Andrew W. Ferich (*pro hac vice*)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

[Additional Counsel Listed Below]

Interim Class Counsel

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

KATHLEEN JORDAN, MARLO EASTMAN, EDWINA JACKSON, AMANDA MADUIKE-IWATA, VIRIDIANA TINAJERO MONTERROZA, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

ABSOLUTE DENTAL GROUP, LLC and JUDGE CONSULTING, INC.

Defendants.

Case No. 2:25-cv-00986-JAD-MDC

THIRD AMENDED CLASS ACTION COMPLAINT

CLASS ACTION

JURY DEMAND

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs Kathleen Jordan, Marlo Eastman, Edwina Jackson, Amanda Maduike-Iwata, and Viridiana Tinajero Monterroza (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Absolute Dental Group, LLC ("ADG") and Judge Consulting, Inc. ("JCI") (collectively, "Defendants") based upon personal knowledge with respect to Plaintiffs and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated patients' personally identifiable information ("PII") and protected health information ("PHI"), from criminal hackers, including at least some of the following information, among other sensitive information: full names, dates of birth, health information, dental information and records, doctor's name, health and/or dental insurance information, medical billing or claims information, prescription or medication information, Social Security numbers, treatment information, and financial account data (collectively, "Private Information").

2. ADG is a Nevada-based dental care provider that serves thousands of patients each year. In the ordinary course of its business, ADG collects and stores sensitive Private Information belonging to patients seeking care. In exchange for receiving dental care, ADG's patients entrust their Private Information to ADG with the reasonable expectation and mutual understanding that ADG will safeguard their data from unauthorized access.

3. JCI is a Pennsylvania-based global professional services firm specializing in technology consulting, staffing solutions, and corporate training. JCI provides services to numerous companies, including ADG (hereinafter, the "Clients").

4. Rather than build its own dedicated internal IT and data management team, ADG contracted with JCI to be its managed services provider responsible for daily management and operations of its information systems.

5. Though ADG was responsible for hiring competent contractors, JCI was responsible for managing and maintaining ADG's information systems.

6. Cybersecurity is an integral aspect of all IT professional's job; indeed, JCI's corporate page through the Judge Group represents:

> All Judge employees and contractors are held to the highest security standards and undergo a rigorous cybersecurity training program. All contractors are reminded that they are obligated to treat client data with the utmost care and due diligence. This is clearly communicated upfront and regularly throughout employment.
>
> Some of the ways Judge is working with its employees and contractors to ensure the highest standards of cybersecurity:
>
> - In-depth, multiple module training
> - Ongoing education
> - A commitment to best practices from employees and contractors
> - Clear communication of policies and expectations
> - Reinforcing policy through workplace messaging and materials
> - Updated and easily accessible Security Operations Manual[1]

7. JCI does not make these representations gratuitously; the cybersecurity proficiency of their employees is a key factor in their client's decision to entrust their information systems and the digital assets stored therein to JCI's team.

8. Moreover, JCI and all Judge Group companies represent that they have particular expertise in the healthcare industry.[2]

9. Thus, on information and belief, ADG entrusted its information systems to JCI, including by trusting that JCI's engineers and other staff would competently protect the PII and PHI stored thereon and JCI understood that cybersecurity was a pivotal role inherent in its function as ADG's managed services provider—as is made clear by JCI's own statements regarding its focus on preparing its employees to face cybersecurity threats and risks.

[1] *Corporate Policies*, The Judge Group Inc., https://www.judge.com/about-judge/corporate-policies (last visited Nov. 7, 2025).

[2] *Industries We Serve*, The Judge Group, Inc., https://www.judge.com/industries/ (last visited Nov. 7, 2025).

10. On February 26, 2025, ADG became aware of a potential issue involving its information systems.[3] In response, ADG took steps to secure its systems and investigate the nature and scope of the Data Breach.[4] ADG's investigation determined that an unauthorized party accessed some of its systems between February 19, 2025 and March 5, 2025.[5] Based on its investigation, the unauthorized access appears to have originated from the inadvertent execution of a malicious version of a legitimate software tool, which occurred through an account associated with ADG's third-party managed services provider, JCI.

11. As part of its investigation, ADG assessed what sensitive personal information may have been impacted in connection with the event.[6] ADG's assessment concluded on July 28, 2025, and determined that the following types of Private Information may have been compromised as a result of the Data Breach: name, contact information, date of birth, Social Security number, driver's license or state-issued ID information, passport or other governmental ID information, and health information, which may include health history, treatment and diagnosis information, explanation of benefits, health insurance information, and/or MRN number or patient identification number, financial account and/or payment card information.[7]

12. On or about May 2, 2025, ADG filed its first public notice about the Data Breach with the United States Department of Health and Human Services Office for Civil Rights ("HHS OCR").[8] Recently, ADG published a notice on its website about the Data Breach.

13. JCI has yet to issue any public disclosure of the Data Breach.

14. To date, ADG and JCI have not sent notice to individuals whose information was accessed in the Data Breach. Upon information and belief, the Data Breach impacted current and former patients of ADG.

---

[3] *Notice of Data Incident*, Absolute Dental, https://www.absolutedental.com/notice-of-a-data-incident/ (last visited Nov. 7, 2025).
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health and Human Services Office for Civil Rights https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 7, 2025)

15. Though little is known about the Data Breach at this time, what is known establishes that Defendants failed to implement reasonable cybersecurity measures. For example, the hackers were able to infiltrate Defendants information systems, perform the necessary reconnaissance efforts, identify valuable files, gain access to those files, and download data without being caught. The fact that the hackers could perform these noisy operations all without being caught strongly suggests that Defendants failed to implement the necessary monitoring and alerting tools, like endpoint detection and response tools, sufficient to be able to timely identify malicious activity to empower its cybersecurity staff to stop or limit the attack.

16. Defendants have provided no assurance that all personal data or copies of data have been recovered or destroyed, or that they have adequately enhanced their data security practices sufficient to avoid a similar breach of their networks in the future.

17. The potential for improper disclosure and theft of Plaintiffs' and Class members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

18. Upon information and belief, Defendants failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information.

19. The healthcare industry is a prime target for ransomware attacks such as this because these organizations store vast amounts of sensitive data, including medical records, financial information, and personal identification details.[9] This data is incredibly valuable on the black market, where it can be sold for purposes such as identity theft and insurance fraud.[10] The high demand for this data makes healthcare a lucrative target for cybercriminals.[11]

[9] *Safeguarding Patient Data: Why Healthcare is a Prime Target for Cybercrime*, RavenTek, (June 11, 2024, https://www.raventek.com/safeguarding-patient-data-why-healthcare-is-a-prime-target-for-cybercrime/#:~:text=help%20mitigate%20risks.-,High%20Value%20of%20Patient%20Data,identity%20theft%20and%20insurance%20fraud.

[10] *Id.*

[11] *Id.*

20. Plaintiffs' and Class members' identities are now at risk because of Defendants' conduct, as the Private Information that Defendants collected and maintained is now in the hands of data thieves and other unauthorized third parties. Plaintiffs and Class members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminution of the value of their Private Information, loss of privacy, and additional damages as described below.

21. Plaintiffs bring this class action lawsuit to address Defendants' inadequate safeguarding of Class members' Private Information that they collected and maintained, and their failure to provide timely and adequate notice to Plaintiffs and Class members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

22. Plaintiffs, individually and on behalf of the Class, asserts claims for (i) negligence; (ii) negligence per se; (iii) breach of contract, (iv) breach of implied contract; (v) unjust enrichment; (vi) breach of fiduciary; (vii) breach of confidence; (viii) invasion of privacy (ix) violations of the Nevada Privacy of Information Collected on the Internet From Consumers Act, Nev. Rev. Stat. § 603A; and (x) declaratory and injunctive relief.

II. PARTIES

Plaintiffs

23. Plaintiff **Kathleen Jordan** is, and at all times mentioned herein, an individual citizen of the State of Nevada.

24. Plaintiff **Marlo Eastman** is, and at all times mentioned herein, an individual citizen of the State of Nevada.

25. Plaintiff **Edwina Jackson** is, and at all times mentioned herein, an individual citizen of the State of Nevada.

26. Plaintiff **Amanda Maduike-Iwata** is, and at all times mentioned herein, an individual citizen of the State of Nevada.

27. Plaintiff **Viridiana Tinajero Monterroza** is, and at all times mentioned herein , an individual citizen of the State of Nevada.

Defendants

28. Defendant **Absolute Dental Group, LLC** is Delaware limited liability company with its principal place of business located at 8370 W. Cheyenne Ave., Ste. 103, Las Vegas, Nevada 89129. Defendant's registered agent is The Corporation Trust Company of Nevada, located at 701 S. Carson St. Suite 200, Carson City, NV, 89701.

29. Defendant **Judge Consulting, Inc.** is a Delaware corporation with its principal place of business located at 151 South Warner Road, Ste. 100, Wayne, Pennsylvania, 19087.

III. JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class members, the aggregated claims of the individual Class members exceed the sum or value of $5,000,000 exclusive of interest and costs, and, upon information and belief, members of the proposed Class are citizens of states different from Defendants.

31. This Court has jurisdiction over Defendants through their business operations in this District, the specific nature of which occurs in this District. Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

32. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, and because Defendant ADG resides in this judicial district.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

IV. FACTUAL ALLEGATIONS

A. Defendants Businesses and Collection of Plaintiffs' and Class Members' Private Information

33. ADG is a Nevada-based dental service organization with over fifty locations.[12] ADG provides comprehensive dental services ranging from general dental and hygienist services to orthodontics, oral surgery, pedodontics, and endodontics.[13]

34. JCI is a Pennsylvania-based global professional services firm specializing in technology consulting, staffing solutions, and corporate training. JCI provides services to its Clients, including ADG.

35. As a condition of doing business, ADG requires that its patients entrust it with highly sensitive Private Information.

36. As a condition of doing business, JCI requires that its Clients entrust it with sensitive Private Information belonging to their patients.

37. Upon information and belief, Defendants made promises and representations to individuals', including Plaintiffs and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

38. Due to the highly sensitive and personal nature of the information Defendants acquire and store with respect to patients, Defendants also implicitly or explicitly promise to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of patients' Private Information; inform patients of their legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services provided; and provide adequate notice to patients if their Private Information is disclosed without authorization.

---

[12] *Connect With a Trusted General Dentist in Nevada*, Absolute Dental, https://www.absolutedental.com/about/general-dentists/ (last visited Nov. 7, 2025).

[13] *About*, Absolute Dental, https://www.absolutedental.com/about/ (last visited Nov. 7, 2025).

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, Defendants assumed legal and equitable duties they owed to them and knew or should have known that they were responsible for protecting Plaintiffs' and Class members' Private Information from unauthorized disclosure and exfiltration.

40. Defendants recognized their duty to protect and safeguard Plaintiff's and Class members' Private Information. ADG makes the following claim on its website, "We implement a variety of security measures to maintain the safety of your personal information when you enter, submit, or access your personal information . . . ."[14] JCI makes the following claim on its website, "Judge supports online security using secure server technology because we want your data to be safe. We use state-of-the-art security arrangements and facilities on our Sites and through the Judge Services to maintain data security."[15]

41. Current and former patients and employees of ADG, such as Plaintiffs and Class members, made their Private Information available to ADG with the reasonable expectation that any entity with access to this information, including JCI, would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

42. This expectation was objectively reasonable and based on an obligation imposed on Defendants by statute, regulations, industrial custom, and standards of general due care.

43. Plaintiffs and Class members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendants ultimately failed to do.

44. Unfortunately for Plaintiffs and Class members, Defendants failed to carry out their duties to safeguard sensitive Private Information and provide adequate data security. As a

[14] *Privacy Policy*, Absolute Dental, https://www.absolutedental.com/privacy-policy/ (last visited Nov. 7, 2025

[15] *Privacy & Cookies Policy*, The Judge Group, Inc., https://www.judge.com/privacy/ (last visited Nov. 7, 2025)

result, Defendants failed to protect Plaintiffs and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

45. On February 26, 2025, ADG became aware of a potential issue involving its information systems.[16] In response, ADG took steps to secure its systems and investigate the nature and scope of the Data Breach.[17] ADG's investigation determined that an unauthorized party accessed some of its systems between February 19, 2025 and March 5, 2025.[18] Based on its investigation, the unauthorized access appears to have originated from the inadvertent execution of a malicious version of a legitimate software tool, which occurred through an account associated with ADG's third-party managed services provider, JCI.

46. As part of its investigation, ADG assessed what sensitive personal information may have been impacted in connection with the event.[19] ADG's assessment concluded on July 28, 2025, and determined that the following types of Private Information may have been compromised as a result of the Data Breach: name, contact information, date of birth, Social Security number, driver's license or state-issued ID information, passport or other governmental ID information, and health information, which may include health history, treatment and diagnosis information, explanation of benefits, health insurance information, and/or MRN number or patient identification number, financial account and/or payment card information.[20]

47. On or about May 2, 2025, ADG filed its first public notice about the Data Breach with the HHS.[21] Recently, ADG published a notice on its website about the Data Breach.

48. JCI has yet to issue any public disclosure of the Data Breach.

[16] *Notice of Data Incident*, *supra*.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, *supra*.

49. To date, ADG and JCI have not sent notice to individuals whose information was accessed in the Data Breach. Upon information and belief, the Data Breach impacted current and former patients of ADG.

50. Upon information and belief, highly sensitive Private Information was accessed and acquired by cybercriminals during the Data Breach because that is the *modus operandi* of cybercriminals who perpetrate ransomware attacks against healthcare entities such as ADG. As such, there is no question Plaintiff's and Class Members' Private Information is in the hands of cybercriminals who will use the stolen Private Information for nefarious purposes for the rest of their lives.

51. To date, Defendants have failed to disclose crucial details, including: (i) an explanation as to why Defendants allowed the Data Breach to occur, (ii) the root cause of the Data Breach, (iii) the vulnerabilities exploited, (iv) the remedial measures undertaken to ensure such a breach does not occur again, (vii) the extent of the Data Breach and information that was accessed by the hackers, and (v) the steps that victims of the Data Breach should take to protect themselves.

52. To date, these critical facts have not been explained or clarified to Plaintiffs and Class members, who retain a vested interest in ensuring that their Private Information is protected.

53. Upon information and belief, Defendants know individuals' Private Information were compromised in the Data Breach but have yet to individually notify the victims.

54. Defendants have yet to inform Plaintiffs and Class members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

55. In addition, Defendants' offer no substantive steps to help victims like Plaintiffs and Class members to protect themselves.

56. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class members to keep Plaintiffs' and Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

57. Plaintiffs and Class members provided their Private Information to ADG with the reasonable expectation and mutual understanding that ADG, and third-party vendors such as JCI, would comply with their obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

58. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

59. Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

C. Defendants' Failed to Protect Plaintiffs' and Class Members' Private Information

60. Defendants collect and maintain vast quantities of Private Information belonging to Plaintiffs and Class members as part of their normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendants.

61. First, Defendants inexcusably failed to implement reasonable security protections to safeguard their information systems and databases.

62. Second, Defendants failed to inform the public that their data security practices were deficient and inadequate. Had Plaintiffs and Class members been aware that Defendants did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided their Private Information to Defendants.

63. In addition to the failures that led to the successful breach, Defendants failings in handling the breach and responding to the incident exacerbated the resulting harm to the Plaintiffs and Class members.

64. Defendants delay in informing victims of the Data Breach that their Private Information was compromised virtually ensured that the cybercriminals who stole this Private Information could monetize, misuse and/or disseminate that Private Information before the Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

65. Additionally, Defendants failure to attempt to ameliorate the effects of this Data Breach and mitigate the harm they caused is woefully inadequate. Plaintiffs' and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information is immutable.

66. In short, Defendants myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiffs and Class members that their Private Information had been stolen due to Defendants security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiffs' and Class members' Private Information for a significant amount of time victims are able to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Defendants Knew or Should Have Known of the Risk Because Institutions in Possession of Private Information are Susceptible to Cyberattacks

67. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendants'.

68. Data thieves regularly target institutions like Defendants due to the highly sensitive information in their custody. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

69. In 2021, a record 3,205 data breaches occurred, resulting in approximately 353,027,892 individuals being compromised, a 78% increase from 2022.[22]

[22] *ITRC 2023 Data Breach Report – Key Findings and Solutions*, Bluefin, (Jan. 29, 2024), https://www.bluefin.com/bluefin-news/itrc-2023-data-breach-report-key-findings-and-solutions/.

70. As a custodian of Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them, and of the foreseeable consequences if their data security systems, or those belonging to third-party vendors, were breached, including the significant costs imposed on Plaintiffs and Class members as a result of a breach.

71. Despite the prevalence of public announcements of data breaches and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from being compromised.

72. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants server(s), amounting to potentially tens or hundreds of thousands of individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

73. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class members.

74. The ramifications of Defendants failure to keep secure the Private Information of Plaintiffs and Class members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

E. Defendants Knew or Should Have Known that Healthcare Institutions are Particularly Susceptible to Cyberattacks

75. According to the Center for Internet Security, "the health industry experiences more data breaches than any other sector." This is because "Personal Health Information (PHI) is more valuable on the black market than credit card credentials or regular Personally Identifiable Information (PII). Therefore, there is a higher incentive for cyber criminals to target medical databases. They can sell the PHI and/or use it for their own personal gain."

76. "In 2023, more than 540 organizations and 112 million individuals were implicated in healthcare data breaches reported to the HHS Office for Civil Rights (OCR), compared to 590 organizations and 48.6 million impacted individuals in 2022."[23]

77. "The number of cybersecurity attacks disrupting the healthcare sector has continued to be a growing concern. In the last three years, more than 90% of all healthcare organizations have reported at least one security breach which can manifest in denial of service, malicious code, ransomed data, and more."[24]

78. "Healthcare organi[z]ations are rich targets for cybercriminals because they hold a large amount of sensitive patient data. This data can be used to commit identity theft or fraud or sold on the black market. Hackers can access this data in many ways, including phishing emails, malware, and unsecured networks."[25]

79. It is no secret that "[h]ealthcare data breaches are reaching record highs. Indeed, healthcare now sees more cyberattacks than any other industry. Fully one-third of all cyberattacks are aimed at healthcare institutions. Why? Because healthcare is a valuable and vulnerable target. Hospitals and healthcare institutions are a prime target for cybercrime due to the vast amount of sensitive data they hold."[26]

80. Theft of PHI 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."[27]

---

[23] *This Year's Largest Healthcare Data Breaches*, HEALTH IT SECURITY (Dec. 26, 2023), https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches.

[24] *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html.

[25] Troy Beamer, *What Industries Are Most Vulnerable to Cyber Attacks In 2024?*, TECHNEWS (Feb. 27, 2024), https://www.techbusinessnews.com.au/what-industries-are-most-vulnerable-to-cyberattacks-in-2022/.

[26] *What Industries Are Most Vulnerable to Cyberattacks?*, PSM Technology Talent, https://www.psmpartners.com/blog/most-targeted-industries-for-cyber-attacks/ (last visited Nov. 7, 2025)

[27] *Medical I.D. Theft*, EFraudPrevention https://efraudprevention.net/home/education/?a= 187 (last visited Nov. 7, 2025).

81. Medical-related identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013[,]" which is more than identity thefts involving banking and finance, the government and the military, or education.[28]

82. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the health care industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

83. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[29] Indeed, during 2019 alone, over 41 million health care records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[30] In short, these sorts of data breaches are increasingly common, especially among health care systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[31]

84. The healthcare industry is frequently recognized as one of the most vulnerable industries for a cyberattack.[32]

---

[28] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

[29] Adil Hussain She Et Al., *Healthcare Data Breaches: Insights and Implications* (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/.

[30] Steve Alder, *December 2019 Healthcare Data Breach Report*, The HIPAA Journal (Jan. 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.

[31] Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches*, Tenable (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

[32] *See, e.g.*, *id.*; Liudmyla Pryimenko, *The 7 Industries Most Vulnerable to Cyberattacks*, EKRAN (Mar. 25, 2024), https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches; Ani Petrosyan, *Distribution of cyberattacks across worldwide industries in 2023*, STATISTA (Mar. 22, 2024), https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/; *6 Industries Most Vulnerable to Cyber Attacks*, *supra*.

85. The American Dental Association ("ADA") has even published recommendations to help protect dental practices from cyberattacks.[33]

86. In light of recent high profile data breaches at other healthcare providers, Defendants knew or should have known that the Private Information they collected and maintained would be targeted by cybercriminals.

87. Defendants should have been aware, and indeed were aware, that they were at risk of a data breach that could expose the Private Information that they solicited, collected, stored, and maintained, especially given the rise of healthcare data breaches.

88. Defendants recognized they had a duty to use reasonable measures to protect the Private Information that they solicited, collected, and maintained but failed to do so.

89. Defendants were aware of the risks and harm that could result from inadequate data security but threw caution to the wind.

F. Private Information is Valuable, and the Effects of Theft are Serious

90. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[34]

91. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[36]

[33] *Tips to Safeguard Your Practice from Computer Hackers*, American, Dental Association, https://www.ada.org/resources/practice/practice-management/tips-to-safeguard-your-practice-from-computer-hackers (last visited Nov. 7, 2025).
[34] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Aug. 28, 2025).
[35] 17 C.F.R. § 248.201 (2013).
[36] *Id.*

92. Private Information is of great value to hackers and cybercriminals, and the data allegedly compromised in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiffs and Class members and to profit off their misfortune.

93. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[37]

94. For example, Private Information can be sold at a price ranging from $40 to $200.[38] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[39]

95. PHI is even more valuable on the black market than PII.[40]

96. "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place."[41] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[42]

97. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[43]

[37] *Your Personal Data is For Sale on the Dark Web. Here's How Much it Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[38] *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[39] *In the Dark*, VPNOVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 7, 2025).

[40] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited Nov. 7,, 2025).

[41] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015) https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[42] *Managing Cyber Risks in an Interconnected World: Key Findings From the Global State of Information Security Survey 2015*, PRICE WATERHOUSE COOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[43] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

98. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[44]

99. When cybercriminals manage to steal health insurance information and other personally sensitive data—as alleged here—there is no limit to the amount of fraud to which Plaintiffs and Class members are exposed.

100. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.

101. The Data Breach at issue here was targeted and financially motivated, as the only reason cybercriminals go through the trouble of hacking healthcare entities and companies that maintain PHI, such as Defendants, is to steal the highly sensitive information they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

102. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for health care they did not receive to restore coverage.[45] Almost half of medical identity theft victims lose their health care coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[46]

103. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—PHI and names—is impossible to "close" and difficult, if not impossible, to change.

---

[44] Michael Ollove, *supra*.
[45] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[46] *Id*.

104. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[47]

105. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

106. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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.[48]

107. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:.

> [I]n 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.

108. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

109. Defendants has yet to even offer identity monitoring services to Plaintiffs and the Class. Even if they did provide limited coverage, it would be woefully inadequate and would not

---

[47] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[48] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

fully protect Plaintiffs and the Class from the damages and harm caused by Defendants negligent failure to secure and protect their Private Information.

110. The unfortunate truth is the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used.

111. Plaintiffs and Class members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Defendants negligence.

112. Furthermore, identity monitoring services only alert someone to the fact that they have already been the victim of identity theft—it does not prevent identity theft.

113. Nor can an identity monitoring service remove Private Information from the dark web.[49]

114. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[50]

115. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have been damaged and placed at an imminent and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and medical records for unauthorized activity for years to come.

116. Even more serious is the identity restoration that Plaintiffs and other Class members must go through, which can require spending countless hours filing police reports, filling out IRS forms, completing Federal Trade Commission checklists and Department of Motor

[49] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[50] *Id.*

Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

117. Plaintiffs and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property, including their Private Information;

c. Improper disclosure and theft of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their Private Information;

f. Ascertainable losses in the form of time taken to respond to identity theft, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of diminution of the value of Plaintiffs' and Class members' Private Information, for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

l. Moreover, Plaintiffs and Class members have an interest in ensuring that their Private Information, which remains in the possession of Defendants, is protected from further breaches through the implementation of industry standard security

measures and safeguards. Defendants have shown themselves wholly incapable of protecting Plaintiffs' and Class members' Private Information.

118. Plaintiffs and Class members also have an interest in ensuring that their Private Information is removed from all of Defendants servers, systems, and files.

119. Upon information and belief, given the kind of Private Information Defendants made accessible to hackers, Plaintiffs and the Class are certain to incur additional damages.

120. Upon information and belief, because identity thieves have their Private Information, Plaintiffs and Class members will need to have identity theft monitoring protection for the rest of their lives.

121. None of this should have happened because the Data Breach was entirely preventable.

G. Defendants had a Duty to Protect Private Information Under the Law and the Applicable Standard of Care

122. By providing healthcare related services, collecting Private Information from Plaintiffs and Class members as a condition of those services, and storing data containing highly sensitive Private Information, Defendants assumed a duty to safeguard that information from unauthorized access or disclosure.

123. As entities handling medical data and providing services to healthcare organizations, Defendants are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

124. Defendants were also prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce[.]" The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

125. Defendants are further required by various states' laws and regulations to protect Plaintiffs' and Class members' Private Information.

126. Defendants, as data collectors, were required by The Nevada Privacy of Information Collected on the Internet from Consumers Act, Nev. Rev. Stat. § 603A ("NPICICA"), to "implement and maintain reasonable security measures to protect those [Private Information] records from unauthorized access, acquisition, destruction, use, modification, or disclosure." Nev. Rev. Stat. § 603A.210.

127. Defendants owed a duty to Plaintiffs and the Class to design, maintain, and test their systems, and those belonging to third-party vendors, to ensure that the Private Information in their possession and control were adequately secured and protected.

128. Defendants owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the Private Information in their possession, and third-party vendors possession, including adequately training their employees (and any others who accessed Private Information within its computer systems) on how to adequately protect Private Information.

129. Defendants owed a duty to Plaintiffs and the Class to implement processes that would detect a breach of their data security systems in a timely manner.

130. Defendants owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

131. Defendants owed a duty to Plaintiffs and the Class to adequately train and supervise their employees to identify and avoid any phishing emails that make it past their email filtering service.

132. Defendants owed a duty to Plaintiffs and the Class to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in individuals' decisions to entrust Defendants with their Private Information.

133. Defendants owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

134. Defendants owed a duty of care to Plaintiffs and the Class because they were foreseeable and probable victims of any inadequate data security practices.

135. Because Defendants collected and stored sensitive Private Information, they were required to comply with federal laws such as HIPAA, HITECH, and the FTC Act, as well as applicable state laws. It was also expected to follow regulatory guidance and implement reasonable safeguards consistent with standards issued by agencies like the FTC, FBI, CISA, and industry standards.

H. Defendants Failed to Comply with FTC Guidelines

136. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

137. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

138. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

139. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

140. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of their data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

141. Defendants were at all times fully aware of their obligation to protect the Private Information of consumers under the FTCA, yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

I. Defendants Failed to Comply with HIPAA

142. On information and belief, Defendants are covered entities under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA's Standards for Privacy of Individually Identifiable Health Information, and Security Standards for the Protection of Electronic Protected Health Information.

143. On information and belief, Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

144. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

145. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

146. HIPAA requires "comply[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

147. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

148. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

149. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

150. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not

permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

151. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

152. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

153. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

154. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.

155. Defendants were at all times fully aware of its HIPAA obligations to protect the Private Information of consumers yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants conduct was particularly unreasonable given the nature and amount of Private

Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

J. Defendants Failed to Follow FBI Guidelines

156. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."

157. To prevent and detect the Breach, Defendants could and should have taken, as recommended by the Federal Bureau of Investigation, the following measures:

a. Implemented 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.

b. Enabled 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.

c. Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configured firewalls to block access to known malicious IP addresses.

e. Patched operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Managed 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.

h. Configured 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.

i. Disabled macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implemented 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.

k. Considered disabling Remote Desktop protocol (RDP) if it is not being used.

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

m. Executed operating system environments or specific programs in a virtualized environment.

n. Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

158. Upon information and belief, Defendants failed to do any of the above.

K. Defendants Failed to Follow CISA Guidelines

159. The United States Cybersecurity & Infrastructure Security Agency, recommends the following actions to prevent ransomware:

a. **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.

b. **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).

c. **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.

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

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

f. **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.

g. **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[51]

160. Defendants could have and should have taken the above measures to prevent the Breach. Upon information and belief, Defendants failed to do any of the above.

L. Defendants Failed to Comply with Industry Standards

161. Experts studying cybersecurity routinely identify health care providers and entities maintaining PHI like Defendants as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

[51] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (internal citations omitted).

162. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Defendants, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

163. Other best cybersecurity practices that are standard within healthcare networks that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

164. Defendants failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of: the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04); the NIST Special Publications 800-53, 53A, or 800-171; the Center for Internet Security's Critical Security Controls (CIS CSC); and the Federal Risk and Authorization Management Program (FEDRAMP). All of these are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class members' Private Information, resulting in the Data Breach.

165. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

M. Defendants Breached Their Duty to Safeguard Plaintiffs' and Class Members' Private Information

166. In addition to its obligations under federal laws, Defendants owed duties to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Class members.

167. Defendants breached their obligations to Plaintiffs and Class members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data, those belonging to third-party vendors, and failed to audit, monitor, or ensure the integrity of their data security practices. Defendants unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect consumers' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to adhere to industry standards for cybersecurity as discussed above; and

e. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class members' Private Information.

168. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class members' Private Information by allowing cyberthieves to access their computer network and systems, or those belonging to third-party vendors, which contained unsecured and unencrypted Private Information.

169. Had Defendants remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiffs' and Class members' confidential Private Information.

N. Plaintiffs and Class Members Suffered Common Injuries and Damages

170. As a result of Defendants ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession

of criminals, the risk of identity theft to the Plaintiffs and Class members has materialized and is imminent, and Plaintiffs and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; and (e) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Private Information.

Increased and Imminent Risk of Identity Theft

171. Plaintiffs and Class members are at a heightened risk of identity theft for years to come as a result of the Data Breach.

172. The unencrypted Private Information of Class members will end up for sale on the dark web because that is the *modus operandi* of cybercriminals that commit attacks of this type. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class members.

173. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

174. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

175. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a

victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

176. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[52]

177. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

178. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

[52] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

179. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

180. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiffs' and Class members' Private Information is affected because such information is commonly used to commit fraud.

181. By spending this time, Plaintiffs are not manufacturing their own harm but taking necessary steps at ADG direction and because the Data Breach included Plaintiffs' Private Information.

182. Plaintiffs and Class members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

183. These efforts are consistent with the U.S. Government Accountability Office's 2007 report regarding data breaches ("GAO Report"), in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[53]

184. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach,

[53] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* United States Government Accountability Office, GAO-07-737, (June 2007), https://www.gao.gov/new.items/d07737.pdf.

including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven 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.[54]

Diminished Value of Private Information

185. PII and PHI are valuable property rights.[55] Their 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 a doubt that Private Information has considerable market value.

186. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[56]

187. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[57]

188. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[58]

189. As a result of the Data Breach, Plaintiffs' and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class members for their property, resulting in an

[54] *See Identity Theft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited Aug. 28, 2025).

[55] *See, e.g.*, John T. Soma Et Al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, 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).

[56] David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak,* LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[57] *Main Page*, Data Coup Inc., https://datacoup.com/ (last visited Nov. 7, 2025).

[58] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Nov. 7, 2025).

economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

190. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class members, and of the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

191. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on their network, which upon information and belief, amounts to tens or hundreds of thousands of individuals' Private Information, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

192. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class members.

O. The Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.

193. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes.

194. Even if the Private Information is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

195. Such fraud may go undetected for years; consequently, Plaintiffs and Class members are at a present and continuous risk of fraud and identity theft for many years into the future.

196. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class members would not need to bear but for Defendants failure to safeguard their Private Information.

P. Plaintiffs' Experience

Plaintiff Kathleen Jordan

197. Plaintiff Kathleen Jordan is a current patient of ADG and provided her Private Information to ADG as a condition of receiving dental services.

198. Plaintiff Jordan values the privacy and security of her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

199. Plaintiff Jordan reasonably believed that her Private Information would be protected, and that ADG, and any third-party vendor ADG contracts with, including JCI, would implement and maintain reasonable data security measures to safeguard it from unauthorized access, use, or disclosure.

200. Had Plaintiff Jordan known that Defendants do not adequately protect Private Information, Plaintiff Jordan would not have used ADG's services nor agreed to provide Defendants with Private Information.

201. At the time of the Data Breach, Defendants retained Plaintiff Jordan's Private information in its systems, including but not limited to: Plaintiff Jordan's full name, date of birth, health information, dental information and records, health and/or dental insurance information, medical billing or claims information, prescription or medication information, Social Security number, treatment information, and financial account data.

202. Upon information and belief, Plaintiff Jordan's Private Information was compromised in the Data Breach and stolen by unauthorized individuals who unlawfully accessed Defendants network to obtain the sensitive Private Information.

203. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Jordan will need to maintain heightened measures for years, and possibly for life.

204. As a result of the Data Breach, Plaintiff Jordan has suffered loss of time, interference, and inconvenience, as well as anxiety and emotional distress related to the increased risk of identity theft and loss of privacy.

205. Plaintiff Jordan has suffered imminent and impending injury from the substantially heightened risk of identity theft, fraud, and misuse resulting from the exposure of her Private Information in the Data Breach.

206. Plaintiff Jordan has suffered actual injury from having her Private Information compromised as a result of the Data Breach, including but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ADG did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her Private Information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has likely been stolen and published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that ADG obtained from Plaintiff Jordan and/or her medical providers; and (g) other economic and non-economic harm.

207. Specifically, following the Data Breach, Plaintiff Jordan has suffered injuries when she was a victim of identity theft, in which an authorized individual opened a PayPal account in Plaintiff Jordan's name, and incurred charges or debt associated with that account.

208. Plaintiff Jordan has taken reasonable steps to mitigate the impact of the Data Breach, including researching the data breach, reviewing credit reports, monitoring accounts, and taking steps to prevent further harm. Plaintiff Jordan spent more than 4 hours dealing with the Data Breach, valuable time she would have spent on other activities, including, but not limited to, work and recreation. This is time spent that has been lost forever and cannot be recaptured.

209. Plaintiff Jordan has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendants, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff Jordan's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Marlo Eastman

210. Plaintiff Marlo Eastman is a current patient of ADG and provided her Private Information to ADG as a condition of receiving dental services.

211. Plaintiff Eastman values the privacy and security of her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

212. Plaintiff Eastman reasonably believed that her Private Information would be protected, and that ADG, and any third-party vendor ADG contracts with, including JCI, would implement and maintain reasonable data security measures to safeguard it from unauthorized access, use, or disclosure.

213. Had Plaintiff Eastman known that Defendants do not adequately protect Private Information, Plaintiff Eastman would not have used ADG's services nor agreed to provide Defendants with Private Information.

214. At the time of the Data Breach, Defendants retained Plaintiff Eastman's Private information in its systems, including but not limited to: Plaintiff Eastman's full name, date of birth, health information, dental information and records, health and/or dental insurance information, medical billing or claims information, prescription or medication information, Social Security number, treatment information, and financial account data.

215. Upon information and belief, Plaintiff Eastman's Private Information was compromised in the Data Breach and stolen by unauthorized individuals who unlawfully accessed Defendants network to obtain the sensitive Private Information.

216. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Eastman will need to maintain heightened measures for years, and possibly for life.

217. As a result of the Data Breach, Plaintiff Eastman has suffered loss of time, interference, and inconvenience, as well as anxiety and emotional distress related to the increased risk of identity theft and loss of privacy.

218. Plaintiff Eastman has suffered imminent and impending injury from the substantially heightened risk of identity theft, fraud, and misuse resulting from the exposure of her Private Information in the Data Breach.

219. Plaintiff Eastman has suffered actual injury from having her Private Information compromised as a result of the Data Breach, including but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ADG did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her Private Information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has likely been stolen and published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that ADG obtained from Plaintiff Eastman and/or her medical providers; and (g) other economic and non-economic harm.

220. Plaintiff Eastman has taken reasonable steps to mitigate the impact of the Data Breach, including researching the data breach, reviewing credit reports, monitoring accounts, and taking steps to prevent further harm. Plaintiff Eastman spent several hours dealing with the Data Breach, valuable time she would have spent on other activities, including, but not limited to, work and recreation. This is time spent that has been lost forever and cannot be recaptured.

221. Plaintiff Eastman has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendants, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff Eastman's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Edwina Jackson

222. Plaintiff Edwina Jackson is a current patient of ADG and provided her Private Information to ADG as a condition of receiving dental services.

223. Plaintiff Jackson values the privacy and security of her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

224. Plaintiff Jackson reasonably believed that her Private Information would be protected, and that ADG, and any third-party vendor ADG contracts with, including JCI, would implement and maintain reasonable data security measures to safeguard it from unauthorized access, use, or disclosure.

225. Had Plaintiff Jackson known that Defendants do not adequately protect Private Information, Plaintiff Jackson would not have used ADG's services nor agreed to provide Defendants with Private Information.

226. At the time of the Data Breach, Defendants retained Plaintiff Jackson's Private information in its systems, including but not limited to: Plaintiff Jackson's full name, date of birth, health information, dental information and records, health and/or dental insurance information, medical billing or claims information, prescription or medication information, Social Security number, treatment information, and financial account data.

227. Upon information and belief, Plaintiff Jackson's Private Information was compromised in the Data Breach and stolen by unauthorized individuals who unlawfully accessed Defendants network to obtain the sensitive Private Information.

228. After the breach, Plaintiff Jackson has noticed a dramatic increase in suspicious spam calls, emails, and texts. Plaintiff Jackson has also experienced multiple fraudulent charges to her bank account totaling more than $2,000.

229. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Jackson will need to maintain heightened measures for years, and possibly for life.

230. As a result of the Data Breach, Plaintiff Jackson has suffered loss of time, interference, and inconvenience, as well as anxiety and emotional distress related to the increased risk of identity theft and loss of privacy.

231. Plaintiff Jackson has suffered imminent and impending injury from the substantially heightened risk of identity theft, fraud, and misuse resulting from the exposure of her Private Information in the Data Breach.

232. Plaintiff Jackson has suffered actual injury from having her Private Information compromised as a result of the Data Breach, including but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ADG did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her Private Information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has likely been stolen and published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that ADG obtained from Plaintiff Jackson and/or her medical providers; and (g) other economic and non-economic harm.

233. Plaintiff Jackson has taken reasonable steps to mitigate the impact of the Data Breach, including researching the data breach, reviewing credit reports, monitoring accounts, and taking steps to prevent further harm. Plaintiff Jackson spent several hours dealing with the Data Breach, valuable time she would have spent on other activities, including, but not limited to, work and recreation. This is time spent that has been lost forever and cannot be recaptured.

234. Plaintiff Jackson has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendants, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff Jackson's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Amanda Maduike-Iwata

235. Plaintiff Amanda Maduike-Iwata is a current patient of ADG and provided her Private Information to ADG as a condition of receiving dental services.

236. Plaintiff Maduike-Iwata values the privacy and security of her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

237. Plaintiff Maduike-Iwata reasonably believed that her Private Information would be protected, and that ADG, and any third-party vendor ADG contracts with, including JCI, would implement and maintain reasonable data security measures to safeguard it from unauthorized access, use, or disclosure.

238. Had Plaintiff Maduike-Iwata known that Defendants do not adequately protect Private Information, Plaintiff Maduike-Iwata would not have used ADG's services nor agreed to provide Defendants with Private Information.

239. At the time of the Data Breach, Defendants retained Plaintiff Maduike-Iwata's Private information in its systems, including but not limited to: Plaintiff Maduike-Iwata's full name, date of birth, health information, dental information and records, health and/or dental insurance information, medical billing or claims information, prescription or medication information, Social Security number, treatment information, and financial account data.

240. Upon information and belief, Plaintiff Maduike-Iwata's Private Information was compromised in the Data Breach and stolen by unauthorized individuals who unlawfully accessed Defendants network to obtain the sensitive Private Information.

241. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Maduike-Iwata will need to maintain heightened measures for years, and possibly for life.

242. As a result of the Data Breach, Plaintiff Maduike-Iwata has suffered loss of time, interference, and inconvenience, as well as anxiety and emotional distress related to the increased risk of identity theft and loss of privacy.

243. Plaintiff Maduike-Iwata has suffered imminent and impending injury from the substantially heightened risk of identity theft, fraud, and misuse resulting from the exposure of her Private Information in the Data Breach.

244. Plaintiff Maduike-Iwata has suffered actual injury from having her Private Information compromised as a result of the Data Breach, including but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss

of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ADG did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her Private Information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has likely been stolen and published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that ADG obtained from Plaintiff Maduike-Iwata and/or her medical providers; and (g) other economic and non-economic harm.

245. Plaintiff Maduike-Iwata has taken reasonable steps to mitigate the impact of the Data Breach, including researching the data breach, reviewing credit reports, monitoring accounts, and taking steps to prevent further harm. Plaintiff Maduike-Iwata spent about 12 hours dealing with the Data Breach, valuable time she would have spent on other activities, including, but not limited to, work and recreation. This is time spent that has been lost forever and cannot be recaptured.

246. Plaintiff Maduike-Iwata has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendants, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff Maduike-Iwata's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Viridiana Tinajero Monterroza

247. Plaintiff Viridiana Tinajero Monterroza is a patient of ADG and provided her Private Information to ADG as a condition of receiving dental services.

248. Plaintiff Tinajero values the privacy and security of her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

249. Plaintiff Tinajero reasonably believed that her Private Information would be protected, and that ADG, and any third-party vendor ADG contracts with, including JCI, would implement and maintain reasonable data security measures to safeguard it from unauthorized access, use, or disclosure.

250. Had Plaintiff Tinajero known that Defendants do not adequately protect Private Information, Plaintiff Tinajero would not have used ADG's services nor agreed to provide Defendants with Private Information.

251. At the time of the Data Breach, Defendants retained Plaintiff Tinajero's Private information in its systems, including but not limited to: Plaintiff Tinajero's full name, date of birth, health information, dental information and records, health and/or dental insurance information, medical billing or claims information, prescription or medication information, Social Security number, treatment information, and financial account data.

252. Upon information and belief, Plaintiff Tinajero's Private Information was compromised in the Data Breach and stolen by unauthorized individuals who unlawfully accessed Defendants network to obtain the sensitive Private Information.

253. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Tinajero will need to maintain heightened measures for years, and possibly for life.

254. As a result of the Data Breach, Plaintiff Tinajero has suffered loss of time, interference, and inconvenience related to the increased risk of identity theft and loss of privacy.

255. Plaintiff Tinajero has suffered imminent and impending injury from the substantially heightened risk of identity theft, fraud, and misuse resulting from the exposure of her Private Information in the Data Breach.

256. Plaintiff Tinajero has suffered actual injury from having her Private Information compromised as a result of the Data Breach, including but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ADG did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her Private Information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has likely been stolen and published on the dark web; (f) diminution in the value of

her Private Information, a form of intangible property that ADG obtained from Plaintiff Tinajero and/or her medical providers; and (g) other economic and non-economic harm.

257. Plaintiff Tinajero has taken reasonable steps to mitigate the impact of the Data Breach, including researching the data breach, reviewing credit reports, monitoring accounts, and taking steps to prevent further harm. Plaintiff Tinajero hours dealing with the Data Breach, valuable time she would have spent on other activities, including, but not limited to, work and recreation. This is time spent that has been lost forever and cannot be recaptured.

258. Plaintiff Tinajero has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendants, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff Tinajero's Private Information will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

259. Plaintiffs bring this action individually, and on behalf of all members of the following Classes (together, the "Class" or "Classes") of similarly situated persons:

> **Nationwide Class**
> All persons residing in the United States whose Private Information was compromised in the Data Breach disclosed by Absolute Dental Group, LLC.
>
> **Nevada Class**
> All persons residing in the state of Nevada whose Private Information was compromised in the Data Breach disclosed by Absolute Dental Group, LLC.

260. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

261. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes, before the Court determines whether certification is appropriate.

262. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

263. Numerosity. The Class members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class members are unknown at this time, based on information and belief, the Class consists of tens or hundreds of thousands of patients of ADG who are geographically dispersed, including in states beyond Nevada, whose data was compromised in the Data Breach. The identities of Class members are ascertainable through Defendants records, Class members' records, publication notice, self-identification, and other means.

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

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants conduct violated the FTCA and HIPAA;

c. When Defendants learned of the Data Breach

d. Whether Defendants response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class members' Private Information;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Defendants data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendants data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed a duty to Class members to safeguard their Private Information;

j. Whether Defendants breached its duty to Class members to safeguard their Private Information;

k. Whether hackers obtained Class members' Private Information via the Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class members;

m. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

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

o. What damages Plaintiffs and Class members suffered as a result of Defendants misconduct;

p. Whether Defendants conduct were negligent;

q. Whether Defendants conduct was per se negligent;

r. Whether Defendants conduct constitutes a breach of contract;

s. Whether Defendants conduct constitutes a breach of implied contract;

t. Whether Defendants was unjustly enriched;

u. Whether Defendants conduct constitutes a breach of fiduciary duty;

v. Whether Defendants conduct constitutes a breach of confidence;

w. Whether Plaintiffs' privacy was invaded upon;

x. Whether Defendants conduct violates the Nevada Privacy of Information Collected on the Internet From Consumers Act, Nev. Rev. Stat. § 603A;

y. Whether Plaintiffs and Class members are entitled to actual and/or statutory damages;

z. Whether Plaintiffs and Class members are entitled to credit or identity monitoring and monetary relief; and

aa. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

265. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of all other class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

266. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class members because, *inter alia*, all Class members were injured through the common misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of Plaintiffs and all other Class members, and there are no defenses that are unique to each Plaintiff. The claims of Plaintiffs and those of Class members arise from the same operative facts and are based on the same legal theories.

267. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class members. Plaintiffs' counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

268. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class members in that all of Plaintiffs' and Class members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants 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.

269. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. 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 Defendants. In contrast, conducting 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.

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

271. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class members affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by ADG.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

272. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

273. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class members' Private Information.

274. Upon accepting and storing Plaintiffs' and Class members' Private Information on their computer systems and networks, Defendants undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs and Class member's Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

275. Defendants owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that their computer systems and networks, those belonging to their third-party vendors, and the personnel responsible for them, adequately protected the Private Information.

276. Defendants' duty also included the responsibility to implement processes by which they could detect and analyze a breach of their security systems in a reasonably expeditious period of time, and give prompt notice to those affected in the event of a cyberattack.

277. Defendants knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class members and the importance of adequate security. Defendants were on notice because, on information and belief, they knew or should have known that they would be an attractive target for cyberattacks.

278. Defendants owed a duty of care to Plaintiffs and Class members whose Private Information was entrusted to them. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;

b. to exercise reasonable care in designing, implementing, maintaining, monitoring, and testing its networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

c. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

d. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

e. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class members pursuant to HIPAA and the FTCA;

f. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

g. To promptly notify Plaintiffs and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

279. Defendants' duty to employ reasonable data security measures arose, in part, 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.

280. Defendants' duty also arose because Defendants are bound by industry standards to protect individuals' confidential Private Information.

281. Plaintiffs and Class members were foreseeable victims of any inadequate security practices on the part of Defendants, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

282. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class members' Private Information within their possession.

283. Defendants, by their actions and/or omissions, breached their duties of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class members.

284. Defendants, by their actions and/or omissions, breached their duties of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

285. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system maintained reasonable data security safeguards;

d. Failing to implement and maintain adequate mitigation policies and procedures;

e. Allowing unauthorized access to Class members' Private Information;

f. Failing to comply with the FTCA; and

g. Failing to comply with the NPICICA;

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

286. Defendants acted with reckless disregard for the rights of Plaintiffs and Class members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

287. Defendants had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the Private Information that it stored on them) from attack.

288. Defendants breach of duties owed to Plaintiffs and Class members caused Plaintiffs' and Class members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

289. As a result of Defendants' ongoing failure to notify Plaintiffs and Class members regarding exactly what Private Information has been compromised, Plaintiffs and Class members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

290. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

291. As a result of Defendants' negligence in breach of their duties owed to Plaintiffs and Class members, Plaintiffs and Class members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

292. Defendants also had independent duties under state laws that required them to reasonably safeguard Plaintiffs' and Class members' Private Information and promptly notify them about the Data Breach.

293. As a direct and proximate result of Defendants conduct, including, but not limited to, Defendants failure to implement and maintain reasonable data security practices and procedures, Plaintiffs and Class members have suffered or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost time and opportunity costs associated with efforts expended to address and 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 fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

294. The injury and harm that Plaintiffs and Class members suffered was reasonably foreseeable.

295. Plaintiffs and Class members have suffered cognizable injuries and are entitled to actual and punitive damages in an amount to be proven at trial.

296. In addition to monetary relief, Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and

monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

297. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

298. Pursuant to Section 5 of the FTCA, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class members.

299. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class members' Private Information.

300. Defendants also had a duty to use reasonable security measures under HIPAA, which requires covered entities and business associates, like Defendants, 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 action constitutes "protected health information" within the meaning of HIPAA.

301. Title II of HIPAA contains what is 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 Private Information. HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 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).

302. Specifically, pursuant to HIPAA, Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of

assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

303. Pursuant to Nev. Rev. Stat. § 603A.210, data collectors, such as Defendants, have a duty to implement reasonable security measures in order to protect Private Information "from unauthorized access, acquisition, destruction, use, modification, or disclosure."

304. Pursuant to Nev. Rev. Stat. § 603A.220, data collectors, such as Defendants, have a duty to "notify Nevada residents of any data breach "in the most expedient time possible and without unreasonable delay."

305. Plaintiffs and Class members are within the class of persons that the FTCA, HIPAA, and NPICICA intended to protect, and Defendants failure to comply with both constitutes negligence *per se*.

306. Defendants breached their duties to Plaintiffs and Class members under the FTCA, HIPAA, NPICICA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information, and by failing to provide prompt notice of the Data Breach without unreasonable delay.

307. Specifically, Defendants breached their duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

308. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendants' duties in this regard.

309. Defendants also violated the FTCA, HIPAA, and NPICICA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

310. Defendants' violations of the FTCA, HIPAA, and NPICICA each constitute as negligence *per se*.

311. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiffs' and Class members' unencrypted Private Information.

312. Plaintiffs' and Class members' Private Information constitutes personal property that was stolen due to Defendants negligence, resulting in harm, injury, and damages to Plaintiffs and Class members.

313. As a direct and proximate result of Defendants negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the actual misuse of their Private Information and the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

314. As a direct and proximate result of Defendants negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

315. In addition to monetary relief, Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class Against ADG)

316. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

317. Plaintiffs and Class members entered into a valid and enforceable contract through which they paid money to ADG in exchange for services. That contract included promises by

Defendant to secure, safeguard, and not disclose Plaintiffs' and Class members' Private Information.

318. ADG's Privacy Policy memorialized the rights and obligations of ADG and its patients. This document was provided to Plaintiffs and Class members in a manner in which it became part of the agreement for services.

319. In the Privacy Policy, ADG commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class members' Private Information except under certain limited circumstances.

320. Plaintiffs and Class members fully performed their obligations under their contracts with ADG.

321. However, ADG did not secure, safeguard, and/or keep private Plaintiffs' and Class members' Private Information, and therefore ADG breached its contracts with Plaintiffs and Class members.

322. ADG allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class members' Private Information without permission. Therefore, ADG breached the Privacy Policy with Plaintiffs and Class members.

323. ADG's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in ADG providing services to Plaintiffs and Class members that were of a diminished value.

324. As a result, Plaintiffs and Class members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class members.

325. As a direct and proximate result of ADG's conduct, Plaintiffs and Class members suffered and will continue to suffer damages in an amount to be proven at trial.

326. In addition to monetary relief, Plaintiffs and Class members are also entitled to injunctive relief requiring ADG to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class Against ADG)

327. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

328. This Count is pleaded in the alternative to Count III above.

329. ADG provides dental and related services to Plaintiffs and Class members. Plaintiffs and Class members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class members paying for services and/or entrusting their valuable Private Information to Defendant in exchange for such services.

330. Through Defendant's sale of services to Plaintiffs and Class members, it knew or should have known that it must protect Plaintiffs' and Class members' confidential Private Information in accordance with its policies, practices, and applicable law.

331. As consideration, Plaintiffs and Class members paid money to ADG and/or turned over valuable Private Information to ADG. Accordingly, Plaintiffs and Class members bargained with ADG to securely maintain and store their Private Information.

332. ADG accepted payment and/or possession of Plaintiffs' and Class members' Private Information for the purpose of providing services to Plaintiffs and Class members.

333. In paying Defendant and/or providing their valuable Private Information to Defendant in exchange for Defendant's services, Plaintiffs and Class members intended and understood that ADG would adequately safeguard the Private Information as part of those services.

334. Defendant's implied promises to Plaintiffs and Class members include, but are not limited to: (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and

implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

335. Plaintiffs and Class members would not have entrusted their Private Information to ADG in the absence of such an implied contract.

336. Had ADG disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class members would not have provided their Private Information to ADG.

337. As a provider of dental health services, ADG recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class members.

338. ADG violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class members' Private Information. ADG further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

339. Additionally, ADG breached the implied contracts with Plaintiffs and Class members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

340. ADG also breached the implied contracts with Plaintiffs and Class members by failing to implement technical policies and procedures for electronic 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 CFR 164.312(a)(1).

341. ADG further breached the implied contracts with Plaintiffs and Class members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

342. ADG further breached the implied contracts with Plaintiffs and Class members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

343. ADG further breached the implied contracts with Plaintiffs and Class members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

344. ADG further breached the implied contracts with Plaintiffs and Class members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

345. ADG further breached the implied contracts with Plaintiffs and Class members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

346. ADG further breached the implied contracts with Plaintiffs and Class members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

347. ADG further breached the implied contracts with Plaintiffs and Class members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

348. ADG further breached the implied contracts with Plaintiffs and Class members by otherwise failing to safeguard Plaintiffs' and Class members' PHI.

349. A meeting of the minds occurred, as Plaintiffs and Class members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to ADG in exchange for ADG's agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

350. Plaintiffs and Class members have been damaged by ADG's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

351. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

352. This Count is pleaded in the alternative to Counts III and IV above.

353. Plaintiffs and Class members directly and indirectly conferred a monetary benefit on Defendants. They indirectly conferred a monetary benefit on Defendants by purchasing goods and/or services from entities that contracted with Defendants, and from which Defendant received compensation to protect certain data. Plaintiffs and Class members directly conferred a monetary benefit on Defendants by supplying their Private Information, from which Defendants derive their business, and which should have been protected with adequate data security.

354. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including from payments made to them by Plaintiffs, Class members, and Clients.

355. As such, a portion of the payments made by Plaintiffs and Class members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

356. Defendants have retained the benefits of their unlawful conduct, including the amounts of payment received from Plaintiffs and Class members that should have been used for adequate cybersecurity practices that they failed to provide.

357. Defendants knew that Plaintiffs and Class members conferred a benefit upon them, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class members for business purposes, while failing to use the payments they received for adequate data security measures that would have secured Plaintiffs' and Class members' Private Information and prevented the Data Breach.

358. If Plaintiffs and Class members had known that Defendants had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendants.

359. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

360. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Private Information.

361. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendants decision to prioritize its own profits over the requisite data security.

362. As a direct and proximate result of Defendants conduct, Plaintiffs and Class members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) 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; (vi) the continued risk to their Private Information, which remains in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in THEIR continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

363. Plaintiffs and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by ADG from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class members may seek restitution or compensation.

364. Plaintiffs and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class Against ADG)

365. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

366. In light of the special relationship between ADG and its patients, whereby ADG became a guardian of Plaintiffs' and Class members' Private Information (including highly sensitive, confidential, personal, and other PHI) ADG was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class members. This benefit included (1) the safeguarding of Plaintiffs' and Class members' Private Information; (2) timely notifying Plaintiffs and Class members of the Data Breach; and (3) maintaining complete and accurate records of what and where ADG's patients' Private Information was and is stored.

367. ADG had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its patients' relationship, in particular to keep the Private Information secure.

368. These fiduciary duties and responsibilities are also described under the procedures set forth in the HIPAA Privacy Rule, including the procedures and definitions found in 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which requires Defendant to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient and employee information and to secure the healthcare information it maintains and to keep it free from disclosure.

369. ADG breached its fiduciary duties to Plaintiffs and Class members by failing to diligently investigate the Data Breach to determine the number of Class members affected and notify them within a reasonable and practicable period of time.

370. ADG breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

371. ADG breached its fiduciary duties to Plaintiffs and Class members by failing to ensure the confidentiality and integrity of electronic PHI ADG created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

372. ADG breached its fiduciary duties to Plaintiffs 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 CFR 164.312(a)(1).

373. ADG breached its fiduciary duties to Plaintiffs and Class members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

374. ADG breached its fiduciary duties to Plaintiffs and Class members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

375. ADG breached its fiduciary duties to Plaintiffs 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 CFR 164.306(a)(2).

376. ADG breached its fiduciary duties to Plaintiffs 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 CFR 164.306(a)(3).

377. ADG breached its fiduciary duties to Plaintiffs and Class members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

378. ADG breached its fiduciary duties to Plaintiffs and Class members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

379. As a direct and proximate result of ADG's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VII
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class Against ADG)

380. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

381. Plaintiffs and Class members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by ADG and ultimately accessed and acquired in the Data Breach.

382. As a healthcare provider, ADG has a special, fiduciary relationship with its patients, including Plaintiffs and Class members. Because of that special relationship, ADG was provided with and stored Plaintiffs' and Class members' Private Information and had a duty to maintain the Private Information in confidence.

383. Patients like Plaintiffs and Class members have a privacy interest in personal medical and other matters, and ADG had a duty not to disclose such matters concerning its patients.

384. As a result of the parties' relationship, ADG had possession and knowledge of highly sensitive and confidential Private Information belonging to Plaintiffs and Class members, information that was not generally known.

385. Plaintiffs and Class members did not consent nor authorize ADG to release or disclose their Private Information to an unknown criminal actor.

386. ADG breached its duty of confidence owed to Plaintiffs and Class members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiffs' and Class members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' Private Information to a criminal third party.

387. But for ADG's wrongful breach of its duty of confidence owed to Plaintiffs and Class members, their Private Information would not have been compromised.

388. As a direct and proximate result of ADG's wrongful breach of its duty of confidence, Plaintiffs and Class members have suffered and will continue to suffer the injuries alleged herein.

389. It would be inequitable for ADG to retain the benefit of controlling and maintaining Plaintiffs' and Class members' Private Information at the expense of Plaintiffs and Class members.

390. Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VIII
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

391. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

392. Plaintiffs and Class members took reasonable and appropriate steps to keep their Private Information confidential from the public.

393. Plaintiffs' and Class members' efforts to safeguard their own Private Information were successful, as their Private Information was not known to the public prior to the Data Breach.

394. Plaintiffs and Class members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

395. Defendants owed a duty to individuals', including Plaintiffs and the proposed Class members, to keep their Private Information confidential.

396. The unauthorized release of Private Information is highly offensive to any reasonable person.

397. Plaintiffs' and Class members' Private Information is not of legitimate concern to the public.

398. Defendants knew or should have known that Plaintiffs' and Class members' Private Information was private.

399. Defendants publicized Plaintiffs' and Class members' Private Information, by communicating them to cybercriminals who had no legitimate interest in this Private Information and who had the express purpose of monetizing that information by injecting it into the illicit stream of commerce flowing through the dark web and other malicious channels of communication (e.g., Telegram and Signal).

400. It is therefore substantially certain that the Plaintiffs' and the Class members' Private Information is rapidly becoming public knowledge–among the community writ large–due to the nature of the malware attack that procured it, and the identity theft that it is designed for.

401. Moreover, because of the ubiquitous nature of data breaches, Defendants were substantially certain that a failure to protect Private Information would lead to its disclosure to unauthorized third parties, including the thousands of waiting identity thieves who are in a special relationship to Plaintiffs and the proposed Class members—in that those identity thieves are precisely the individuals whose aim it is to misuse such Private Information.

402. Therefore, by failing to keep Plaintiff's and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendants invaded Plaintiff's and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiffs and Class members, which is highly offensive to a reasonable person.

403. Unless and until enjoined, and restrained by order of this Court, Defendants wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that Defendants inadequate data security measures will likely result in additional data breaches. Plaintiffs and Class members have no adequate remedy at law for the injuries that they will sustain in that a judgment for monetary damages will not prevent further invasions of the Plaintiffs' and Class members' privacy by Defendants.

COUNT IX
VIOLATION OF THE NEVADA PRIVACY OF INFORMATION COLLECTED ON THE INTERNET FROM CONSUMERS ACT
NEV. REV. STAT. § 603A
(On Behalf of Plaintiffs and the Nevada Class Against Defendants)

404. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

405. This count is brought on behalf of all members of the Nevada Class.

406. The NPICICA, Nev. Rev. Stat. § 603A, obligates "data collectors" that maintain records containing personal information of Nevada residents to "implement and maintain

reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." Nev. Rev. Stat. § 603A.210.

407. Additionally, the NPICICA creates a duty for data collectors to notify Nevada residents of any data breach "in the most expedient time possible and without unreasonable delay." Nev. Rev. Stat. § 603A.220.

408. Defendants are "data collectors" as defined by NPICICA.

409. Defendants failed to implement and maintain reasonable security measures to safeguard, protect and keep confidential Plaintiffs' and Nevada Class members' Private Information from unauthorized access or disclosure, as alleged herein. Defendants, knowing and/or reasonably believing that Plaintiffs' and Nevada Class members' Private Information was acquired or accessed by unauthorized persons during the Data Breach, failed to provide prompt, immediate, and reasonable notice of the Data Breach to Plaintiffs and the Nevada Subclass as required by NPICICA.

410. Defendants' failure to implement and maintain reasonable security measures to protect Plaintiffs' and Nevada Class members' Private Information, and/or Defendants failure to provide timely and accurate notice of the Data Breach violated the NPICICA.

411. As a result of Defendants failure to reasonably safeguard the Private Information belonging to Plaintiffs and the Nevada Class, and Defendants failure to provide reasonable and timely notice of the Data Breach to Plaintiffs and the Nevada Class, Plaintiffs and the Nevada Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their Private Information in Defendants possession, and are entitled to damages in an amount to be proven at trial.

COUNT X
DECLARATORY AND INJUNCTIVE RELIEF, 28 U.S.C. § 2201
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

412. Plaintiffs restate and incorporate by reference all preceding paragraphs as if fully set forth herein.

413. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

414. As previously alleged, Defendants were required to provide adequate security for the protection of the Private Information Defendants collected.

415. Defendants owe duties of care to Plaintiffs and Class members that required them to adequately secure their Private Information.

416. Defendants still possess Plaintiffs' and Class members' Private Information, yet do not adequately protect their Private Information against the threat of another data breach.

417. Defendants have not satisfied their contractual obligations and legal duties to Plaintiffs and Class members.

418. Actual harm has arisen in the wake of the Data Breach regarding Defendants' obligations and duties of care to provide security measures to Plaintiffs and Class members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendants' ongoing failure to address the security failings that led to such exposure.

419. Since the Data Breach, Defendants have not announced any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

420. There is no reason to believe that Defendants employee training and security measures are any more adequate now than they were before the Data Breach.

421. Plaintiffs, therefore, seek a declaration (1) that Defendants existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, being ordered as follows:

a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

b. ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

c. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

d. ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

e. ordering that Defendants audit, test, and train security personnel and employees regarding any new or modified data security policies and procedures;

f. ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for provision of services;

g. ordering that Defendants conduct regular database scanning and security checks;

h. prohibiting Defendants from maintaining Private Information of Plaintiffs and Class members on a cloud-based database;

i. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants network is compromised, hackers cannot gain access to other portions of Defendants systems;

j. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive Private Information;

k. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding paragraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

l. requiring Defendants to meaningfully educate all class members about the threats they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

m. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

n. such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class described above, seeks the following relief:

a. Certifying the class as requested herein, designating Plaintiffs as Class representative, and appointing Plaintiffs' counsel as Class Counsel;

b. Judgment in favor of Plaintiffs and Class members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members;

e. An order requiring Defendants to pay the costs involved in notifying Class members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Dated: November 7, 2025

Respectfully submitted,

/s/ Andrew W. Ferich

Andrew W. Ferich (*pro hac vice*)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Alyssa Brown (*pro hac vice*)
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
abrown@ahdootwolfson.com

Andrew E. Mize (*pro hac vice*)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
amize@stranchlaw.com

Nathan R. Ring
Nevada Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Blvd., Suite 208
Las Vegas, Nevada 89102
(725) 235-9750
nring@stranchlaw.com

William B. Federman
(*pro hac vice* admission pending)
Kennedy M. Brian
(*pro hac vice* admission pending)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
T: (405) 235-1560
E: wbf@federmanlaw.com
E: kpb@federmanlaw.com

Mariya Weekes (pro hac vice)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (786) 879-8200 / Fax: (786) 879-7520
mweekes@milberg.com

Nickolas J. Hagman (pro hac vice)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
nhagman@caffertyclobes.com

Interim Co-Lead Class Counsel

George Haines
Nevada Bar No. 9411
Gerardo Avalos
Nevada Bar No. 15171
FREEDOM LAW FIRM
8985 S. Eastern Avenue Suite 100
Las Vegas, NV 89123
Telephone: 702-880-5554
Facsimile: 702-385-5518
Email: info@freedomlegalteam.com

Patrick R. Leverty
Nevada Bar No. 8840
LEVERTY AND ASSOCIATES LAW, CHTD.
832 Willow Street
Reno, NV 89503
(775)-322-6636
pat@levertylaw.com

Additional Class Counsel for Plaintiffs and the Proposed Class