UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DELTA AIR LINES, INC., Plaintiff, v. [24]7.AI, INC. and 24/7 CUSTOMER PHILIPPINES, INC., Defendants.	Civil Action No.: 1:19cv7430 **COMPLAINT** JURY TRIAL DEMANDED

Delta Air Lines, Inc. ("Delta"), by and through its undersigned counsel, for its Complaint against Defendants [24]7.ai, Inc. ("[24]7") and 24/7 Customer Philippines, Inc. ("24/7 Philippines," collectively, "Defendants") allege as follows:

NATURE OF THE ACTION

1. This lawsuit stems from a data breach that occurred as a direct result of Defendants' substandard data security practices maintained in violation of the clear requirements of Defendants' obligations to Delta assumed in connection with Defendants' provision of certain technology services to Delta and its customers.

2. Defendants operate a sophisticated software, services, and technology company under the name "[24]7.ai." Defendants' business focuses on managing online customer interactions for companies in all manner of customer-facing industries.

3. One of the services provided by Defendants is placing a "chat" function on their clients' websites that allows individuals visiting those websites to engage in text-based conversations with customer service representatives.

4. In order to perform these services, Defendants place "tags" on the infrastructure of their clients' webpages. The "tags" allow Defendants to monitor customer activity on those

websites and initiate the chat function when customers visit certain pages within a company's website.

5. Beginning in early 2017, Delta desired to add a "chat" function to its website and sought proposals from several vendors to implement and manage this function. After several months of presentations and trials, Delta chose [24]7 as the winning vendor.

6. Throughout this request for proposal process and in agreements ultimately entered into by the parties, Defendants made numerous representations regarding the data security measures that Defendants had in place and would maintain throughout the time period in which Defendants provided services to Delta.

7. Despite these representations as to the extensive data security measures Defendants would have in place, Defendants allowed at least one third party attacker unfettered access to Defendants' computer systems from September 26, 2017 through October 12, 2017, (the "Data Breach")—just months after signing a definitive agreement to provide chat services to Delta.

8. Specifically, an attacker was able to exploit Defendants' insufficient user authentication protocols in order to log in to [24]7's computer system using all-access [24]7 employee credentials.

9. After accessing [24]7's computer systems, the attacker then modified [24]7's source code so that tags Defendants had placed on Delta's website not only monitored visitor activity and facilitated the [24]7 chat function, but also "scraped" customer Personally Identifying Information ("PII") and payment card data inputted by Delta's customers via Delta's website and transmitted that data to a third party, presumably a website under the attacker's control.

10. Based on Delta's investigation to date, the third-party attacker was potentially able to exfiltrate the names, addresses, and payment card information of approximately 800,000 to 825,000 U.S. Delta customers who inputted that information via Delta's website, www.delta.com.

11. Not only did Defendants allow the Data Breach to occur, Defendants waited for more than five months to notify Delta of the Data Breach. And, during this period, while knowing that the Data Breach had occurred, [24]7 executed and provided to Delta a European General Data Protection Regulation ("GDPR") certification re-affirming its commitment to compliance with data security standards and agreeing to notify Delta immediately in the event of a data security incident.

12. The results of this Data Breach have been significant for Delta, incurring millions of dollars in costs in order to investigate the breach, provide notification to its customers, offer identity monitoring products and call center services to potentially impacted individuals, and defend consumer class action litigation arising out of the Data Breach.

13. Because Defendants' actions, as described more fully below, violated their representations regarding data security, and because the Data Breach stemmed entirely from Defendants' access to Delta's website infrastructure using Defendants' source code, as modified by a third party with or without authorized access, Delta is entitled to recover from Defendants all costs and expenses incurred by Delta as a result of the Data Breach.

THE PARTIES

14. Plaintiff Delta is a Delaware corporation with its principal place of business located at 1030 Delta Boulevard, Atlanta, GA 30354.

15. Defendant [24]7 is a California Corporation with its principal place of business located at 2001 All Programmable Drive, Suite 200, San Jose, CA 95124. Service can be made upon [24]7's registered agent, William Bose, at 2001 Logic Drive, San Jose, CA 95124.

16. [24]7's business focuses on assisting companies with "customer acquisition and engagement." Specifically, [24]7 advertises that by "[u]sing artificial intelligence and machine learning to understand consumer intent, [[24]7's] technology helps companies create a personalized, predictive, and effortless customer experience across all channels." [24]7 touts that "[t]he world's largest and most recognizable brands are using intent-driven engagement from [24]7.ai to assist several hundred million visitors annually, through more than 1.5 billion conversations, most of which are automated."

17. Defendant 24/7 Philippines is a Philippines corporation with its principal place of business at 24/7 Plaza Building, 106 Valero Street, Salcedo Village, Makati City 1227, Philippines. Upon information and belief, 24/7 Philippines is a subsidiary of [24]7.

18. Defendants do not recognize any distinction between [24]7 and 24/7 Philippines. On [24]7's website, [24]7 represents that it maintains a Philippines "delivery center" at the same address as 24/7 Philippines' office. When 24/7 Philippines entered its contracts with Delta, [24]7 handled the marketing for and negotiation of the agreements. And following execution of the agreements with 24/7 Philippines, [24]7 assumed responsibility for performing under those agreements, as evidenced by the use of [24]7 contact phone numbers and email addresses in agreements executed by 24/7 Philippines.

19. Defendants employ approximately 12,000 individuals, including many individuals that reside and work in New York. Upon information and belief, Defendants also service numerous

clients that are located in New York, and interface with thousands of New York residents through Defendants' online platforms each day.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction under 28 U.S.C. § 1332, because there is complete diversity of citizenship between Plaintiff and Defendants, and the amount in controversy exceeds $75,000 (not including interest and costs).

21. Venue is proper in this District under 28 U.S.C. § 1391(a) because Defendants have a place of business located in this District, a substantial part of the events giving rise to Delta's claim occurred in this District, and the contract at issue provides, in relevant part, that the "Federal or state courts situated in New York County, New York, United States of America, shall have exclusive jurisdiction over the resolution of all disputes that arise under this Agreement, and each party irrevocably submits to the personal jurisdiction of such courts."

FACTUAL ALLEGATIONS

A. [24]7 Engages Delta as a Client

22. In early 2017, Delta wished to add a "chat" feature to its website, www.delta.com, whereby individuals visiting the website could engage in text-based conversations with Delta customer service representatives in order to ask questions about their trips, request changes to itineraries, purchase tickets, and carry out other common customer service related functions.

23. To identify potential vendors for a chat function, Delta issued a request for proposals, seeking bids from those who could install and manage the desired chat function on Delta's website.

24. [24]7 was not initially invited to participate in the request for proposal process. However, [24]7 lobbied its contacts at Delta—cultivated through interactions at various industry

conferences and elsewhere—to give [24]7 an opportunity to bid for the project. [24]7 was therefore added as a late addition to the request for proposals.

25. [24]7 made a number of presentations and submitted voluminous documentation to Delta as part of its bid to be awarded Delta's business.

26. Notably, all of the materials submitted by [24]7 referred only to [24]7 (not "24/7 Philippines") and each of the sales executives participating in [24]7's bid were U.S.-based employees of [24]7.

27. One of the documents submitted by [24]7 as part of this sales process was a "[24]7 Chat Platform Security Overview White Paper," dated February 2017 and copyrighted by [24]7 (the "Security White Paper"). A true and correct copy of the Security White Paper is attached as Exhibit A.

28. As discussed in more detail below, the Security White Paper represented that [24]7 had achieved and maintained compliance with a number of third-party data security protocols, periodically trained its employees regarding proper data security practices, and enforced strict controls on access to the [24]7 chat console and key management system.

29. Delta ultimately narrowed the list of potential chat services vendors to two companies: [24]7 and a competitor.

30. Delta decided to allow each of these final competitors to participate in a "bake-off" in which both [24]7 and the other remaining bidder would have the opportunity to perform a live trial of their chat services and Delta representatives would score, and ultimately select, the service they most preferred.

31. In selecting [24]7 to participate in this "bake-off," Delta relied on the representations made by [24]7 in the Security White Paper and elsewhere regarding [24]7's data security practices.

32. Before beginning the "bake-off," Delta and [24]7 entered into a Professional Services Evaluation Agreement, dated April 21, 2017 (the "Evaluation Agreement"), governing [24]7's provision of chat services during this trial period.

33. Without explanation, [24]7—through its general counsel Michael Bose—inserted 24/7 Philippines as the contracting entity and purportedly had an employee of 24/7 Philippines sign the Evaluation Agreement.

34. All correspondence regarding the Evaluation Agreement, including the emails by which Delta and Defendants exchanged executed copies, were between employees of Delta and [24]7.

35. Following the "bake-off," Delta employees submitted their grades and reviews for both [24]7's chat service and the service of the other remaining bidder, and [24]7 received the highest score.

36. Delta and [24]7 therefore determined to move forward with a long-term agreement governing the provision of [24]7 chat services, which resulted in execution of a Subscription Services Agreement, dated July 24, 2017 (the "Subscription Services Agreement"). A true and correct copy of the Subscription Services Agreement is attached as Exhibit B.

37. The Subscription Services Agreement was adapted from the Evaluation Agreement, and therefore included 24/7 Philippines as the counterparty to Delta. However, as with the Evaluation Agreement, all contract negotiations and communications regarding the Subscription

Services Agreement, including emails exchanging the signed agreements, were between Delta and employees of [24]7.

B. [24]7's Access to Delta's Website Infrastructure

38. In order to implement and maintain the [24]7 Chat service, Delta granted Defendants access to certain layers of Delta's website infrastructure. Defendants informed Delta that this access was necessary in order for Defendants to provide the [24]7 chat services that Delta had purchased.

39. Specifically, [24]7 informed Delta that it would need to place a "tag" on Delta's website that would monitor the activity of individuals visiting certain webpages. Through this "tag," [24]7 could cause a chat bubble to appear on the browser of individuals visiting Delta's website. Text would appear in the chat bubble asking customers if they needed assistance. If the visitor responded by typing in a question, the conversation would be routed to a Delta customer service representative who could then type back answers.

40. In certain situations—such as when visitors to the website sought to purchase tickets or change flight itineraries—[24]7's chat function also allowed customer service representatives to accept payment card information through a separate pop-up window.

C. [24]7's GDPR Certification

41. Following the effective date of the European Union's General Data Protection Regulation in early 2018, Delta approached all of its vendors that handled consumer data and asked that they execute a Data Protection Standards Document confirming the adequacy of their data security protocols and general commitment to data security.

42. Delta tasked that [24]7 sign and return a Data Protection Standards Document as a condition of its continued provision of services to Delta.

43. [24]7 agreed and, on or about February 1, 2018, [24]7's general counsel, William Bose, signed and returned an agreement regarding [24]7's data protection standards, which Delta then countersigned (the "GDPR Agreement"). A true and correct copy of the GDPR Agreement is attached as Exhibit C.

44. The GDPR Agreement set forth minimum data security standards that [24]7 agreed to comply with in connection with its work for Delta and required [24]7 to notify Delta immediately in the event of a data breach by sending a written communication to a Delta email address. Despite the fact that [24]7 was aware of the Data Breach when it signed the GDPR Agreement (and specifically that William Bose was aware of the Data Breach), and despite the fact the GDPR Agreement required [24]7 to notify Delta immediately in the event of a data breach, 24[7] failed to disclose the Data Breach to Delta upon execution of the GDPR Agreement.

D. The Data Breach

45. On September 26, 2017—just months after the execution of the Subscription Services Agreement— at least one third-party attacker gained access to Defendants' computer networks and modified the source code of Defendants' chat services software to enable the attacker to "scrape" PII and payment card data from individuals using the websites of Defendants' clients, including Delta's website, www.Delta.com.

46. Specifically, the third party attacker was able to log in to [24]7's systems using "full access" credentials meant to be utilized by members of Defendants' development operations team to deploy the chat services functionality on Delta's website for which Delta had contracted.

47. The attacker was able to exploit this "full access" login as a result of Defendants' facially inadequate authentication measures.

48. Upon information and belief, Defendants:

a. Allowed numerous employees to utilize the same login credentials;

b. Did not limit access to the source code running the [24]7 chat function to only those individuals who had a clear need to access that code;

c. Did not require the use of passwords that met PCI DSS and other industry minimum standards;

d. Did not have sufficient automatic expiration dates for login credentials and passwords with access to sensitive source code; and,

e. Did not require users to pass multi-factor authentication prior to being granted access to sensitive source code.

49. Using this "full access" login, the attacker was able to modify the code that utilized the tags Delta had allowed [24]7 to imbed in Delta's website.

50. Specifically, the attackers modified this source code to not only monitor website activity and facilitate [24]7's chat services, but also to capture certain types of data input by visitors to the website and to then transmit that data back to the attackers. This data included names, addresses, payment card numbers, CVV codes, and expiration dates of Delta customers purchasing goods and services through Delta's website.

51. Had Defendants employed even basic access restrictions, the attackers would not have been able to modify Defendants' source code to allow the collection of PII from visitors on Delta's website. In other words, the Data Breach would never have happened.

E. [24]7's Delayed Notification to Delta

52. The third-party intrusion remained undetected by [24]7 until October 12, 2017, by which time the information of thousands of Delta customers had been at risk for over two weeks.

53. However, despite being made aware of the breach by October 12, 2017, at the latest, Defendants did not notify Delta of the incident until March 28, 2018, *i.e.,* over five months after the fact.

54. Moreover, despite the existence of established (and contractually mandated) channels of communication between [24]7 and Delta, when [24]7 finally reached out to Delta about the Data Breach, it did so through the LinkedIn pages of individual Delta and [24]7 employees.

55. Even when [24]7 finally issued an official communication, it too was short and inadequate. [24]7 provided just three sentences about the [24]7 breach on the [24]7 website.

56. To this day, no employee or other representative of 24/7 Philippines has provided Delta formal detailed notice of the Data Breach.

57. Defendants' failure to provide timely, complete information hindered Delta's ability to proactively address the breach and communicate with its customers about the incident, thereby exacerbating Delta's costs in responding to the Data Breach.

F. The Aftermath of the Data Breach

58. On March 29, 2018, immediately after being informed of the potential issue with Defendants' [24] Chat services, Delta removed the chat functionality from its website.

59. Delta also began an investigation of its own into the incident, which required Delta to hire outside consultants and advisors with expertise in data breaches.

60. Delta ultimately determined that approximately 800,000 to 825,000 of Delta's U.S. customers may have been impacted as a result of the [24]7 Data Breach.

61. After the initial phases of its investigation were completed, on April 4, 2018, Delta publicly announced that the data breach had occurred.

62. In order to mitigate any further harm to Delta, its brand, or its customers and to comply with certain state data breach laws, Delta incurred significant costs in providing direct notification to potentially impacted customers, offering those customers credit monitoring products, and engaging call center support services.

63. Shortly after the public announcement of the Data Breach, putative class actions were filed against Delta in California and Georgia federal courts. Delta has incurred significant expense in defending these lawsuits, and, even though Defendants are entirely at fault for the incident for which Delta is being sued, Delta faces significant litigation expenses even if Delta secures a victory on the merits.

G. Defendants' Specific Written Representations and Agreements

64. Defendants' failure to safeguard the personal information of Delta customers is particularly glaring in light of the numerous written representations and contract provisions under which Defendants agreed to protect that information.

65. Specifically, Defendants made specific, written representations in the Security White Paper, and violated contract provisions in the Subscription Services Agreement and GDPR Agreement.

66. With regard to the Security White Paper, [24]7 made the following relevant representations:

Section	Applicable Language
§ 2 – Certifications and Third Party Audits	[24]7 represented that it had completed, and remained in compliance with, the following third party certifications: PCI-DSS 3.1 Level 1, SOC 2+ Type 2, TRUSTed Cloud Data Privacy Certification, TRUSTed Data Certification, and Privacy Shield.
§ 3 – PCI DSS Compliance	"The [24]7 Platform (PCI certified environment) includes the data center infrastructure, applications, policies, procedures, processes and controls that are used for Chat. The [24]7 Chat Platform has been reviewed and is compliant with the twelve PCI DSS 3.0 requirements."

§ 5 – Access to Chat Console	"To enable secure access to the agent console, following controls including but not limited to are in place: • Access to the chat console is only available from whitelisted IPs • Every user is provided with a unique ID • The default password policy of the platform meets the minimum requirement outlined in PCI-DSS 3.2 • These password policies can further be strengthened based on client requirements through the [24]7 Chat admin console."
§ 7 – Secure Data Handling	"[24]7 Platform key management system is compliant with PCI DSS."
§ 12 – Data Breach Reporting	"Notifications include a description of how and why the breach occurred, what data was involved, and what has been done to mitigate the risks. If a breach involving client data has been confirmed, the client would be immediately notified through agreed upon channels."

67. With regard to the Subscription Services Agreement 24/7 Philippines agreed to the following key contract terms:

Section	Applicable Language
§ 2.7 – Customer Data	"'Customer Data' means data, information or material uploaded or routed to the Subscription Services, transmitted using the Subscription Services or otherwise provided to Service Provider in any medium by Delta or third parties . . . Service Provider will maintain the security and integrity of the Subscription Services and the Customer Data and will inform Delta of any third party who requests or obtains access to the Customer Data."
§ 3.3 - Third Party Data	"Service Provider . . . does warrant that after its receipt Service Provider will collect, process and deliver . . . Third Party Data using qualified personnel in a thorough and workmanlike manner consistent with the highest industry standards."
§ 3.7 – PCI Compliance	"Service Provider . . . shall [ ] comply with, and shall have a program to assure its continued compliance with, the Payment Card Industry Data Security Standards (the "**PCI DSS**") published by the PCI Security Standards Council . . . ."
§ 8.2 – Standards	"Service Provider shall take commercially reasonable efforts to avoid the introduction, and Service Provider will not subsequently introduce into the Subscription Services, the Software or the Customer Data, any 'back door,' 'time bomb,' 'Trojan horse,' 'worm,' 'drop dead device,' 'virus,' 'preventative routines' or other computer software routines designed: to permit access to or use of Delta's computer systems by Service Provider or a third party not authorized by this Agreement . . . ."

§ 13.1 – Confidential Information	"Each party . . . shall maintain in strict confidence, and agrees not to disclose to any third party . . . Confidential Information that the Recipient receives from Discloser or its Affiliates. '**Confidential Information**' means all non-public information . . . concerning . . . customers or suppliers . . . ."
§ 13.4 – Third Party Information	"The confidentiality provisions herein apply to and shall also protect Confidential Information of third parties provided by Discloser to Recipient."
§ 13.8 – Additional Provisions regarding PII	"In the event Service Provider obtains access to the Personally Identifying Information of Delta and its affiliates, in addition to the other obligations contained herein, Service Provider shall comply with the provisions of Exhibit C, Personally Identifying Information."
Exhibit C – Personally Identifying Information	"For the purposes of these provisions, the term '**Personally Identifying Information**' or '**PII**' mean any information regarding identifiable individuals . . . . Service provider shall implement, at a minimum, the data security measures and observe the minimum standards for the protection of PII as set forth in this paragraph . . . Service Provider agrees to use reasonable measures, including encryption, to prevent unauthorized persons from gaining access to the data processing equipment or media where PII is stored or processed. Service provider agrees to provided its employees and agents access to PII on a need-to-know basis only and agrees to cause any persons having authorized access to such information to be bound by obligations of confidentiality, non-use and non-disclosure no less stringent than those imposed upon Service Provider by this Agreement. . . .Service Provider agrees to use reasonable measures, including encryption, to prevent PII from being read, copied, altered or deleted by unauthorized parties during the transmission thereof . . . . Service Provider shall report security breaches (data or network) to Delta in a prompt and timely manner and assist Delta's Information Security and Privacy Office ("ISPO") in the investigation thereof. . . . Article 13 in the main body of this Agreement shall apply to Personally Identifying Information to the same extent as Confidential Information."
Exhibit D – Electronic Access	"Service Provider shall not permit or allow any unauthorized person or third party to access, use or modify the Permitted Systems. . . . Service Provider shall take commercially reasonable efforts to avoid the introduction into Delta's or its Affiliates' computer systems, intranet, databases or extranet . . . designed: to permit unauthorized access to or use or modification of . .. Confidential Information . . . ."

68. With regard to the GDPR Agreement, [24]7 agreed to the following key contract terms:

Section	Applicable Language
§ 2 – Data Processing	"[[24]7 shall] maintain all appropriate Technical and Organizational Security Measures in accordance with Good Industry Practice regarding the security of Data including: (i) protection against unauthorized or unlawful processing (including, without limitation, unauthorized or unlawful disclosure of, access to and/or alteration of Data); and (ii) protection against accidental loss, destruction or damage, to ensure that the processing of the Personal Data shall meet the requirements of the Regulation and the protection of the rights of Data Subjects shall be compliant with Data Protection Laws at all times and shall comply with Delta's applicable IT security policies."
§ 3 – Sub-contracting and transfers to third parties	"[[24]7] shall enter into a written agreement with each Sub-Processor under this Clause 3 containing obligations on such third party which are no less stringent than those set out in this Document and Service Provider shall remain fully liable to Delta for the performance of the Sub-Processor's obligations."
§ 6 – Data breaches	"[[24]7] shall notify Delta immediately in writing to privacy@delta.com after becoming aware of any Reportable Breach or any other breach of this Document. . . . [[24]7] shall investigate the Reportable Breach in the most expedient time possible and shall then provide Delta as soon as possible with complete information relating to a Reportable Breach, including, without limitation, the nature of the Reportable Breach, the nature of the personal data affected, the categories and number of Data Subjects concerned, the categories and number of personal data records concerned, the possible consequences of the Reportable Breach, the measures taken to, or proposed to be taken, to address the Reportable Breach and mitigate its possible effects and any other information that Delta may reasonably request concerning the Reportable Breach."

H. Defendants Refuse Delta's Demand for Payment

69. After Delta's own investigation into the incident revealed that Defendants' inadequate data security measures were the primary cause of the attackers' ability to access the information of Delta's customers, Delta made due demand on Defendants for reimbursement of the costs Delta incurred to date as a result of the Data Breach.

70. Defendants have repeatedly refused Delta's demands and instead have forced Delta to incur these ongoing Data Breach response costs as well as to litigate these otherwise clear claims.

CLAIMS FOR RELIEF

COUNT I – Breach of Contract (Against 24/7 Philippines)

71. Delta incorporates each of the above allegations as if set forth fully herein.

72. 24/7 Philippines and Delta entered into the Subscription Services Agreement on or about July 24, 2017. The Subscription Services Agreement went into effect on that date and remained in effect until after the Data Breach was disclosed to Delta.

73. Delta performed under the Subscription Services Agreement in all respects, including by tendering all payments due to 24/7 Philippines under the Subscription Services Agreement during the period it was in force.

74. 24/7 Philippines breached §§ 2.7, 3.3, 3.7, 8.2, 13.1, 13.4, 13.8, and Exhibit C of the Subscription Services Agreement. Specifically, 24/7 Philippines:

a. Failed to keep Delta customers' data in strict confidence as required under §§ 2.7 and 13.1;

b. Failed to process Delta customers' data using only qualified personnel in a thorough and workmanlike manner consistent with the highest industry standards as required under § 3.3;

c. Failed to comply with, and have a program to assure continued compliance with, PCI DSS as required under § 3.7;

d. Failed to take commercially reasonable efforts to avoid the introduction of computer software designed to permit access to or use of Delta's computer systems by unauthorized third parties as required under § 8.2 and Exhibit D;

e. Failed to implement reasonable data security measures, including measures that would (1) prevent unauthorized persons from gaining access to Delta customers' information, (2) limit employees and agents access to PII to a need-to-know basis, and (3) require persons having access to such information to be bound by obligations of confidentiality, non-use and non-disclosure no less stringent than those imposed upon 24/7 Philippines by the Subscription Services Agreement in violation of §§ 13.4, 13.8, and Exhibit C;

f. Failed to use reasonable measures, including encryption, to prevent PII from being read, copied, altered or deleted by unauthorized parties during the transmission thereof in violation of §§ 13.4, 13.8, and Exhibit C; and,

g. Failed to report the Data Breach to Delta in a prompt and timely manner in violation of §§ 13.4, 13.8, and Exhibit C.

75. With specific regard to PCI DSS Version 3.2, upon information and belief, at a minimum 24/7 Philippines failed to comply with "Requirement 8: Identify and authenticate access to system components," which requires that organizations:

a. "Assign[] a unique identification (ID) to each person with access [to system components]" in order to "ensure[] that each individual is uniquely accountable for their actions."

b. "Define and implement policies and procedures to ensure proper user identification management for nonconsumer users and administrators on all system components."

c. "Manage IDs used by third parties to access, support, or maintain system components via remote access."

d. "In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: Something you know, such as a password or passphrase; Something you have, such as a token device or smart card; [and] Something you are, such as a biometric."

e. "Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication."

f. "Do not use group, shared, or generic IDs, passwords, or other authentication methods."

g. "Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer."

76. As a result of these breaches, the personal information of thousands of Delta customers was potentially exposed to third parties, triggering millions of dollars of damages for Delta, including lost use of [24]7 Chat, investigation and remediation of the security incident, the costs of notifying Delta customers and certain regulators of the incident, the cost of providing

credit monitoring products and call center support services to Delta customers, penalty assessments imposed by card companies for the costs incurred by the card companies related to the Data Breach and the costs of defending multiple class action lawsuits.

77. Moreover, because 24/7 Philippines violated the confidentiality obligations set forth in the Subscription Services Agreement, Delta's damages are not subject to any limitation on liability and Delta may recover for all the losses described above. *See* Subscription Servs. Agmt. § 11.3.

78. Delta is therefore entitled to damages as a result of 24/7 Philippines's breach of the Subscription Services Agreement in an amount sufficient to reimburse Delta for all costs incurred as a result of the Data Breach.

COUNT II – Piercing of the Corporate Veil
(Against [24]7)

79. Delta incorporates each of the above allegations as if set forth fully herein.

80. A New York court may pierce the corporate veil to reach a parent company upon a showing that that the parent exercised complete domination in respect to the transaction at issue so that the subsidiary had at the time no separate will of its own.

81. Here, [24]7 exercised complete domination over its wholly owned subsidiary, 24/7 Philippines, with respect to the marketing for, negotiation of, and performance under the Subscription Services Agreement, including by:

a. Marketing the services provided to Delta under the Subscription Services Agreement exclusively through employees of [24]7;

b. Representing on the [24]7 website that 24/7 Philippines is an office location of [24]7 without including any indication that 24/7 Philippines is a separate entity;

c. Negotiating the Subscription Services Agreement through U.S. based employees of [24]7;

d. Performing the services under the Subscription Services Agreement through U.S. based employees of [24]7, as evidenced by the inclusion of [24]7 contact information for operational support in the Subscription Services Agreement; and,

e. Otherwise entirely controlling the actions of 24/7 Philippines with respect to the Subscription Services Agreement and 24/7 Philippines relationship with Delta.

82. [24]7 utilized its subsidiary 24/7 Philippines solely in an attempt to limit its liability for liability triggering events such as the security incident at issue here. There was no other business or operational purpose for [24]7's decision to contract through 24/7 Philippines.

83. As a result, the Court should hold [24]7 jointly and severally liable for 24/7 Philippines' breach of the Subscription Services Agreement and the resultant damages to Delta.

COUNT III – Negligence
(Against [24]7)

84. Delta incorporates each of the above allegations as if set forth fully herein.

85. By accessing Delta's website infrastructure for purposes of deploying and managing the [24]7 chat feature, [24]7 undertook a duty to use reasonable care to avoid causing foreseeable risk of harm to Delta.

86. Moreover, [24]7's sole business purpose is to provide technology services such as those it provided to Delta, and [24]7 holds itself out as an expert in providing such services.

87. As alleged herein, [24]7 breached its duties by failing to act in accordance with a minimum standard of care in allowing an attacker to gain unfettered access to [24]7's computer

systems, and thereby facilitating that attacker's access to the PII and payment card information of Delta's customers.

88. As a direct and proximate result of [24]7's negligence, Delta has suffered and will continue to suffer injury and damages as described herein.

COUNT IV – Fraud
(Against [24]7)

89. Delta incorporates each of the above allegations as if set forth fully herein.

90. In marketing its chat services to Delta, [24]7 made a number of representations regarding the data security certifications and protocols it maintained to prevent unauthorized access to its computer systems and the computer systems of its customers.

91. At a minimum, [24]7 made the specific written representations contained in the Security White Paper, set forth in detail above.

92. [24]7 made the representations in an attempt to induce Delta to rely on those representations in granting [24]7 certain access to Delta's website infrastructure, and Delta did rely on these representations in granting [24]7 such access.

93. However, despite the numerous specific representations regarding [24]7's data security certifications and protocols, at a minimum, [24]7 was not, at the time of those representations and thereafter:

a. In compliance with PCI DSS standards, particularly PCI DSS Requirement 8, as set forth in detail above;

b. Implementing standard restrictions on access to the chat console;

c. Utilizing sufficient platform key management; or,

d. Practicing adequate data breach reporting measures.

94. On information and belief, [24]7 knew the representations in the Security White Paper to be false at the time the representations were made.

95. But for Delta's reliance on [24]7's representations regarding data security certifications and protocols, it would not have allowed [24]7 any access to Delta's website infrastructure. The Data Breach therefore would never have occurred and Delta would not have incurred the significant costs triggered as a result of the Data Breach but for [24]7's misrepresentations.

96. Delta is therefore entitled to damages as a result of [24]7's fraud in an amount sufficient to reimburse Delta for all costs incurred as a result of the Data Breach.

COUNT V – Breach of Contract
(Against [24]7)

97. Delta incorporates each of the above allegations as if set forth fully herein.

98. [24]7 and Delta entered into the GDPR Agreement on or about February 1, 2018. The GDPR Agreement went into effect on that date and remains in effect through the filing of this lawsuit.

99. Delta has performed under the GDPR Agreement in all respects, including by tendering all payments due to Defendants for services performed for Delta.

100. However, upon information and belief, [24]7 violated §§ 2, 3, and 6 of the GDPR Agreement. Specifically, 24[7]:

a. Failed to maintain all appropriate Technical and Organizational Security Measures in accordance with Good Industry Practice regarding the security of Data as required by § 2;

b. Failed to ensure that sub-contractors and third parties performing work in conjunction with or on behalf of [24]7 complied with the terms of the GDPR Agreement, as required by § 3; and,

c. Failed to notify Delta immediately following the Data Breach or to investigate the Data Breach in the most expedient time possible and provide Delta as soon as possible with complete information relating to the Data Breach, as required by § 6.

101. Though the GDPR Agreement was entered into after the Data Breach occurred, at a minimum, the GDPR Agreement required [24]7 to inform Delta of the data breach so that Delta could mitigate the potential damages from the Data Breach by informing its customers and card issuers, by terminating Defendants as vendors, and by discontinuing payment to Defendants.

102. Delta is therefore entitled to damages as a result of [24]7's breach of the GDPR Agreement in an amount sufficient to reimburse Delta for all costs incurred as a result of [24]7's failure to notify Delta of the Data Breach.

COUNT VI - Common Law Indemnity
(Against All Defendants)

103. Delta incorporates each of the above allegations as if set forth fully herein.

104. Defendants' actions in failing to implement adequate security and causing the Data Breach have obligated Delta to incur an array of different costs and expenses including, but not limited to, investigating the Data Breach, notifying its customers and regulators of the Data Breach, providing identity protection products and call center services to its customers, and defending against consumer litigation alleging harm as a result of the Data Breach.

105. Delta's obligations with regard to the above costs arose entirely as a result of Delta's relationship with Defendants and through no fault of Delta's own.

106. Under the doctrine of Common Law indemnification, Delta is therefore entitled to a declaration that Defendants are required to indemnify Delta for all costs and obligations incurred a result of the Data Breach as well as an award of damages for all such costs and obligations incurred by the time of trial in this action.

COUNT VII – Contractual Indemnity,
In the Alternative to Count VI
(Against 24/7 Philippines)

107. Delta incorporates each of the above allegations as if set forth fully herein.

108. Article 10 of the Subscription Services Agreement provides that 24/7 Philippines shall indemnify Delta for all "liabilities, obligations, losses, damages, deficiencies, penalties, levies, fines, judgments, settlements, costs and expenses, including interest, litigation costs, and reasonable attorney's fees ('Losses') asserted by a third party . . . under this Article 10 . . . ."

109. As set forth in detail above, Delta has suffered significant Losses, as that term is defined in Article 10 of the Subscription Services Agreement, as a result of third-party claims asserted against Delta as a result of the Data Breach.

110. Delta provided notice of those Losses to 24/7 Philippines and demanded that 24/7 Philippines indemnify Delta for those Losses pursuant to Article 10 of the Subscription Services Agreement.

111. To date, 24/7 Philippines has refused to provide any such indemnity or otherwise comply with the terms of Article 10 of the Subscription Services Agreement.

112. Delta is therefore entitled to a declaration that 24/7 Philippines is required to indemnify Delta for all costs and obligations incurred a result of the Data Breach as well as an award of damages for all such costs and obligations incurred by the time of trial in this action.

PRAYER FOR RELIEF

WHEREFORE, Delta prays for judgment as follows:

a) That 24/7 Philippines be adjudged and decreed to have violated the Subscription Services Agreement;

b) That the Court pierce [24]7's corporate veil and declare [24]7 to be jointly and severally liable for any liabilities of 24/7 Philippines to Delta;

c) That [24]7 be adjudged and decreed to have negligently injured Delta through its inadequate data security procedures that led to the Data Breach;

d) That [24]7 be adjudged and decreed to have committed fraud by making false representations regarding its data security procedures on which Delta relied in allowing [24]7 to access Delta's website infrastructure;

e) That [24]7 be adjudged and decreed to have violated the GDPR Agreement;

f) The Court imply an agreement of indemnification between Defendants and Delta with regard to the costs and obligations incurred by Delta as a result of the Data Breach or, in the alternative, declare that 24/7 Philippines is contractually obligated to indemnify Delta pursuant to Article 10 of the Subscription Services Agreement;

g) That Delta recover damages from [24]7 and 24/7 Philippines, jointly and severally, for all losses stemming from 24/7 Philippines' breach of the Subscription Services Agreement, including but not limited to the costs Delta incurred in investigating and remediating the security incident, notifying customers, providing credit monitoring products and call center services to customers, and defending lawsuits arising out of the incident;

h) That Delta be awarded pre- and post-judgment interest, and that such interest be awarded at the highest rate from and after the date of service of the initial complaint in this action;

i) That Delta recover its costs and disbursements of this suit, including reasonable attorneys' fees as provided by law; and,

j) That Delta be awarded such other, further, and different relief as the case may require and the Court may deem just and proper.

JURY TRIAL DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for all issues so triable.

Dated: New York, New York
August 8, 2019

KING & SPALDING LLP

By: s/*Paul A. Straus*

Paul A. Straus
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel: (212) 556-2136/Fax: (212) 556-2222
pstraus@kslaw.com

David L. Balser*
J. Andrew Pratt*
James Matthew Brigman*
KING & SPALDING LLP
1180 Peachtree Street, NE
Atlanta, Georgia 30309
Tel: (404) 572-4600
Fax: (404) 572-5100
dbalser@kslaw.com
apratt@kslaw.com
mbrigman@kslaw.com
(*pro hac vices forthcoming*)

Attorneys for Delta Air Lines, Inc.