UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

NIKI PARAS, on behalf of herself and all others similarly situated,	
Plaintiff,	**Case No.**
v.	**CLASS ACTION COMPLAINT**
DENTAL CARE ALLIANCE, LLC,	DEMAND FOR JURY TRIAL
Defendant.	

CLASS ACTION COMPLAINT

1. Plaintiff NIKI PARAS, on behalf of herself and all others similarly situated, brings this action against Defendant Dental Care Alliance, LLC ("DCA" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from the Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual Class Members exceed

the sum or value of $5,000,000.00 exclusive of interest and costs, and members of the Proposed Class (such as named Plaintiff) are citizens of states different from Defendant.

3. Defendant has sufficient minimum contacts in Georgia, as it conducts a substantial part of its business in the State of Georgia, thus rendering the exercise of jurisdiction by this Court proper and necessary.

4. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to these claims occurred in this District.

NATURE OF THE ACTION

5. This class action arises out of the recent cyberattack and data breach involving Defendant (the "Data Breach"), which held in its possession certain Protected Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively, the "Private Information") of the Plaintiff, who was a patient of Imagix Dental—one of many dental service providers who are affiliated with DCA[1] and whose Private Information is hosted on DCA's servers.

[1] *See* https://www.dentalcarealliance.net/affiliated-practices/georgia/.

6. The Private Information compromised in the Data Breach involved highly sensitive information including patient names, addresses, dental diagnoses, treatment information, patient account numbers, billing information, bank account numbers, and health insurance data of patients who visited dental practices that were in the DCA network.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' Private Information.

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

9. In addition, Defendant (acting in the course and scope of its agency relationship with its affiliated dental practices) and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

10. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

11. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Member Private Information; and failing to take standard and reasonably available steps to prevent the Data Breach.

12. Plaintiff's and Class Members are now at an increased risk of identity theft because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

13. Armed with the Private Information accessed in the Data Breach, malicious actors can commit a variety of crimes including, *e.g.*, using Class

Members' names to extensions of credit , obtain medical services using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, filing false medical claims using Class Members' information, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future spend time to closely monitor their financial accounts to guard against identity theft.

15. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect financial fraud and identity theft.

16. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

18. Accordingly, Plaintiff brings this action against Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence; (ii) intrusion into private affairs; (iii) negligence *per se*; (iv) breach of express contract; (v) breach of implied contract; (vi) breach of fiduciary duty; and (vii) breach of confidence.

PARTIES

19. Plaintiff Niki Paras ("Paras") is and at all times mentioned herein was as individual citizen of the state of Georgia, residing in the city of Buford. Plaintiff Paras received notice of the Data Breach from Imagix Dental, who is one of many dental service providers affiliated with Defendant. A copy of the notice she received is attached hereto as Exhibit A (the "Notice Letter").

20. Defendant is a Florida limited liability company that is headquartered at 6240 Lake Osprey Drive, Sarasota, Florida 34240.

I. STATEMENT OF FACTS

A. Nature of Defendant's Businesses

21. Defendant is a for-profit company that specializes in providing practice support services to dental practices that it is affiliated with and part of its network.

22. Defendant is a practice support vendor for over 320 affiliated dental practices in twenty states, including Georgia.[2]

23. As a practice support vendor for its network of dental practices, Defendant handles insurance billing, customer service, accounting and payroll, information technology, and operations management for its affiliated practices.

24. In order to obtain dental health care services, Plaintiff and Class Members provided Private Information to their respective dental practices, including their names, contact information, dental history, dental insurance information and billing information.

25. Defendant (in the course of providing its services and acting as an agent of these respective dental practices) maintained this Private Information on its servers and within its data infrastructure.

26. In the course of providing dental services, Plaintiff's and Class Members' dental service providers and by extension Defendant DCA, agreed to and undertook legal duties to maintain the Private Information entrusted to them by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

---

[2] See *About DCA*, Dental Care Alliance, https://www.dentalcarealliance.net/about-dca/ (last visited: Dec. 22, 2020).

27. Defendant , acting as an agent of Plaintiff's and Class Members' dental service providers, held the patient information collected by the dental service providers at its servers located in Sarasota, Florida.[3]

28. The patient information held by Defendant in its computer systems and networks included the Private Information of Plaintiff and Class Members.

B. The Data Breach

29. On or about October 11, 2020, DCA became aware of a cybersecurity incident on its network.

30. DCA engaged a cybersecurity firm to investigate the incident. The investigation then determined that for nearly a month between September 18, 2020 and October 13, 2020 there had been unauthorized activity on Defendant's network and that confidential files belonging to 1 million patients had been accessed.[4]

31. The data that was accessed by an unauthorized third party during the incident included the Private Information of Plaintiff and Class Members, including patient names, addresses, dental diagnosis, treatment information, patient

[3] *See* Notice Letter.
[4] *See* Jessica Davis, *Third-Party Vendor Dental Care Alliance Breach Impacts 1M Patients*, Health IT Security (Dec. 16, 2020), https://healthitsecurity.com/news/third-party-vendor-dental-care-alliance-breach-impacts-1m-patients (last visited Dec. 23, 2020).

account numbers, billing information, bank account numbers, and health insurance data.

32. On or about December 7, 2020, DCA notified Plaintiff and other Class Members of the Data Breach.

33. DCA advised Plaintiff and Class Members to remain vigilant and to review financial statements and accounts for suspicious activity, however, Defendant did not offer any complimentary financial fraud or identity monitoring services.

C. DCA's Privacy Obligations

34. Defendant had an obligation created by contract, HIPPA, industry standards, common law, and representations made to Class Members, to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

35. Plaintiff and Class Members provided their Private Information to Defendant's affiliated dental service providers and, by extension Defendant who was acting as agent for each of these dental service providers, with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

36. DCA's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting healthcare providers in the last few years.

37. Experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

38. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread.

39. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[5]

40. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[6]

41. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[7]

---

[5] See https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 23, 2020)

[6] *Id.*

42. Indeed, cyber- attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

43. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

44. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data infrastructure. Defendant's unlawful conduct includes, but is not limited to, its failure to:

---

[7] *Id*. at p15.
[8] See https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Dec. 23, 2020).

a. maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. adequately protect patients' Private Information;

c. properly monitor its own data security systems for existing intrusions;

45. As the result of computer systems in need of security upgrading, failure to implement proper cybersecurity hardware and software (such as next generation firewalls and multi-factor authentication), and inadequately trained employees, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

46. Accordingly, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

D. Defendant's Conduct Violated HIPPA

47. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

48. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of Private Information. Safeguards must include physical, technical, and administrative components.

49. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS")

create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

50. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

E. Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identify Theft

51. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which they noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

52. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended

[9]*See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 22, 2020) ("GAO Report").

fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[10]

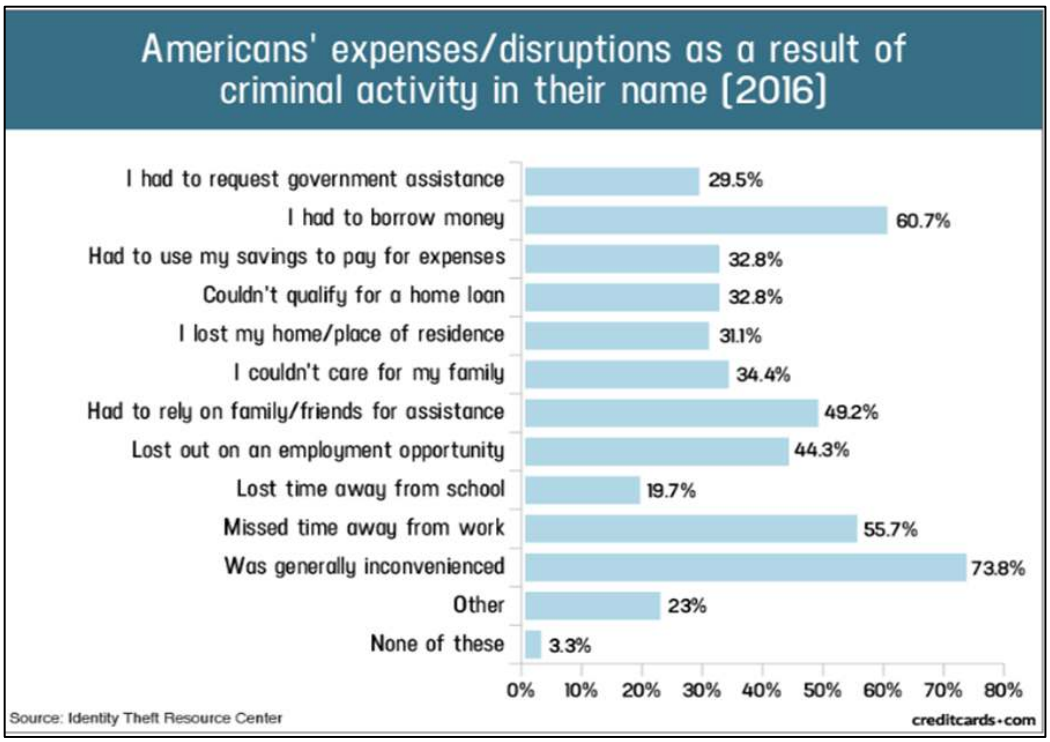
53. Identity thieves use stolen personal information such as bank account numbers and health insurance information for a variety of crimes, including identity theft, financial fraud, and insurance fraud.

54. Identity thieves can also use Class Members' names and information to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, filing false medical claims using Class Members' information, and giving false information to police during an arrest.

55. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[11]

---

[10] *See* https://www.identitytheft.gov/Steps (last visited Dec. 22, 2020).
[11] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed December 22, 2020).



56. What's more, theft of PHI is also gravely serious. PHI and other Private Information is a valuable property right.[12]

57. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

[12] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (Private Information, "which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

58. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[13]

59. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

60. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when they is discovered, and also between when PHI and/or financial information is stolen and when they is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to

[13] *See Medical Identity Theft*, Federal Trade Commission Consumer Information (last visited: Dec 23, 2020), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

> commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

61. PHI and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

62. Where the PHI belonging to Plaintiff and Class Members was accessed and removed from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

63. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

64. Medical information is especially valuable to identity thieves.

65. While credit card information can sell for as little as $1-$2 on the black market, the asking price on the Dark Web for medical data is $50 and up.[14]

---

[14] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed Dec. 23, 2020).

66. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

67. Defendant therefore knew or should have known this risk and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

68. Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

V. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

69. To date, Defendant has done absolutely nothing to compensate Class Members for the damages they sustained in the Data Breach.

70. Defendant has not even bothered to offer Plaintiff and Class Members basic credit monitoring.

71. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

72. After the Data Breach, Plaintiff discovered unauthorized use of her Private Information. Indeed, Plaintiff discovered unauthorized and fraudulent

charges on her payment card, which is the same card she used to pay for dental services related to the Data Breach.

73. Similarly, after the Data Breach occurred, Plaintiff received scam phone calls, which appeared to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

74. Simply put, Plaintiff's Private Information was compromised and exfiltrated by cyber criminals as a direct and proximate result of the Data Breach.

75. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

76. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

77. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

78. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private

Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

79. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

80. Plaintiff and Class Members also suffered a loss of value of their Private Information when they was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

81. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

82. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered 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 relating to:

a. finding fraudulent insurance reimbursements;

b. finding fraudulent charges;

c. canceling and reissuing credit and debit cards;

d. purchasing credit monitoring and identity theft prevention;

e. addressing their inability to withdraw funds linked to compromised accounts;

f. taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. lacing "freezes" and "alerts" with credit reporting agencies;

h. spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. contacting financial institutions and closing or modifying financial accounts;

j. resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

83. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of the

Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information and financial information is not accessible online and that access to such data is password-protected.

84. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

85. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

86. Defendant's delay in identifying and reporting the Data Breach caused additional harm. It is axiomatic that "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage.

Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[15]

87. Indeed, once a Data Breach has occurred, "[o]ne thing that does matter is hearing about a Data Breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cyber criminals and warn other businesses of emerging dangers. If consumers don't know about a breach because they wasn't reported, they can't take action to protect themselves" (internal citations omitted).[16]

VI. CLASS ACTION ALLEGATIONS

88. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated (the "Class") pursuant to Rule 23 (b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

---

[15] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

[16] Consumer Reports, The Data Breach Next Door: Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too, January 31, 2019, https://www.consumerreports.org/data-theft/the-data-breach-next-door/

89. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised in the Data Breach and who were sent Notice of the Data Breach from Defendant or one of its affiliates (the "Class").

90. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

91. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

92. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 1,000,000 patients whose data was compromised in the Data Breach.

93. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common question of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

94. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

95. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class and Subclass. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

96. Predominance. Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

97. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant . In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

98. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

99. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

100. Finally, all members of the proposed Class are readily ascertainable. Defendant have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT

Negligence
(On Behalf of Plaintiff and All Class Members)

101. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 100 above as if fully set forth herein.

102. Plaintiff and Class Members were required to submit non-public Private Information to Defendant in order to obtain medical services.

103. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiff and Class Members' Private Information held within it—to prevent disclosure of the Private Information, and to safeguard the Private Information from theft.

Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

104. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPPA and Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

105. Defendant's duty of care to use reasonable security measures arose as a result of the special relationships that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

106. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the

medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

107. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

108. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

109. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Mishandling phishing emails, so as to allow for unauthorized person(s) to access Plaintiff's and Class Members' Private Information;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff and Class Members' Private Information;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff and Class Members' Private Information;

f. Failing to detect in a timely manner that Plaintiff and Class Members' Private Information had been compromised; and

g. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

110. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

111. It was therefore foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in one or more types of injuries to Plaintiff and Class Members.

112. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach

113. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT

Intrusion Into Private Affairs / Invasion Of Privacy (On Behalf of Plaintiff and All Class Members)

114. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 100 as if fully set forth herein.

115. The state of Georgia recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

116. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

117. Defendant's conduct as alleged above intruded upon Plaintiff and Class Members' seclusion under common law.

118. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff and Class Members' privacy by intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person, and by intentionally causing anguish or suffering to Plaintiff and Class Members.

119. Defendant knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

120. Defendant invaded Plaintiff and Class Members' right to privacy and intruded into Plaintiff and Class Members' private affairs by intentionally misusing

and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

121. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

122. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests, caused anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

123. In failing to protect Plaintiff and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seek an award of damages on behalf of themselves and the Class.

THIRD COUNT

Breach of Express Contract
(On Behalf of Plaintiff and All Class Members)

124. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 100 above as if fully set forth herein.

125. Plaintiff and Members of the Class allege that they entered into valid and enforceable express contracts, or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

126. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant.

127. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

128. Both the provision of medical services healthcare and the protection of Plaintiff's and Class Members' Private Information were material aspects of these express contracts.

129. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members Private Information – are formed and embodied in multiple documents, including (among other documents) the Privacy Notices of the dental service providers for whom Defendant was acting as their agent when it received Plaintiff's and Class Members' Private Information.

130. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these contracts with Defendant and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

131. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

132. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

133. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

134. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and more than 1 million Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTC Act, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

135. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

136. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

137. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant's affiliated healthcare providers.

138. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future,

disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

139. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

FOURTH COUNT

Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

140. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 100 above as if fully set forth herein.

141. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such Private Information.

142. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

143. Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiff's and Class Members' Private Information.

144. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

145. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

146. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contracts between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

147. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

148. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their Private Information.

149. As a result of Defendant's failure to fulfill the data security protections promised in these implied contracts, Plaintiff and Members of the Class

did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that agreed upon in the implied contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

150. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

151. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

152. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH COUNT

Negligence *Per Se*
(On Behalf of Plaintiff and All Class Members)

153. Plaintiff re-alleges and incorporates by reference Paragraphs 1

through 100 above as if fully set forth herein.

154. Pursuant to Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information.

155. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

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

157. Pursuant to HIPAA (42 U.S.C. § 1302d, *et seq.*), Defendant had a duty to implement reasonable safeguards to protect Plaintiff and Class Members' Private Information.

158. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning

without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

159. Plaintiff and Class Members are within the class of persons that the HIPAA was intended to protect.

160. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The federal Health and Human Services' Office for Civil Rights (OCR) has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class.

161. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

163. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

164. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

165. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

SIXTH COUNT

Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

166. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 100 above as if fully set forth herein.

167. In light of the special relationships between Defendant and Plaintiff and Class Members, whereby Defendant became guardians of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members: (i) for the safeguarding of Plaintiff and Class Members' Private Information; (ii) to timely notify Plaintiff and Class Members of a data breach and disclosure; and (iii) maintain complete and

accurate records of what Private Information (and where) Defendant did and does store.

168. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

169. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

170. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff and Class Members' Private Information.

171. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

172. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

173. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

174. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

175. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

176. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

177. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or

disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

178. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

179. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

180. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all Members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

181. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures

establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

182. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff and Class Members' Private Information.

183. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data

Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

184. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SEVENTH COUNT

Breach of Confidence
(On Behalf of Plaintiff and All Class Members)

185. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 100 above as if fully set forth herein.

186. At all times during Plaintiff and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff and Class Members' Private Information that Plaintiff and Class Members provided to Defendant.

187. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

188. Plaintiff and Class Members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

189. Plaintiff and Class Members also provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of protecting its networks and data systems, including employees' email accounts.

190. Defendant voluntarily received in confidence Plaintiff and Class Members' Private Information with the understanding that Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

191. Due to Defendant's failure to prevent, detect, avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

192. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

193. But for Defendant's disclosure of Plaintiff and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff and Class Members' Private Information, as well as the resulting damages.

194. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff and Class Members' Private Information. Defendant knew its computer systems and technologies for accepting and securing Plaintiff and Class Members' Private Information had numerous security vulnerabilities.

195. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated

with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

196. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

b. For equitable relief enjoining Defendant Dental Care Alliance from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PRIVATE INFORMATION;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PRIVATE INFORMATION compromised during the Data Breach;

d. Ordering Defendant to pay for an identity theft protection service for Plaintiff and the Class;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees, and costs, and any other expense, including expert witness fees;

h. Pre- and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: January 6, 2021

Respectfully submitted,

/s/ Gregory Bosseler

MORGAN & MORGAN, P.A.

Gregory Bosseler
191 Peachtree Street N.E., Suite 4200
P.O. Box 57007
Atlanta, Georgia 30343-1007
gbosseler@forthepeople.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP

John A. Yanchunis (FL Bar No. 324681)
201 N. Franklin St., 7th Floor
Tampa, FL 33602

Telephone: (813) 223-5505
Facsimile: (813) 222-2434
jyanchunis@forthepeople.com

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel: (202) 429-2290
Email: gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff