information exposed to unauthorized persons and/or entities for months without receiving notification from Delta or [24]7.ai.

11. Plaintiff received a letter from Delta dated April 11, 2018. The letter stated:

We are writing to tell you about a cyber incident involving [24]7.ai, a company that provides online chat services for Delta and many other companies. This incident may have resulted in unauthorized access to payment card information relating to a purchase you made on delta.com. The security and confidentiality of our customers' information is of critical importance to us and a responsibility we take very seriously. We've included in this letter the information we have on the incident as well as instructions to contact the team dedicated to answering your questions should you need additional assistance.

We cannot at this point say definitively whether any of our customers' information was accessed. However, out of an abundance of caution and as part of our commitment to the security of your information, we are partnering with AllClear ID, a leading customer security and fraud protection firm, to offer a suite of identity theft protection and credit monitoring services for two years from the date of this letter at no cost to you. As an eligible customer, you can enroll in this service by calling (855) 815-0534 or visiting delta.allclearid.com.

The latest updates on this incident will be available at delta.com/response.

What Happened

On March 28, 2018, Delta was notified by [24]7.ai, a company that provides online chat services for Delta and many other companies, that [24]7.ai had been involved in a cyber incident. It is our understanding that the incident occurred at [24]7.ai from Sept. 26 to Oct. 12, 2017 and that during this time certain customer payment

information for [24]7.ai clients, including Delta, may have been accessed – no other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.

We understand malware present in [24]7.ai's software between Sept. 26 and Oct. 12, 2017, made unauthorized access possible for the following fields of information when manually completing a payment card purchase on any page of the delta.com desktop platform during the same timeframe: name, address, payment card number, CVV number, and expiration date. There was no impact to the Fly Delta app, mobile delta.com or and Delta computer system.

At this point, even though only a small subset of our customers would have been exposed, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.

Based on our investigation to date, we have determined that the payment card information of customers who completed a purchase on the delta.com desktop platform between Sept. 26, 2017 and Oct. 12, 2017 may have been exposed. Our records indicate that you may have completed such a purchase during this time frame. As a result, information relating to the payment card used for that purchase may have been exposed, including name, address, payment card number, CVV number, and expiration date. No other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.

What We Are Doing

While [24]7.ai recently advised us that the incident was contained and stopped on Oct. 12, 2017, upon learning of the incident, Delta immediately launched an investigation and engaged federal law enforcement and forensic teams. We have also initiated diligent efforts to directly contact customers, including by first-class postal mail, who may have been impacted by the [24]7.ai cyber event.

Delta is committed to protecting your personal information and, out of an abundance of caution, is offering you a paid subscription for AllClear ID credit monitoring and identity theft protection services for two years at no cost to you. Information on how to enroll in these services is included with this notice.

The latest information will be available to you at delta.com/response.

Letter from Delta to Plaintiff dated April 11, 2018, attached hereto as Ex. A.

12. Delta also acknowledged the data breach in its 10-Q for the quarterly period ended March 31, 2018: “Breaches or lapses in the security of our technology systems and the data we store could compromise passenger or employee information and expose us to liability, possibly having a material adverse effect on our business.”

A. Defendants’ Security Protocols Were Insufficient

13. Delta and [24]7.ai (“Defendants”) maintained an insufficient and inadequate system to protect the payment information of Plaintiff and the Class. It

is well known, and the subject of many media reports, that PII is highly coveted and a frequent target of hackers. Despite well-publicized litigation and frequent public announcements of data breaches, Defendants maintained an insufficient and inadequate system to protect the PII of Plaintiff and the Class.

14. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The two years of credit monitoring offered by Delta is insufficient. 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.

B. Plaintiff and the Class Suffered Damages

15. The data breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and Class' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law. The data breach was also a result of Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of

Plaintiff's and Class' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

16. Plaintiff's and Class' PII is private and sensitive in nature and was inadequately protected by Defendants. Defendants did not obtain Plaintiff's and Class' consent to disclose their PII as required by applicable law and industry standards.

17. As a direct and proximate result of Defendants' wrongful action and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing 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 subject data breach on their lives by, among other things, 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.

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

- a. Theft of their PII;
- b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- c. The imminent and impending injury flowing from sale of Plaintiff's and the Class Members' PII on the Internet black market;
- d. The untimely and inadequate notification of the data breach;
- e. The improper disclosure of their PII;
- f. Loss of privacy;
- g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;
- h. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;
- i. Overpayments to Defendants for booking and purchase during the subject data breach in that a portion of the price paid for such booking by Plaintiff and Class to Defendants was for the

costs of reasonable and adequate safeguards and security measures that would protect customers' PII, which Defendants did not implement and, as a result, Plaintiff and Class did not receive what they paid for and were overcharged by Defendants; and

- j. Deprivation of rights they possess under the Unfair Competition Laws.

V. CLASS ACTION ALLEGATIONS

19. Pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert that Defendants are liable for common law claims for negligence, negligence *per se*, bailment, and unjust enrichment, as well as declaratory and injunctive relief, on behalf of themselves and the following nationwide class (the "Nationwide Class" or the "Class"):

All persons residing in the United States who made a reservation or booking with Delta and/or flew with Delta from the time period September 26, 2017 to October 12, 2017 (the "Nationwide Class").

The (the "State Name Class") is initially defined as follows:

All persons residing in (State Name) who made a reservation or booking with Delta and/or flew with Delta from the time period September 26, 2017 to October 12, 2017 (the "State Name Class").

20. Excluded from each of the above Classes are Defendants, including any entity in which Defendants have a controlling interest, are a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

21. **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 Plaintiff at this time, Defendants have estimated that the number is in the hundreds of thousands. **See Ex. A.** The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendants' possession, custody, or control, such as reservation receipts and confirmations.

22. **Commonality.** Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Classes, which predominate over any

questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendants owed a duty of care to Plaintiff and Class with respect to the security of their personal information;
- b. Whether Defendants took reasonable steps and measures to safeguard Plaintiff's and Class' personal information;
- c. Whether Defendants violated State Unfair Competition Laws by failing to implement reasonable security procedures and practices;
- d. Whether Defendants violated common and statutory law by failing to promptly notify the Class that their PII had been compromised;
- e. Which security procedures and which data-breach notification procedure should Defendants be required to implement as part of any injunctive relief ordered by the Court;
- f. Whether Defendants have an implied contractual obligation to use reasonable security measures;
- g. Whether Defendants have complied with any implied contractual obligation to use reasonable security measures;

- h. Whether Defendants' acts and omissions described herein give rise to a claim of negligence;
- i. Whether Defendants knew or should have known of the security breach prior to the disclosure;
- j. Whether Defendants had a duty to promptly notify Plaintiff and the Class that their personal information was, or potentially could be, compromised;
- k. What security measures, if any, must be implemented by Defendants to comply with their implied contractual obligations;
- l. Whether Defendants violated state privacy laws in connection with the acts and omissions described herein;
- m. What the nature of the relief should be, including equitable relief, to which Plaintiff and the Class are entitled; and
- n. Whether Plaintiff and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

23. **Typicality.** Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of the Class because Plaintiff's PII, like that of every other Class Member, was misused and/or disclosed by Defendants without authorization.

24. **Adequacy of Representation.** Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff has retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiff intend to prosecute this action vigorously. Plaintiff's claims are typical of the claims of other members of the Class and Plaintiff has the same non-conflicting interests as the other members of the Class. The interests of the Class will be fairly and adequately represented by Plaintiff and her counsel.

25. **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 Classes is impracticable. Furthermore, the adjudication of this controversy through a class action 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.

26. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied.

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

COUNT I

Breach of Implied Contract (On Behalf of Plaintiff and the Nationwide Class)

28. Plaintiff alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 27, inclusive of this Complaint as if set forth fully herein.

29. Defendants solicited and invited Plaintiff and the members of the Class to make flight and/or other travel related reservations with Delta. Plaintiff and Class Members accepted Defendants' offers and made such reservations with Delta.

30. When Plaintiff and the Class made reservations with Delta, they provided their PII. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised.

31. Each reservation by Plaintiff and Class Members was made pursuant to the mutually agreed-upon implied contract with Defendants under which Defendants agreed to safeguard and protect Plaintiff's and Class Members' PII and to timely and accurately notify them if such information was compromised or stolen.

32. Plaintiff and Class Members would not have provided and entrusted their PII to Defendants in the absence of the implied contract.

33. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

34. Defendants breached the implied contracts they made with Plaintiff and Class Members by failing to safeguard and protect the PII of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the data breach.

35. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants and Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT II

Negligence (On Behalf of Plaintiff and the Nationwide Class)

36. Plaintiff alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 27, inclusive of this Complaint as if set forth fully herein.

37. Upon accepting Plaintiff's and Class Members' PII in their respective systems, Defendants undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure that Plaintiff's and the Class Members' PII was adequately secured and protected.

38. Defendants further had a duty to implement processes that would detect a breach of their security systems in a timely manner and to timely act upon warnings and alerts, including those generated by their own security systems.

39. Defendants owed a duty to Plaintiff and the Class to provide security consistent with industry standards and requirements, to ensure that its computer

systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiff and the other Class members.

40. Defendants knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiff and the Class and of the critical importance of providing adequate security of that information.

41. Defendants breached the duties they owed to Plaintiff and the other Class Members by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal and financial information of Plaintiff and the Class.

42. Defendants breached the duties they owed to Plaintiff and the Class members by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

43. Defendants had a duty to timely disclose to Plaintiff and the Class that their PII had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiff and the Class could take appropriate measures to avoid use of bank funds and monitor their account information and credit reports for fraudulent activity.

44. Defendants' failure to comply with their legal obligations and with industry standards and regulations, and the delay between the date of intrusion and the date Delta disclosed the data breach, further evidence Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the other members of the Class' personal and financial information in Defendants' possession.

45. Defendants knew that Plaintiff and the other Class members were foreseeable victims of a data breach of their systems because of laws and statutes that require Defendants to reasonably safeguard sensitive payment information.

46. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the other Class members, their personal and financial information would not have been compromised.

47. The injury and harm suffered by Plaintiff and members of the Class as set forth above was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' personal and financial information within Defendants' possession. Defendants knew or should have known that their systems and technologies for processing, securing, safeguarding and deleting Plaintiff's and the other Class

members' personal and financial information were inadequate and vulnerable to being breached by hackers.

48. Plaintiff and the other Class members suffered injuries and losses described herein as a direct and proximate result of Defendants' conduct resulting in the data breach, including Defendants' lack of adequate reasonable and industry standard security measures. Had Defendants implemented such adequate and reasonable security measures, Plaintiff and the other Class members would not have suffered the injuries alleged, as the data breach would likely have not occurred.

49. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class have suffered injury and the significant risk of harm in the future, and are entitled to damages in an amount to be proven at trial.

50. Defendants breached their duty to discover and to notify Plaintiff and the Class of the unauthorized access by failing to discover the security breach within reasonable time and by failing to notify Plaintiff and Class Members of the breach until April, 2018. To date, Defendants have not provided sufficient information to Plaintiff and the Class regarding the extent and scope of the unauthorized access and Defendants continue to breach their disclosure obligations to Plaintiff and the Class.

51. Defendants also breached their duty to Plaintiff and Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering its negligent practices, Defendants failed to provide adequate supervision and oversight of the PII, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiff's and Class Members' PII, misuse the PII, and intentionally disclose it to others without consent.

52. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and their failure to protect Plaintiff's and Class' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class' PII during the time it was within Defendants' control.

53. Further, through their failure to timely discover and provide clear notification of the data breach to consumers, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

54. Upon information and belief, Defendants improperly and inadequately safeguarded the PII of Plaintiff and Class Members that deviated from standard industry rules, regulations, and practices at the time of the data breach.

55. Neither Plaintiff nor the other Class Members contributed to the data breach and subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class sustained actual losses and damages as described in detail above.

COUNT III

Bailment (On behalf of Plaintiff and the Nationwide Class)

56. Plaintiff, individually and on behalf of the other Class members, repeats and realleges Paragraphs 1 through 27, as if fully alleged herein.

57. Plaintiff and the other Class members provided, or authorized disclosure of, their PII to Delta for the exclusive purpose of booking airline travel.

58. In allowing their personal and financial information to be made available to Delta, Plaintiff and the other Class members intended and understood that Delta would adequately safeguard their personal and financial information.

59. Delta accepted possession of Plaintiff's and the other Class members' personal and financial information for the purpose of making available to Plaintiff and the other Class members Delta's services for their benefit.

60. By accepting possession of Plaintiff's and the other Class members' personal and financial information, Delta understood that Plaintiff and the other Class members expected Delta to adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Delta owed a duty to Plaintiff and the other Class members to exercise reasonable care, diligence, and prudence in protecting their personal and financial information.

61. Delta breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and the other Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and the other Class members' personal and financial information.

62. Delta further breached its duty to safeguard Plaintiffs' and the other Class members' personal and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the data breach.

63. As a direct and proximate result of Delta's breach of its duty, Plaintiff and the other Class members suffered consequential damages that were reasonably foreseeable to Delta, including but not limited to the damages set forth above.

64. As a direct and proximate result of Delta's breach of its duty, the personal and financial information of Plaintiff and the other Class members entrusted, directly or indirectly, to Delta during the bailment (or deposit) was damaged and its value diminished.

COUNT IV

Unfair and Deceptive Business Practices (On Behalf of Plaintiff and the Class)

65. Plaintiff alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 27, inclusive of this Complaint as if set forth fully herein.

66. Plaintiff brings this Count individually, and on behalf of all similarly situated residents of each of the 50 States and the District of Columbia for violations of the respective statutory consumer protection laws, as follows:

- a. the Alabama Deceptive Trade Practices Act, Ala.Code 1975, § 8-19- 1, et seq.;
- b. the Alaska Unfair Trade Practices and Consumer Protection Act, AS § 45.50.471, et seq seq.;

- c. the Arizona Consumer Fraud Act, A.R.S §§ 44-1521, et seq.;
- d. the Arkansas Deceptive Trade Practices Act, Ark.Code §§ 4-88-101, et seq.;
- e. the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, et seq.;
- f. the Colorado Consumer Protection Act, C.R.S.A. §6-1-101, et seq.;
- g. the Connecticut Unfair Trade Practices Act, C.G.S.A. § 42-110, et seq.
- h. the Delaware Consumer Fraud Act, 6 Del. C. § 2513, et seq.;
- i. the D.C. Consumer Protection Procedures Act, DC Code § 28-3901, et seq.;
- j. the Florida Deceptive and Unfair Trade Practices Act, FSA § 501.201, et seq.;
- k. the Georgia Fair Business Practices Act, OCGA § 10-1-390, et seq.;
- l. the Hawaii Unfair Competition Law, H.R.S. § 480-1, et seq.;
- m. the Idaho Consumer Protection Act, I.C. § 48-601, et seq.;

- n. the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 501/1 et seq.;
- o. the Indiana Deceptive Consumer Sales Act, IN ST § 24-5-0.5-2, et seq.
- p. the Iowa Private Right of Action for Consumer Frauds Act, Iowa Code Ann. § 714H.1, et seq.;
- q. the Kansas Consumer Protection Act, K.S.A. § 50-623, et seq.;
- r. the Kentucky Consumer Protection Act, KRS 367.110, et seq.;
- s. the Louisiana Unfair Trade Practices and Consumer Protection Law, LSA-R.S. 51:1401, et seq.;
- t. the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 205-A, et seq.;
- u. the Maryland Consumer Protection Act, MD Code, Commercial Law, § 13-301, et seq.;
- v. the Massachusetts Regulation of Business Practices for Consumers Protection Act, M.G.L.A. 93A, et seq.;
- w. the Michigan Consumer Protection Act, M.C.L.A. 445.901, et seq.;

- x. the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. § 325F.68, et seq.;
- y. the Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, et seq.
- z. the Missouri Merchandising Practices Act, V.A.M.S. § 407, et seq.;
- aa. the Montana Unfair Trade Practices and Consumer Protection Act of 1973, Mont. Code Ann. § 30-14-101, et seq.;
- bb. the Nebraska Consumer Protection Act, Neb.Rev.St. §§ 59-1601, et seq.;
- cc. the Nevada Deceptive Trade Practices Act, N.R.S. 41.600, et seq.;
- dd. the New Hampshire Regulation of Business Practices for Consumer Protection, N.H.Rev.Stat. § 358-A:1, et seq.;
- ee. the New Jersey Consumer Fraud Act, N.J.S.A. 56:8, et seq.;
- ff. the New Mexico Unfair Practices Act, N.M.S.A. §§ 57-12-1, et seq.;
- gg. the New York Consumer Protection from Deceptive Acts and Practices, N.Y. GBL (McKinney) § 349, et seq.;

- hh. the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, et seq.;
- ii. the North Dakota Consumer Fraud Act, N.D. Cent.Code Chapter 51-15, et seq.;
- jj. the Ohio Consumer Sales Practices Act, R.C. 1345.01, et seq.;
- kk. the Oklahoma Consumer Protection Act, 15 O.S.2001, §§ 751, et seq.;
- ll. the Oregon Unlawful Trade Practices Act, ORS 646.605, et seq.;
- mm. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, et seq.;
- nn. the Rhode Island Deceptive Trade Practices Act, G.L.1956 § 6-13.1-5.2(B), et seq.;
- oo. the South Carolina Unfair Trade Practices Act, SC Code 1976, §§ 39-5-10, et seq.;
- pp. the South Dakota Deceptive Trade Practices and Consumer Protection Act, SDCL § 37-24-1, et seq.;
- qq. the Tennessee Consumer Protection Act, T.C.A. § 47-18-101, et seq.;

- rr. the Texas Deceptive Trade Practices-Consumer Protection Act, V.T.C.A., Bus. & C. § 17.41, et seq.;
- ss. the Utah Consumer Sales Practices Act, UT ST § 13-11-1, et seq.;
- tt. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, et seq.;
- uu. the Virginia Consumer Protection Act of 1977, VA ST § 59.1-196, et seq.;
- vv. the Washington Consumer Protection Act, RCWA 19.86.010, et seq.;
- ww. the West Virginia Consumer Credit And Protection Act, W.Va.Code § 46A-1-101, et seq.;
- xx. the Wisconsin Deceptive Trade Practices Act, WIS.STAT. § 100.18, et seq.; and
- yy. the Wyoming Consumer Protection Act, WY ST § 40-12-101, et seq.

67. Defendants violated the statutes set forth above (collectively, the “Consumer Protection Acts”) by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff’s and Class

Members' PII, and by allowing third parties to access Plaintiff's and Class Members' PII.

68. Defendants further violated the Consumer Protection Acts by failing to disclose to the consumers that its data security practices were inadequate, thus inducing consumers to book flights with Defendants.

69. Defendants' acts and/or omissions constitute fraudulent, deceptive, and/or unfair acts or omissions under the Consumer Protection Acts.

70. Plaintiff and Class Members were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their PII.

71. Defendants' intended for Plaintiff and Class Members to rely on them to protect the information furnished to it in connection with debit and credit card transactions, in such manner that Plaintiff's and Class Members' PII would be protected, secure and not susceptible to access from unauthorized third parties.

72. Defendants instead handled Plaintiff's and Class Members' information in such a manner that it was compromised.

73. Defendants failed to follow industry best practices concerning data security or was negligent in preventing the data breach from occurring.

74. It was foreseeable that Defendants' willful indifference or negligent course of conduct in handling PII it collected would put that information at the risk of compromise by data thieves.

75. On information and belief, Defendants benefited from mishandling the PII of customers, by not taking effective measures to secure this information, and therefore saving on the cost of providing data security.

76. Defendants' fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and Class Members' reliance on Defendants' deception that their PII was secure.

77. Defendants' conduct offends public policy and constitutes unfair acts or practices under the Consumer Protection Acts because Defendants caused substantial injury to Plaintiff and Class Members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

78. Defendants' acts or practice of failing to employ reasonable and appropriate security measures to protect Private Information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a), which the courts consider when evaluating claims under the Consumer Protection Acts, including 815 ILCS 505/2.

79. Defendants' conduct constitutes unfair acts or practices as defined in the Consumer Protection Acts because Defendants caused substantial injury to Plaintiff and Class members, which injury is not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers.

80. Plaintiff and Class Members have suffered injury in fact and actual damages including lost money and property as a result of Defendants' violations of the Consumer Protection Acts.

81. Defendants' fraudulent and deceptive behavior proximately caused Plaintiff's and Class Members' injuries, and Defendants conducted themselves with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

82. Defendants' failure to disclose information concerning the data breach directly and promptly to affected customers, constitutes a separate fraudulent act or practice in violation of the Consumer Protection Acts.

83. Plaintiff seek attorney's fees and damages to the fullest extent permitted under the Consumer Protection Acts.

COUNT V

Negligence *Per Se* (On Behalf of Plaintiff and the Nationwide Class)

84. Plaintiff alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 27, inclusive of this Complaint as if set forth fully herein.

85. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

86. Pursuant to state laws in the following 13 states, Defendants operating in those states had a duty to those respective states' Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Personal Information:

- a. Arkansas: Ark. Code § 4-110-104
- b. California: Cal Civ. Code § 1798.81.5
- c. Connecticut: Conn. Gen. Stat. § 42-471
- d. Florida: Fla. Stat. § 501.171(2)
- e. Georgia: Ga. Code Ann., § 10-1-912
- f. Indiana: Ind. Code § 24-4.9-3.5
- g. Maryland: Md. Code. Comm. Law § 14-5303

- h. Massachusetts: Mass. Gen Laws Ch. 93H, § 3(a)
- i. Nevada: Nev. Rev. Stat. § 603A.210
- j. Oregon: Ore. Rev. Stat. § 646A.622(1)
- k. Rhode Island: R.I. Gen Laws § 11-49.2-2(2)
- l. Texas: Tex. Bus. & Com. Code § 521.052(a)
- m. Utah: Utah Code § 14-44-201(1)(a)

87. Defendants breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and the state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information.

88. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

89. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

90. The injury and harm suffered by Plaintiff and the Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that the

breach would cause Plaintiff and the State Class Members to experience the foreseeable harms associated with the exposure of their PII.

91. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT VI

Breach of the Covenant of Duty of Good Faith and Fair Dealing (On Behalf of Plaintiff and the Nationwide Class)

92. Plaintiff alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 27, inclusive of this Complaint as if set forth fully herein.

93. The law implies a covenant of good faith and fair dealing in every contract.

94. Plaintiff and Class Members contracted with Defendants by accepting Defendants' offers and paying for the booking of flights.

95. Plaintiff and Class Members performed all of the significant duties under their agreements with Defendants.

96. The conditions required for Defendants' performance under the contract has occurred.

97. Defendants did not provide and/or unfairly interfered with and/or frustrated the right of Plaintiff and the Class Members to receive the full benefits under their agreement.

98. Defendants breached the covenant of good faith and fair dealing implied in its contracts with Plaintiff and the Class Members by failing to use and provide reasonable and industry-leading security practices.

99. Plaintiff and the Class Members were damaged by Defendants' breach in that they paid for, but never received, the valuable security protections to which they were entitled, and which would have made their products and services more valuable.

COUNT VII

Violation of State Data Breach Acts (On Behalf of Plaintiff and the State Name Class)

100. Plaintiff alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 27, inclusive of this Complaint as if set forth fully herein.

101. Defendants were required, but failed, to take all reasonable steps to dispose, or arrange for the disposal, of records within their custody or control containing PII when the records were no longer to be retained, by shredding,

erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

102. Defendants' conduct, as alleged above, violated the data breach statutes of many states, including:

- a. California, Cal. Civ. Code §§ 1798.80 et. seq.;
- b. Georgia: Ga. Code Ann., § 10-1-912
- c. Hawaii, Haw. Rev. Stat. § 487N-1-4 (2006);
- d. Illinois, 815 Ill. Comp Stat. Ann. 530/1-30 (2006);
- e. Louisiana, La. Rev. Stat. § 51:3071-3077 (2005), and L.A.C. 16:III.701;
- f. Michigan, Mich. Comp. Laws Ann. §§ 445.63, 445.65, 445.72 (2006);
- g. New Hampshire, N.H. Rev. Stat. Ann. §§ 359-C:19-C:21, 358-A:4 (2006)., 332-I:1-I:610;
- h. New Jersey, N.J. Stat. Ann. § 56:8-163-66 (2005);
- i. North Carolina, N.C. Gen. Stat. §§ 75-65 (2005); as amended (2009);
- j. Oregon, Or. Rev. Stat. §§ 646A.602, 646A.604, 646A.624 (2011);

- k. Puerto Rico, 10 L.P.R.A. § 4051; 10 L.P.R.A. § 4052 (2005), as amended (2008);
- l. South Carolina, S.C. Code § 1-11-490 (2008); S.C. Code § 39-1-90 (2009);
- m. Virgin Islands, 14 V.I.C. § 2208, et seq. (2005);
- n. Virginia, Va. Code Ann. § 18.2-186.6 (2008); Va. Code Ann. § 32.1– 127.1:05 (2011); and
- o. the District of Columbia, D.C. Code § 28-3851 to 28-3853 (2007) (collectively, the “State Data Breach Acts”).

103. Defendants were required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

104. The data breach constituted a “breach of the security system” within the meaning of section 1798.82(g) of the California Civil Code, and other State Data Breach Acts.

105. The information compromised in the data breach constituted “personal information” within the meaning of section 1798.80(e) of the California Civil Code, and other State Data Breach Acts.

106. Like other State Data Breach Acts, California Civil Code § 1798.80(e) requires disclosure of data breaches “in the most expedient time possible and without unreasonable delay.”

107. Defendants violated Cal. Civ. Code § 1798.80(e) and other State Data Breach Acts by unreasonably delaying disclosure of the data breach to Plaintiff and other Class Members, whose PII was, or was reasonably believed to have been, acquired by an unauthorized person.

108. Upon information and belief, no law enforcement agency instructed Defendants that notification to Plaintiff and Class Members would impede a criminal investigation.

109. As a result of Defendants’ violation of State Data Breach Acts, including Cal. Civ. Code § 1798.80, et seq., Plaintiff and Class Members incurred economic damages, including expenses associated with monitoring their personal and financial information to prevent further fraud.

110. Plaintiff, individually and on behalf of the Class, seeks all remedies available under Cal. Civ. Code § 1798.84 and under the other State Data Breach Acts, including, but not limited to: (a) actual damages suffered by Plaintiff and Class Members as alleged above; (b) statutory damages for Defendants’ willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; (c) equitable

relief; and (d) reasonable attorneys' fees and costs under Cal. Civ. Code §1798.84(g).

111. Because Defendants were guilty of oppression, fraud or malice, in that they acted with a willful and conscious disregard of Plaintiff's and Class Members' rights, Plaintiff also seeks punitive damages, individually and on behalf of the Class.

VI. PRAYER FOR RELIEF

112. WHEREFORE, Plaintiff, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendants as follows:

- A. For an Order certifying the Class and State Classes as defined here, and appointing Plaintiff and her Counsel to represent the Class and the State Classes;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Identifiable Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

- C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Plaintiff and Class Members the type of PII compromised.
- D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;
- E. For an award of actual damages and compensatory damages, in an amount to be determined;
- F. For an award of costs of suit and attorney's fees, as allowable by law; and
- G. Such other and further relief as this court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

113. Based on the foregoing, Plaintiff, on behalf of herself, and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated this 7th day of June, 2018.

Respectfully submitted,

CONLEY GRIGGS PARTIN LLP

/s/ Cale Conley

CALE CONLEY
Georgia Bar No. 181080
RANSE M. PARTIN
Georgia Bar No. 556260

4200 Northside Parkway, NW
Building One, Suite 300
Atlanta, Georgia 30327
(404) 467-1155
cale@conleygriggs.com
ranse@conleygriggs.com

To Be Admitted Pro Hac Vice:

KOHN SWIFT & GRAF, P.C.

DENIS F. SHEILS
BARBARA L. GIBSON
1600 Market Street
Suite 2500
Philadelphia, Pennsylvania 19103-7225
(215) 238-1700
dsheils@kohswift.com
bgibson@kohswift.com

**WOLF HALDENSTEIN ADLER FREEMAN
& HERZ LLP**

GREGORY M. NESPOLE
270 Madison Avenue
New York, NY 10016
(212) 545-4600
gmn@whafh.com

**ATTORNEYS FOR PLAINTIFF TERESA J.
MCGARRY AND THE PROPOSED CLASS**