IN THE STATE COURT OF FULTON COUNTY
STATE OF GEORGIA

NIKI PARAS, REGINA ROSARIO, JENNIFER SILLAH, CHRISTIAN STEPHENS, EVELYN WALLACE, and TANYA WILDRICK,	:	
on behalf of themselves and all others similarly situated,	:	**Case No**.
Plaintiffs,	:	**CLASS ACTION COMPLAINT**
v.	:	
DENTAL CARE ALLIANCE, LLC,	:	DEMAND FOR JURY TRIAL
Defendant.	:	

CLASS ACTION COMPLAINT

Plaintiffs NIKI PARAS, REGINA ROSARIO, JENNIFER SILLAH, CHRISTIAN STEPHENS, EVELYN WALLACE, and TANYA WILDRICK, on behalf of themselves and all others similarly situated, bring 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. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of his counsel, and the facts that are a matter of public record.

JURISDICTION AND VENUE

1. This Court has personal jurisdiction over Defendant, as DCA has sufficient minimum contacts with the State of Georgia. Through its business operations in the State of Georgia and in Fulton County, Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper. Defendant DCA does

business in the State of Georgia (through, among other things, its contracts with dental practices in Fulton Count) and the business being done in Georgia directly relates to the subject of this lawsuit, thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

2. Venue is proper because a substantial part of the events and omissions giving rise to these claims occurred in Fulton County.

NATURE OF THE ACTION

3. 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 Plaintiffs, who were patients and/or employees of dental service providers who are affiliated with Defendant[1] and whose Private Information is hosted on Defendant's servers.

4. The Private Information compromised in the Data Breach involved highly sensitive information of patients who sought treatment, or employees who worked for, dental practices that were included in Defendant's network, including: (a) patient names, addresses, dental diagnoses, treatment information, account numbers, billing information, bank account numbers, and health insurance data and (b) employee names, Social Security numbers, dates of birth, Employee Identification numbers, and financial account numbers.

5. 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.

6. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they

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

collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs 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.

7. 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.

8. 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 Plaintiffs' 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.

9. Defendant disregarded the rights of Plaintiffs 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.

10. Plaintiffs 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.

11. 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.

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

13. Plaintiffs 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.

14. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal 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.

16. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its 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

17. Plaintiff Niki Paras ("Paras") is and at all times mentioned herein was an individual citizen of the state of Georgia, residing in the city of Buford. Prior to the Data Breach, Plaintiff Paras was a patient at Imagix Dental, which is one of many dental service providers affiliated with Defendant. Plaintiff Paras received a patient-oriented Data Breach notice dated December 7, 2020 on or about that date, a copy of which is attached hereto as Exhibit A (the "Patient Notice Letter").

18. Plaintiff Regina Rosario ("Rosario") is and at all times mentioned herein was an individual citizen of the state of Florida, residing in the city of Jacksonville. Prior to the Data Breach, Plaintiff Rosario was an employee of Advanced Dental Care, located in Jacksonville, Florida, which is one of many dental service providers affiliated with Defendant. Plaintiff Rosario received an employee-oriented Data Breach notice dated October 28, 2020, on or around that date.

19. Plaintiff Jennifer Sillah ("Sillah") is and at all times mentioned herein was an individual citizen of the state of Florida, residing in the city of Jacksonville. Prior to the Data Breach, Plaintiff Sillah was an employee of Advanced Dental Care, located in Jacksonville, Florida, which is one of many dental service providers affiliated with Defendant. Plaintiff Sillah received an employee-oriented Data Breach notice dated April 9, 2021 on or about that date, a copy of which is attached hereto as Exhibit B (the "Employee Notice Letter"). Prior to the Data Breach, Ms. Sillah was also a patient of Advanced Dental Care, but she did not receive a patient-oriented notice of the Data Breach.

20. Plaintiff Christian Stephens ("Stephens") is and at all times mentioned herein was an individual citizen of the state of Pennsylvania, residing in the city of Philadelphia. Prior to the Data Breach, Plaintiff Stephens was a patient of Dental Solutions, located in Bala Cynwyd,

Pennsylvania, which is one of many dental services providers affiliated with Defendant. Plaintiff Stephens received a patient-oriented data breach notice in or around December 2020.

21. Plaintiff Evelyn Wallace ("Wallace") is and at all times mentioned herein was an individual citizen of the state of Florida, residing in the city of Lehigh Acres, Florida. Prior to the Data Breach, Plaintiff Wallace was a patient of Towncare Dental, located in Ft. Myers, Florida which is one of many dental services providers affiliated with Defendant. Plaintiff Wallace received a patient-oriented data breach notice in or around December 2020.

22. Plaintiff Tanya Wildrick ("Wildrick") is and at all times mentioned herein was an individual citizen of the state of Florida, residing in the city of Eulee. Prior to the Data Breach, Plaintiff Wildrick was an employee of Advanced Dental Care, located in Jacksonville, Florida, which is one of many dental service providers affiliated with Defendant. Plaintiff Wildrick called the phone number on Defendant's sample breach notice filed with the Attorney General of Maine and confirmed that her PII was exposed in the Data Breach.

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

STATEMENT OF FACTS

A. Nature of Defendant's Businesses

24. 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.

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

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

26. 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.

27. In order to obtain dental health care services or employment, Plaintiffs and Class Members provided Private Information to their respective dental practices and employers, including (a) patient names, addresses, dental diagnoses, treatment information, account numbers, billing information, bank account numbers, and health insurance data and (b) employee names, Social Security numbers, dates of birth, Employee Identification numbers, and financial account numbers.

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

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

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

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

[3] *See* Notice Letter.

B. The Data Breach

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

33. Defendant 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]

34. The data that was accessed by an unauthorized third party during the incident included the Private Information of Plaintiffs and Class Members, including (a) patient names, addresses, dental diagnoses, treatment information, account numbers, billing information, bank account numbers, and health insurance data and (b) employee names, Social Security numbers, dates of birth, Employee Identification numbers, and financial account numbers.

35. From October 2020 to April 2021, Defendant notified Plaintiffs and Class Members of the Data Breach.

36. Defendant advised Plaintiffs 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. Defendant's Privacy Obligations

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

---

[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).

38. Plaintiffs 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.

39. Defendant'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.

40. 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.

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

42. 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]

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

44. 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.*
[7] *Id*. at 15.

45. 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]

46. 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.

47. Defendant breached its obligations to Plaintiffs 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:

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.

48. 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 Plaintiffs' and Class Members' Private Information.

[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).

49. Accordingly, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

D. Defendant's Conduct Violated HIPPA

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

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

52. 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).

53. 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

54. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO 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]

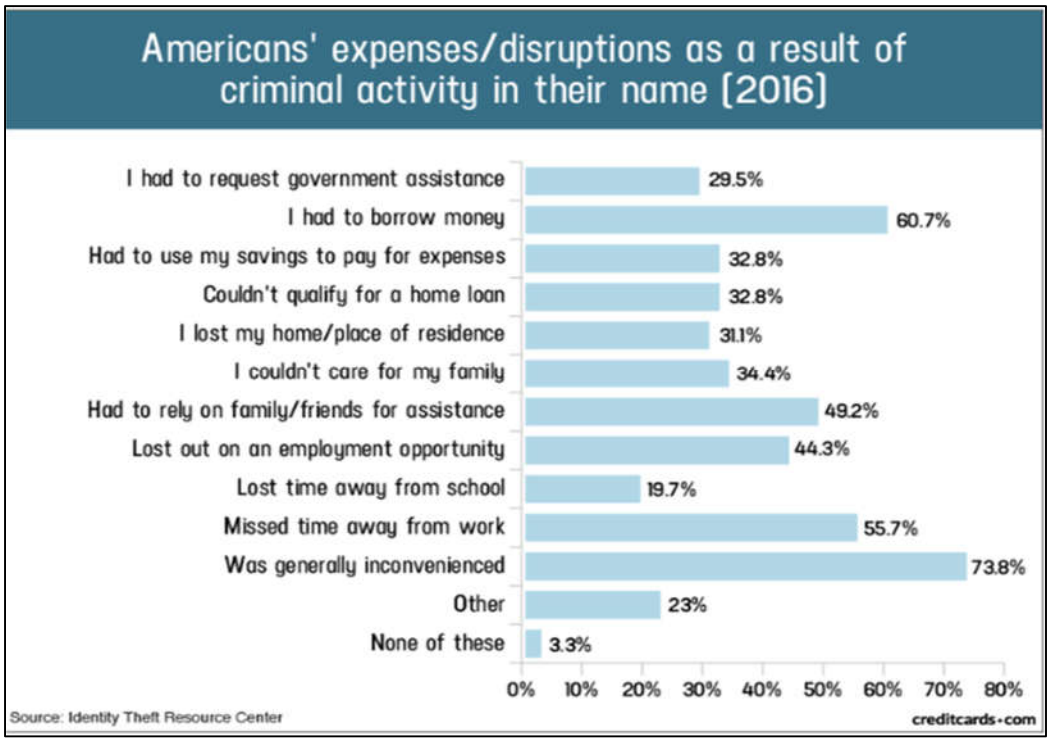
55. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), 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]

56. 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.

57. 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.

[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").
[10] *See* https://www.identitytheft.gov/Steps (last visited Dec. 22, 2020).

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



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

60. 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.

---

[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 Dec. 22, 2020).

[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).

61. 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]

62. 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.

63. 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 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.

64. 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.

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

65. Where the Private Information belonging to Plaintiffs 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 Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

67. Medical information is especially valuable to identity thieves.

68. 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]

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

70. 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.

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

[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).

F. Defendant failed to adequately implement measures to detect and prevent ransomware attacks

72. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[15]

73. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full

[15] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Mar. 15, 2021).

office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[16]

74. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to

[16] *Id.* at 3–4.

verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[17]

75. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

[17] *See* Security Tip (ST19-001) Protecting Against Ransomware (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Mar. 15, 2021).

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[18]

76. Given that Defendant was storing the Private Information of more than 1 million individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

77. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Private Information of more than 1 million individuals, including Plaintiffs and Class Members.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

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

79. Defendant has not even bothered to offer Plaintiffs and Class Members basic credit monitoring.

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

[18] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Mar. 15, 2021).

Plaintiff Paras

81. After the Data Breach, Plaintiff Paras discovered unauthorized use of her Private Information. Indeed, Plaintiff Paras 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.

82. Similarly, after the Data Breach occurred, Plaintiff Paras 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.

Plaintiff Rosario

83. After the Data Breach, Plaintiff Rosario experienced a dramatic increase in "spam" telephone calls.

Plaintiff Sillah

84. After the Data Breach, Plaintiff Sillah experienced a dramatic increase in "spam" telephone calls, which ultimately resulted in Ms. Sillah changing her telephone number in or around April 2021.

Plaintiff Stephens

85. After the Data Breach, an unknown and unauthorized individual attempted to use Plaintiff Stephens' credit card.

Plaintiff Wallace

86. After the Data Breach, Plaintiff Wallace experienced a dramatic increase in "spam" telephone calls.

Plaintiff Wildrick

87. After the Data Breach, someone used Plaintiff Wildrick's Social Security number without authorization to redirect her unemployment compensation payments. This happened multiple times. Ms. Wildrick had to file documents and otherwise spend time to address the issue.

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

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

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

91. Plaintiffs 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.

92. Plaintiffs 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 Plaintiffs and Class Members.

93. Plaintiffs 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.

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

95. Plaintiffs 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.

96. Plaintiffs 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.

97. Moreover, Plaintiffs 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.

98. Further, as a result of Defendant's conduct, Plaintiffs 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.

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

100. 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."[19]

101. 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).[20]

CLASS ACTION ALLEGATIONS

102. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated (the "Class").

103. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All residents of the United States whose Private Information was compromised in the Data Breach (the "Class").

104. Pursuant to O.G.C.A. § 9-11-23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Paras, Stephens, and Wallace assert claims on behalf of a separate subclass, defined as follows:

> All residents of the United States who were patients of Defendant prior to the Data Breach and whose Private Information was compromised in the Data Breach (the "Patients Class").

---

[19] *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.

[20] 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* (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/.

105. Pursuant to O.G.C.A. § 9-11-23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Rosario, Sillah, and Wildrick assert claims on behalf of a separate subclass, defined as follows:

> All residents of the United States who were employees of Defendant prior to the Data Breach and whose Private Information was compromised in the Data Breach (the "Employees Class").

106. Pursuant to O.G.C.A. § 9-11-23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Rosario, Wallace, and Wildrick assert claims on behalf of a separate subclass, defined as follows:

> All residents of Florida whose Private Information was compromised in the Data Breach (the "Florida Class").

107. Pursuant to .G.C.A. § 9-11-23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Stephens asserts claims on behalf of a separate subclass, defined as follows:

> All residents of Pennsylvania whose Private Information was compromised in the Data Breach (the "Pennsylvania Class").

108. Excluded from the Classes 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 Classes are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

109. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

110. Numerosity - O.C.G.A. § 9-11-23(a)(1). The Class Members are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, Class Members include more than

1,000,000 individuals whose data was compromised in the Data Breach. Defendant has reported to the U.S. Department of Health and Human Services that 1,004,304 individuals were affected.

111. Commonality - O.C.G.A. § 9-11-23(a)(2). 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 Plaintiffs' 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 Plaintiffs 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's acts, inactions, and practices violated state statutes;

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

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

112. Typicality - O.C.G.A. § 9-11-23(a)(3).. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of each of Class Members, was compromised in the Data Breach.

113. Adequacy of Representation - O.C.G.A. § 9-11-23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

114. Predominance - O.C.G.A. § 9-11-23(b)(3). Defendant have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' 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.

115. Superiority - O.C.G.A. § 9-11-23(b)(3). 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.

116. 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.

117. Finally, all Class Members are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Some of 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 Plaintiffs and the Nationwide Class)

118. Plaintiffs and the Nationwide Class re-allege and incorporate by reference Paragraphs 1 through 117 above as if fully set forth herein.

119. Plaintiffs and the Nationwide Class were required to submit non-public Private Information to Defendant in order to obtain medical services or employment.

120. 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 Plaintiffs' and the Nationwide Class' 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.

121. Defendant owed a duty of care to Plaintiffs and the Nationwide Class 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.

122. 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 and employees, 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 the Nationwide Class from a data breach.

123. 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.

124. 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.

125. 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.

126. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and the Nationwide Class' 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 Plaintiffs' and the Nationwide Class's Private Information;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and the Nationwide Class's 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 Plaintiffs' and the Nationwide Class's Private Information;

f. Failing to detect in a timely manner that Plaintiffs and the Nationwide Class's Private Information had been compromised; and

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

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

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

129. Plaintiffs and the Nationwide Class are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

130. Plaintiffs and the Nationwide Class 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 the Nationwide Class.

SECOND COUNT

Intrusion Into Private Affairs / Invasion Of Privacy (On Behalf of Plaintiffs and the Nationwide Class)

131. Plaintiffs and the Nationwide Class re-allege and incorporate by reference Paragraphs 1 through 117 above as if fully set forth herein.

132. 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).

133. Plaintiffs and the Nationwide Class had a reasonable expectation of privacy in the Private Information Defendant mishandled.

134. Defendant's conduct as alleged above intruded upon Plaintiffs' and the Nationwide Class' seclusion under common law.

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

136. Defendant knew that an ordinary person in Plaintiffs' and the Nationwide Class' position would consider Defendant's intentional actions highly offensive and objectionable.

137. Defendant invaded Plaintiffs' and the Nationwide Class' right to privacy and intruded into Plaintiffs' and the Nationwide Class' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

138. Defendant intentionally concealed from Plaintiffs and the Nationwide Class an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

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

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

THIRD COUNT

Breach of Express Contract
(On Behalf of Plaintiffs Paras, Stephens, and Wallace and the Patients Class)

141. Plaintiffs Paras, Stephens, and Wallace and the Patients Class re-allege and incorporate by reference Paragraphs 1 through 117 above as if fully set forth herein.

142. Plaintiffs Paras, Stephens, and Wallace and the Patients 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.

143. The valid and enforceable express contracts to provide medical and health care services that Plaintiffs Paras, Stephens, and Wallace and the Patients Class entered into with

Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant.

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

145. Both the provision of medical services healthcare and the protection of Plaintiffs Paras, Stephens, and Wallace's and the Patients Class' Private Information were material aspects of these express contracts.

146. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiffs Paras, Stephens, and Wallace's and the Patients Class' 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 Plaintiffs Paras, Stephens, and Wallace's and the Patients Class's Private Information.

147. 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 Plaintiffs Paras, Stephens, and Wallace and the Patients Class, 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. Plaintiffs Paras, Stephens, and Wallace and the Patients Class 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.

148. A meeting of the minds occurred, as Plaintiffs Paras, Stephens, and Wallace and the Patients 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.

149. Plaintiffs Paras, Stephens, and Wallace and the Patients Class performed their obligations under the contract when they paid for their health care services and provided their Private Information.

150. 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.

151. 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 Plaintiffs Paras, Stephens, and Wallace's and the Patients Class' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs 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 Plaintiffs Paras, Stephens, and Wallace's and the Patients Class' Private Information, as set forth above.

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

153. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs Paras, Stephens, and Wallace and the Patients 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. Plaintiffs Paras, Stephens, and Wallace and the Patients Class 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.

154. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiffs Paras, Stephens, and Wallace, nor the Patients Class, nor any reasonable person would have purchased healthcare from Defendant's affiliated healthcare providers.

155. As a direct and proximate result of the Data Breach, Plaintiffs Paras, Stephens, and Wallace and the Patients Class 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.

156. Plaintiffs Paras, Stephens, and Wallace and the Patients Class are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

FOURTH COUNT

Breach of Express Contract
(On Behalf of Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class)

157. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class re-allege and incorporate by reference Paragraphs 1 through 117 above as if fully set forth herein.

158. Plaintiffs Rosario, Sillah, and Wildrick and the Employees 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 employment.

159. The valid and enforceable express contracts to provide employment that Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant.

160. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide employment to Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class; and (b) protect Plaintiffs Rosario, Sillah, and Wildrick's and the Employees Class' PII/PHI: (i) provided to obtain such employment; and/or (ii) created as a result of providing such employment. In exchange, Plaintiffs Rosario, Sillah, and Wildrick's and the Employees Class's agreed to the employment, and to turn over their Private Information.

161. Both the provision of employment and the protection of Plaintiffs Rosario, Sillah, and Wildrick's and the Employees Class' Private Information were material aspects of these express contracts.

162. The express contracts for the provision of employment – contracts that include the contractual obligations to maintain the privacy of Plaintiffs Rosario, Sillah, and Wildrick's and the Employees Class' 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 Plaintiffs Rosario, Sillah, and Wildrick's and the Employees Class's Private Information.

163. The Employees Class value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To employees such as Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class, employment that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than employment that adheres to industry-standard data security. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class 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.

164. A meeting of the minds occurred, as Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class agreed to and did provide their Private Information to Defendant and/or its affiliated healthcare providers, and accepted the provided employment in exchange for, amongst other things, both the provision of employment and the protection of their Private Information.

165. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class performed their obligations under the contract when they accepted employment and provided their Private Information.

166. 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.

167. 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 Plaintiffs Rosario, Sillah, and Wildrick's and the Employees Class' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and more than 1 million Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTC Act, or otherwise protect Plaintiffs Rosario, Sillah, and Wildrick's and the Employees Class' Private Information, as set forth above.

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

169. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class did not receive the full benefit of the bargain, and instead received employment that was of a diminished value to that described in the contracts. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class therefore were damaged in an amount at least equal to the difference in the value of the employment they accepted and the employment they received.

170. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiffs Rosario, Sillah, and Wildrick, nor the Employees Class, nor any reasonable person would have accepted employment from Defendant's affiliated healthcare providers.

171. As a direct and proximate result of the Data Breach, Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class 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 employment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

172. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

FIFTH COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs Paras, Stephens, and Wallace and the Patients Class)

173. Plaintiffs Paras, Stephens, and Wallace and the Patients Class re-allege and incorporate by reference Paragraphs 1 through 117 above as if fully set forth herein.

174. When Plaintiffs Paras, Stephens, and Wallace and the Patients Class 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.

175. Defendant solicited and invited Plaintiffs Paras, Stephens, and Wallace and the Patients Class to provide their Private Information as part of Defendant's regular business practices. Plaintiffs Paras, Stephens, and Wallace and the Patients Class accepted Defendant's offers and provided their Private Information to Defendant.

176. Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiffs Paras, Stephens, and Wallace's and the Patients Class's Private Information.

177. In entering into such implied contracts, Plaintiffs Paras, Stephens, and Wallace and the Patients Class reasonably believed and expected that Defendant's data security practices

complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

178. Plaintiffs Paras, Stephens, and Wallace and the Patients Class 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.

179. Plaintiffs Paras, Stephens, and Wallace and the Patients Class 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. Plaintiffs Paras, Stephens, and Wallace and the Patients Class 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.

180. Plaintiffs Paras, Stephens, and Wallace and the Patients Class fully and adequately performed their obligations under the implied contracts with Defendant.

181. Defendant breached its implied contracts with Plaintiffs Paras, Stephens, and Wallace and the Patients Class by failing to safeguard and protect their Private Information.

182. As a result of Defendant's failure to fulfill the data security protections promised in these implied contracts, Plaintiffs Paras, Stephens, and Wallace and the Patients 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. Plaintiffs Paras, Stephens, and Wallace and the Patients Class 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.

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

184. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

185. Plaintiffs 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 the Patients Class.

SIXTH COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs Rosario, Sillah, and Wildrick and the Patients Class)

186. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class re-allege and incorporate by reference Paragraphs 1 through 117 above as if fully set forth herein.

187. When Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class provided their Private Information to Defendant in exchange for employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such Private Information.

188. Defendant invited Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class to provide their Private Information as part of Defendant's regular employment practices. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class accepted Defendant's offers and provided their Private Information to Defendant.

189. Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiffs Rosario, Sillah, and Wildrick's and the Employees Class's Private Information.

190. In entering into such implied contracts, Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

191. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class who accepted employment with Defendant reasonably believed and expected that Defendant would obtain adequate data security. Defendant failed to do so.

192. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class 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. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class 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.

193. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class fully and adequately performed their obligations under the implied contracts with Defendant.

194. Defendant breached its implied contracts with Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class by failing to safeguard and protect their Private Information.

195. As a result of Defendant's failure to fulfill the data security protections promised in these implied contracts, Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class did not receive the full benefit of the bargain, and instead received employment that was of a diminished value to that agreed upon in the implied contracts. Plaintiffs Rosario, Sillah, and

Wildrick and the Employees Class therefore were damaged in an amount at least equal to the difference in the value of the employment with data security protection they accepted and the employment they received.

196. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiffs Rosario, Sillah, and Wildrick, nor the Employees Class, nor any reasonable person would have accepted employment from Defendant and/or its affiliated healthcare providers.

197. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

198. Plaintiffs Rosario, Sillah, and Wildrick and the Employees Class 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 the Patients Class.

SEVENTH COUNT

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

199. Plaintiffs and the Nationwide Class re-allege and incorporate by reference Paragraphs 1 through 117 above as if fully set forth herein.

200. 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 Plaintiffs' and the Nationwide Class's Private Information.

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

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

203. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and the Nationwide Class's Private Information.

204. 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).

205. Plaintiffs and the Nationwide Class are within the class of persons that the HIPAA was intended to protect.

206. 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 Plaintiffs and the Nationwide Class.

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

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

209. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and the Nationwide Class, Plaintiffs and the Nationwide Class would not have been injured.

210. The injury and harm suffered by Plaintiffs and the Nationwide Class 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 Plaintiffs and the Nationwide Class to experience the foreseeable harms associated with the exposure of their Private Information.

211. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Nationwide Class have suffered injury and are entitled to compensatory, consequential, and nominal damages in an amount to be proven at trial.

EIGHTH COUNT

Violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 502.201, et seq. (On Behalf of Plaintiffs Rosario, Wallace, and Wildrick and the Florida Class)

212. Plaintiffs Rosario, Wallace, and Wildrick and the Florida Class re-allege and incorporate by reference Paragraphs 1 through 117 above as if fully set forth herein.

213. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained Plaintiffs Rosario, Wallace, and Wildrick' and the Florida Class' Private Information through advertising, soliciting, providing, offering, and/or distributing goods and services or employment to Plaintiffs Rosario, Wallace, and Wildrick and the Florida Class and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

214. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard the Private Information;

b. failure to make only authorized disclosures of the Private Information;

c. failure to timely and accurately disclose the Data Breach to Plaintiffs Rosario, Wallace, and Wildrick and the Florida Class; and

d. failure to disclose that its computer systems and data security practices were inadequate to safeguard the Private Information from theft.

215. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to its current and former patients.

216. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to its current and former patients that it did not follow industry best practices for the collection, use, and storage of the Private Information.

217. As a direct and proximate result of Defendant's conduct, Plaintiffs Rosario, Wallace, and Wildrick and the Florida Class have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

218. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs Rosario, Wallace, and Wildrick and the Florida Class have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

219. Also as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs Rosario, Wallace, and Wildrick and the Florida Class are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment the Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner any Private Information not necessary for its provisions of services or employment;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its current and former patients and employees about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps Defendant's current and former patients must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Nationwide Class, the Patients Class, and the Employees 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 Plaintiffs' 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 Plaintiffs and Class Members;

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

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

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: January 10, 2022

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)*
Ryan Maxey (FL Bar No. 59283)*
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