THE STATE OF NEW HAMPSHIRE

ROCKINGHAM COUNTY SUPERIOR COURT

SEAN SKILLINGS, MAUREEN MARCH, CHRISTINE WILLIS, JAMES GIGUERE, CAMERON LAFONTAINE, E.B., a minor, by and through her guardian, SARAH BARR, and E.B., a minor, by and through her guardian, AMBER BASSETT, individually, and on behalf of all others similarly situated;

v.

ACCESS SPORTS MEDICINE AND ORTHOPAEDICS, PLLC,

Docket No. 218-2024-CV-01086

[MOTION FOR CONSOLIDATION GRANTED ON 10/30/24].

CONSOLIDATED CLASS ACTION COMPLAINT

1. Representative Plaintiffs Sean Skillings, Maureen March, Christine Willis, James Giguere, Cameron Lafontaine, E.B., a minor, by and through her guardian, Sarah Barr and E.B., a minor, by and through her guardian, Amber Bassett, (collectively, "Representative Plaintiffs") bring this class action against Defendant Access Sports Medicine and Orthopaedics, PLLC ("Defendant") for its failure to properly secure and safeguard Representative Plaintiffs' and/or Class Members' protected health information and personally identifiable information stored within Defendant's information network, including, without limitation, Social Security numbers, dates of birth, financial information, medical information and health insurance information (these types of information, *inter alia*, being thereafter referred to, collectively, as "protected health information"

or "PHI"[1] and "personally identifiable information" or "PII").[2] All such information is referred to in the aggregate herein as "Private Information."

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harm it caused and will continue to cause Representative Plaintiffs and thousands of other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on May 10, 2024, by which cybercriminals infiltrated Defendant's inadequately protected network and accessed the Private Information which was being kept under-protected (the "Data Breach").

3. Representative Plaintiffs further seek to hold Defendant responsible for not ensuring that the Private Information was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards.

4. While Defendant claims to have discovered the breach as early as May 10, 2024, Defendant did not begin informing victims of the Data Breach until September 11, 2024 and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative

---

[1] Protected health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it. The Notice received by Representative Plaintiffs was dated September 11, 2024.

5. Defendant acquired, collected and stored Representative Plaintiffs' and Class Members' Private Information. Therefore, at all relevant times, Defendant knew or should have known that Representative Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential Private Information.

6. HIPAA establishes national minimum standards for the protection of individuals' medical records and other protected health information. HIPAA generally applies to health plans and insurers, healthcare clearinghouses and those healthcare providers that conduct certain healthcare transactions electronically and sets minimum standards for Defendant's maintenance of Representative Plaintiffs' and Class Members' Private Information. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiffs' and Class Members' Private Information, including rights to examine and obtain copies of their health records and to request corrections thereto.

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is created, received, used or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

8. By obtaining, collecting, using and deriving a benefit from Representative Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles. Representative Plaintiffs do not bring claims in this action for direct violations of HIPAA, but charge Defendant with various legal violations merely predicated upon the duties set forth in HIPAA.

9. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiffs' and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to New Hampshire Revised Statutes ("RSA") Sections 491:7 and 491:22.

11. Venue is proper in Rockingham County as Defendant is headquartered and routinely conducts business in the State where this County is located, has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction by marketing and

selling products and services, and by accepting and processing payments for those products and services within this State. A substantial part of the events that gave rise to Representative Plaintiffs' claims took place within this County, and Defendant does business in this Judicial District.

PLAINTIFFS

Plaintiff Sean Skillings

12. Plaintiff Sean Skillings is an adult individual and, at all relevant times herein, was a resident and citizen of the State of New Hampshire. Plaintiff Skillings is a victim of the Data Breach.

13. Defendant received highly sensitive Private Information from Plaintiff Skillings in connection with the services Plaintiff obtained. As a result, Plaintiff Skillings' information was among the data accessed by an unauthorized third party in the Data Breach.

14. At all times herein relevant, Plaintiff Skillings is and was a member of the Class.

15. Plaintiff Skillings' Private Information was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's Private Information. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

16. Plaintiff Skillings received a letter from Defendant stating Plaintiff's Private Information was involved in the Data Breach (the "Notice").

17. As a result, Plaintiff Skillings spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff Skillings' options for

remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

18. Plaintiff Skillings suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

19. Plaintiff Skillings suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's Private Information.

20. Plaintiff Skillings suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

21. Plaintiff Skillings has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Maureen March

22. Plaintiff Maureen March is an adult individual and, at all relevant times herein, was a resident and citizen of the State of New Hampshire. Plaintiff March is a victim of the Data Breach.

23. Defendant received highly sensitive Private Information from Plaintiff March in connection with the services Plaintiff obtained. As a result, Plaintiff March's information was among the data accessed by an unauthorized third party in the Data Breach.

24. At all times herein relevant, Plaintiff March is and was a member of the Class.

25. Plaintiff March's Private Information was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's Private Information. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

26. Plaintiff March received a letter from Defendant stating Plaintiff's Private Information was involved in the Data Breach (the "Notice").

27. As a result, Plaintiff March spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff March's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

28. Plaintiff March suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

29. Plaintiff March suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's Private Information.

30. Plaintiff March suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

31. Plaintiff March has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Christine Willis

32. Plaintiff Christine Willis is an adult individual and, at all relevant times herein, was a resident and citizen of the State of New Hampshire. Plaintiff Willis is a victim of the Data Breach.

33. Defendant received highly sensitive Private Information from Plaintiff Willis in connection with the services Plaintiff obtained. As a result, Plaintiff Willis' information was among the data accessed by an unauthorized third party in the Data Breach.

34. At all times herein relevant, Plaintiff Willis is and was a member of the Class.

35. Plaintiff Willis' Private Information was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's Private Information. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

36. Plaintiff Willis received a letter from Defendant stating Plaintiff's Private Information was involved in the Data Breach (the "Notice").

37. As a result, Plaintiff Willis spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiffs' accounts and seeking legal counsel regarding Plaintiff Willis' options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

38. Plaintiff Willis suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

39. Plaintiff Willis suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's Private Information.

40. Plaintiff Willis suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

41. Plaintiff Willis has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff James Giguere

42. Plaintiff James Giguere is an adult individual and, at all relevant times herein, was a resident and citizen of the State of New Hampshire. Plaintiff Giguere is a victim of the Data Breach.

43. Defendant received highly sensitive Private Information from Plaintiff Giguere in connection with the services Plaintiff obtained. As a result, Plaintiff Giguere's information was among the data accessed by an unauthorized third party in the Data Breach.

44. At all times herein relevant, Plaintiff Giguere is and was a member of the Class.

45. Plaintiff Giguere's Private Information was exposed in the Data Breach because Defendant stored and/or shared Plaintiffs' Private Information. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

46. Plaintiff Giguere received a letter from Defendant stating Plaintiff's Private Information was involved in the Data Breach (the "Notice").

47. As a result, Plaintiff Giguere spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff Giguere's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

48. Plaintiff Giguere suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

49. Plaintiff Giguere suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's Private Information.

50. Plaintiff Giguere suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

51. Plaintiff Giguere has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Cameron Lafontaine

52. Plaintiff Cameron Lafontaine is an adult individual and, at all relevant times herein, was a resident and citizen of the State of New Hampshire. Plaintiff Lafontaine is a victim of the Data Breach.

53. Defendant received highly sensitive Private Information from Plaintiff Lafontaine in connection with the services Plaintiff obtained. As a result, Plaintiff Lafontaine's information was among the data accessed by an unauthorized third party in the Data Breach.

54. At all times herein relevant, Plaintiff Lafontaine is and was a member of the Class.

55. Plaintiff Lafontaine's Private Information was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's Private Information. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

56. Plaintiff Lafontaine received a letter from Defendant stating Plaintiff's Private Information was involved in the Data Breach (the "Notice").

57. As a result, Plaintiff Lafontaine spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiffs' accounts and seeking legal counsel regarding Plaintiff Lafontaine's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

58. Plaintiff Lafontaine suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

59. Plaintiff Lafontaine suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's Private Information.

60. Plaintiff Lafontaine suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

61. Plaintiff Lafontaine has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff E.B., by and through her guardian, Sarah Barr,

62. Representative Plaintiff E.B., by and through her guardian, Sarah Barr, is a minor child and, at all relevant times herein, was a resident and citizen of the State of New Hampshire. Plaintiff E.B., by and through her guardian, Sarah Barr, is a victim of the Data Breach.

63. Defendant received highly sensitive Private Information from Plaintiff E.B., by and through her guardian, Sarah Barr in connection with the services Plaintiff obtained. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

64. At all times herein relevant, Plaintiff E.B., by and through her guardian, Sarah Barr is and was a member of the Class.

65. Plaintiff E.B., by and through her guardian, Sarah Barr's Private Information was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's Private Information. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

66. Plaintiff E.B., by and through her guardian, Sarah Barr, received a letter from Defendant stating Plaintiff's Private Information was involved in the Data Breach (the "Notice").

67. As a result, Plaintiff E.B., by and through her guardian, Sarah Barr, spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

68. Plaintiff E.B., by and through her guardian, Sarah Barr, suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Representative Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

69. Plaintiff E.B., by and through her guardian, Sarah Barr, suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's Private Information.

70. Plaintiff E.B., by and through her guardian, Sarah Barr, suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse

resulting from Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

71. Plaintiff E.B., by and through her guardian, Sarah Barr, has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff E.B., by and through her guardian, Amber Bassett

72. Representative Plaintiff E.B., by and through her guardian, Amber Bassett, is a minor child and, at all relevant times herein, was a resident and citizen of the State of New Hampshire. Plaintiff E.B., by and through her guardian, Amber Bassett, is a victim of the Data Breach.

73. Defendant received highly sensitive Private Information from Plaintiff E.B., by and through her guardian, Amber Bassett in connection with the services Plaintiff obtained. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

74. At all times herein relevant, Plaintiff E.B., by and through her guardian, Sarah Barr is and was a member of the Class.

75. Plaintiff E.B., by and through her guardian, Amber Bassett's Private Information was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's Private Information. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

76. Plaintiff E.B., by and through her guardian, Amber Bassett received a letter from Defendant stating Plaintiff's Private Information was involved in the Data Breach (the "Notice").

77. As a result, Plaintiff E.B., by and through her guardian, Amber Bassett spent time dealing with the consequences of the Data Breach, which included, and continues to include, time

spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

78. Plaintiff E.B., by and through her guardian, Amber Bassett suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Representative Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

79. Plaintiff E.B., by and through her guardian, Amber Bassett suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's Private Information.

80. Plaintiff E.B., by and through her guardian, Amber Bassett suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

81. Plaintiff E.B., by and through her guardian, Amber Bassett has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

82. Defendant is a for-profit corporation with a principal place of business located in Exeter, New Hampshire. Defendant specializes in the prevention and treatment of disorders, injuries and illness to the muscles, bones and joints.[3]

83. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

84. Representative Plaintiffs bring this action pursuant to the provisions of NH RSA 358-A:10 on behalf of Representative Plaintiff and the following class (collectively, the "Class"):

> **Plaintiff Class:**
> "All individuals within the United States whose Private Information was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on or before May 10, 2024."

85. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including, but not limited to, its departments, agencies, divisions, bureaus, boards, sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

[3] https://www.accesssportsmed.com/about-access/ (last assessed November 27, 2024).

86. In the alternative, Representative Plaintiffs may request additional subclasses as necessary based, e.g., on the types of Private Information that were compromised.

87. Representative Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and its motion for class certification.

88. This action has been brought and may properly be maintained as a class action under NH RSA 358-A:10 because there is a well-defined community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Membership in the Class will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs and Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Class to exercise due care in collecting, storing, using and/or safeguarding their Private Information;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiffs and Class Members that their Private Information had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiffs' and Class Members' Private Information;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiffs' and Class Members' Private Information;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct; and

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiff Class. Representative Plaintiffs and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiffs in this class action is an adequate representative of each of the Plaintiff Class in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in its entireties. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought

> or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

89. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

90. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiffs.

91. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

92. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under NH RSA 358-A:10.

COMMON FACTUAL ALLEGATIONS

Defendant's Business

93. Defendant is a New Hampshire company offering "the highest standard of care" as a "leader in innovative orthopedics and services"[4] Defendant boasts a total annual revenue of $21.8 million.[5]

94. As part of its business, Defendant receives and maintains the Private Information of thousands of current and former patients. In doing so, Defendant implicitly promises to safeguard their Private Information.

95. In collecting and maintaining its current and former patients' private Information, Defendant agreed it would safeguard the data in accordance with state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Private Information

96. Indeed, Defendant boasts in its Privacy Policy that it "is required by law to maintain the privacy of your health information and to provide you with a description of our legal duties and privacy practices regarding your health information."[6]

97. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect its patients' Private Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Private Information.

---

[4] ASMO, linkedin, https://www.accesssportsmed.com/about-access/ (last visited September 19, 2024).

[5] Zoominfo, ASMO, https://www.zoominfo.com/c/access-sports-medicine/353576461 (last visited September 19, 2024).

[6] https://www.accesssportsmed.com/terms-and-conditions/ (last visited September 19, 2024).

The Cyberattack

98. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' Private Information. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

99. According to the Data Breach Notification and/or publicly filed documents, Representative Plaintiffs state, on information and belief, that thousands of persons were affected by the Data Breach.

100. Representative Plaintiffs were provided the information detailed above upon Representative Plaintiffs' receipt of a letter from Defendant. Representative Plaintiffs were not aware of the Data Breach until receiving that letter.

101. According to its Breach Notice, on May 10, 2024, Defendant discovered the Breach on May 10, 2024, when it "detected suspicious activity in its network environment. Following an internal investigation, Defendant discovered that an "unauthorized actor accessed certain files and data stored within our network.

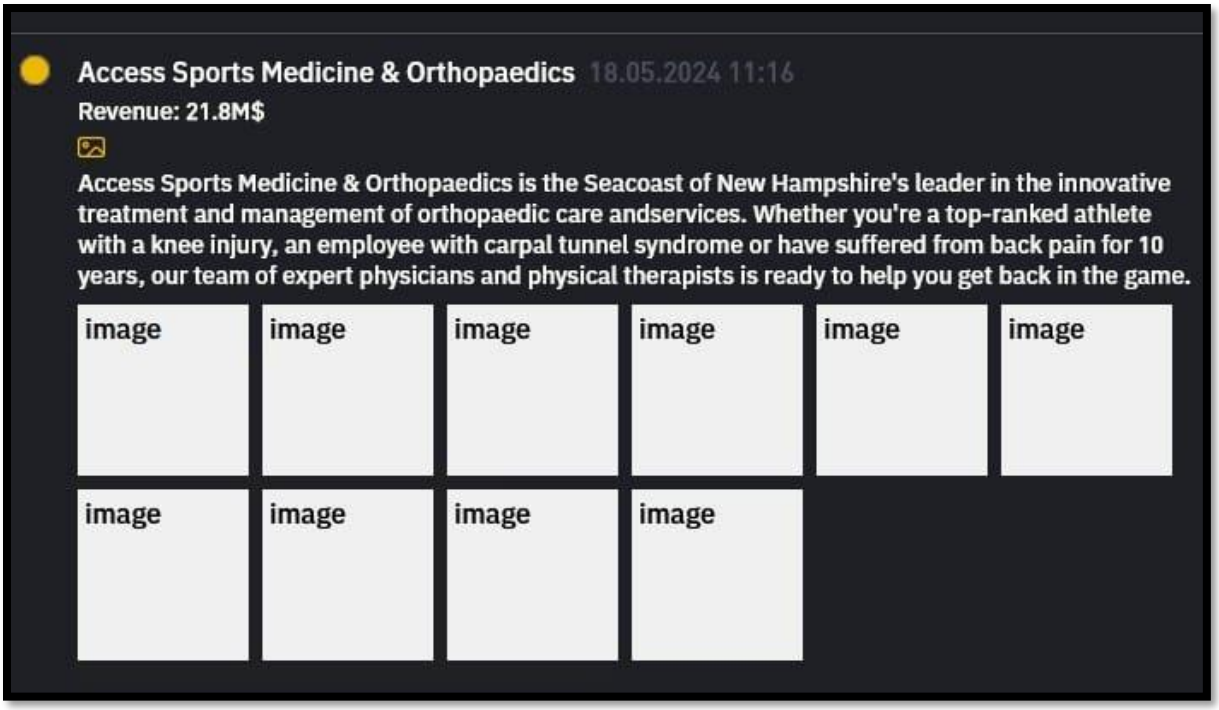
102. In other words, Defendant's cyber and data security systems were completely inadequate that it allowed cybercriminals to obtain files containing a treasure trove of thousands of its patients' highly sensitive Private Information.

103. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

104. Upon information and belief, the notorious ransomware gang 'Inc.' was responsible for the cyberattack. Known as one of the most notorious and active ransomware actors, Inc has

perpetrated multiple high-profile breaches in the last year alone.[7] Defendant knew or should have known of the tactics that groups like Inc employ.

105. With the Sensitive Information secured and stolen by Inc, the hackers then purportedly issued a ransom demand to Defendant. Though Defendant has provided no public information on the ransom demand or payment, on information and belief, Inc. began releasing files for download on May 18, 2024, and intends to release all stolen information on the dark web for access by cybercriminals following the deadline of its ransom demand.



106.

[7] Comperitech, https://www.comparitech.com/news/access-sports-medicine-and-orthopaedics-notifies-88k-people-of-data-breach-that-compromised-ssns-medical-and-financial-info/ (last visited Nov. 27, 2024).

Defendant's Failed Response to the Breach

107. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiff's and Class Members' Private Information with the intent of misusing the Private Information, including marketing and selling Representative Plaintiff's and Class Members' Private Information.

108. Not until long after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose Private Information Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

109. In response to the Data Breach, Defendant contends that it will "enhance the security of our systems." Although Defendant fails to expand on what these alleged "enhancements" are, such enhancements, if they get implemented at all, should have been in place before the Data Breach.

110. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to be "remain vigilant and monitor your accounts for suspicious or unusual activity."

111. Defendant also recognized through its Breach Notice, its duty to implement safeguards in accordance with state law, and federal law, insisting that, despite the Breach showing otherwise, "Access Sports takes the protection and proper use of your data very seriously."

112. Representative Plaintiffs and Class Members were required to provide their Private Information to Defendant in order to receive services. Thus, Defendant created, collected and stored Representative Plaintiffs' and Class Members' Private Information with the reasonable

expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

113. Despite this, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their Private Information going forward. Representative Plaintiffs and Class Members are thus left to speculate as to where their Private Information ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

114. Representative Plaintiffs' and Class Members' Private Information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without Representative Plaintiffs' and/or Class Members' approval. Either way, unauthorized individuals can now easily access Representative Plaintiffs' and Class Members' Private Information.

Defendant Collected/Stored Class Members' Private Information

115. Defendant acquired, collected, stored, and assured reasonable security over Representative Plaintiffs' and Class Members' Private Information.

116. As a condition of its relationships with Representative Plaintiffs and Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential Private Information. Defendant, in turn, stored that information unencrypted and in an internet accessible portion of Defendant's system that was ultimately affected by the Data Breach.

117. By obtaining, collecting and storing Representative Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties over the Private Information and knew or should have known that it was thereafter responsible for protecting Representative Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

118. Representative Plaintiffs and Class Members have taken reasonable steps to maintain their Private Information's confidentiality. Representative Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

119. Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' Private Information.

120. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' Private Information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

121. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

122. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' Private Information from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

123. In failing to adequately secure Representative Plaintiffs' and Class Member's sensitive data, Defendant breached duties it owed Representative Plaintiffs and Class Members under statutory and common law.

124. Representative Plaintiffs and Class Members surrendered their highly sensitive Private Information to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their Private Information, independent of any statute.

125. Moreover, under HIPAA, health insurance providers have an affirmative duty to keep patients' Private Information confidential. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' Private Information.

126. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is 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 Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

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

128. 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.

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

130. 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.

131. HIPAA also requires Defendant to "review and modify the security measures implemented […] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement 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). Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant 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."

132. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (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).

133. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. Defendant owed a duty to Representative Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks and protocols adequately protected Representative Plaintiffs' and Class Members' Private Information.

134. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain and test its computer systems, servers and networks to ensure that all Private Information in its possession was adequately secured and protected.

135. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all Private Information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

136. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

137. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

138. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its 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 the decision to entrust their Private Information to Defendant.

139. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

140. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' Private Information and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

141. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, medical 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 in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

142. The high value of Private Information to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[9] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[10]

143. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud.

144. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers, which were compromised for some Class Members in the Data Breach, are among the worst kind of Private Information to

---

[8] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

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

[10] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

145. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [11] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[12]

146. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

147. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[14] "Someone who has your SSN can use it to

[11] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.
[12] *Id.*
[13] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf
[14] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/

impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[15]

148. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

149. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

150. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves"

[15] *See* https://www.investopedia.com/terms/s/ssn.asp

[16] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

151. Theft of PHI is also 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."[17]

152. 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, PHI/PII 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.

153. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[18] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[19] In short, these sorts of data breaches are

[17] *Medical I.D. Theft*, EFraudPrevention https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited Nov. 27, 2023).

[18] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/.

[19] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.

increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[20]

154. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain Private Information compromised in the 2017 Equifax data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

155. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 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."

156. Identity thieves can use Private Information, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

[20] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/.

157. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

158. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

159. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[21]

160. 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

[21] "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 of 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.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

161. 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 Plaintiff's 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.

162. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiff and the other Class Members.

163. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

164. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

165. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[22]

[22] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Nov. 27, 2024).

166. 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.[23,24]

167. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[25]

168. As a result of the Data Breach, Representative 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 Representative Plaintiffs or Class Members for their property, resulting in an 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.

169. The ramifications of Defendant's failure to keep secure Representative Plaintiffs' and Class Members' Private Information are long lasting and severe. Once Private Information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Representative Plaintiffs' and Class Members' Private Information was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the Private Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

170. 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:

[23] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[24] https://datacoup.com/
[25] https://digi.me/what-is-digime/

> [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.[26]

171. The harm to Representative Plaintiffs and Class Members are especially acute given the nature of the leaked data. Medical 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.[27]

172. "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."[28]

173. When cybercriminals access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members.

174. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[29] Almost

---

[26] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf/.

[27] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

[28] *Id.*

[29] Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010),

half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[30]

175. And data breaches are preventable.[31] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[32] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…."[33]

176. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[34]

177. Here, Defendant knew of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' Private Information was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols

---

https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

30 *Id.*; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

31 Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

32 *Id.* at 17.

33 *Id.* at 28.

34 *Id.*

were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

178. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia,* (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' Private Information, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Plaintiff Class)

179. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

180. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia,* to act with reasonable care to secure and safeguard their Private Information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Representative Plaintiffs' and Class Members' Private Information on its computer systems.

181. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;

b. to protect Representative Plaintiffs' and Class Members' Private Information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their Private Information.

182. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

183. Defendant knew or should have known of the risks inherent in collecting and storing Private Information, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

184. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' Private Information.

185. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the Private Information that Representative Plaintiffs and Class Members had entrusted to it.

186. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' Private Information.

187. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

188. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with its Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the Private Information it stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

189. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiff and/or the remaining Class Members.

190. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' Private Information;

b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' Private Information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the Private Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information;

d. by failing to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiff's and Class Members' Private Information, misuse the Private Information and intentionally disclose it to others without consent;

e. by failing to adequately train its employees to not store Private Information longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' Private Information;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Representative Plaintiffs' and Class Members' Private Information and monitor user behavior and activity in order to identify possible threats.

191. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

192. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

193. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Private Information to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their Private Information.

194. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting excessively after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

195. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative

Plaintiffs and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or access their Private Information.

196. There is a close causal connection between Defendant's failure to implement security measures to protect Representative Plaintiffs' and Class Members' Private Information and the harm suffered, or risk of imminent harm suffered, by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' Private Information was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing and maintaining appropriate security measures.

197. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

198. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

199. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

200. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

201. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including, but not limited to, (i) actual identity theft, (ii) the loss of the opportunity of 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, tax fraud 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 embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' Private Information in its continued possession and (viii) 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 Representative Plaintiffs and Class Members.

202. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

203. Additionally, as a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession

and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Plaintiff Class)

204. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

205. Through their course of conduct, Defendant, Representative Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' Private Information.

206. Defendant solicited, invited and required Representative Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers by, in part, providing their Private Information to Defendant.

207. As a condition of being direct customers and/or employees of Defendant, Representative Plaintiffs and Class Members provided and entrusted their Private Information to Defendant. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiffs and Class Members if its data had been breached and compromised or stolen.

208. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide their Private Information to Defendant, in exchange for, amongst other things, the protection of their Private Information.

209. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

210. Defendant breached the implied contracts it made with Representative Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

211. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiffs and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time and (vi) other economic and noneconomic harm.

THIRD CLAIM FOR RELIEF
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Plaintiff Class)

212. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

213. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

214. Representative Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

215. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Representative Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

216. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

FOURTH CLAIM FOR RELIEF
Breach of the New Hampshire Unfair Competition Law- RSA 358-A
(On behalf of the Plaintiff Class)

217. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

218. Defendant is a "person" as defined by NH RSA 358-A.

219. Defendant violated NH RSA 358-A by engaging in unlawful, unfair and deceptive business acts and practices.

220. Defendant's "unfair" acts and practices include:

a. Defendant's failure to implement and maintain reasonable security measures to protect Representative Plaintiffs' and Class Members' Private

Information from unauthorized disclosure, release, data breaches and theft, which was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks and adequately maintain and/or improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Representative Plaintiffs and Class Members, whose Private Information has been compromised;

b. Defendant's failure to implement and maintain reasonable security measures, which was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45, *et seq.*); and

c. Defendant's failure to implement and maintain reasonable security measures, which also leads to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused.

221. Defendant's unlawful, unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Representative Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately maintain and/or improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Representative Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*;

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Representative Plaintiffs' and Class Members' Private Information; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*

176. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

177. As a direct and proximate result of Defendant's unfair, unlawful and fraudulent acts and practices, Representative Plaintiffs and Class Members were injured and lost money or property, including the price received by Defendant for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their Private Information.

178. Defendant acted intentionally, knowingly and maliciously to violate New Hampshire's Unfair Competition Law and recklessly disregarded Representative Plaintiffs' and Class Members' rights.

179. Representative Plaintiffs and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful and fraudulent business practices or use of their Private Information, declaratory relief, reasonable attorneys' fees and costs under NH RSA 358-A., injunctive relief and other appropriate equitable relief.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves, and on behalf of each member of the proposed Class, respectfully requests that the Court enter judgment in favor of Representative Plaintiffs and the Class and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify the proposed Class and/or any other appropriate subclasses under NH RSA 358-A:10, including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Representative Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including, but not limited to, an Order:

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

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

c. requiring Defendant to delete and purge Representative Plaintiffs' and Class Members' Private Information unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' Private Information;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' Private Information on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Representative Plaintiffs and Class Members;

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

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats that 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.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law; and

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually, and on behalf of the Plaintiff Class, hereby demand a trial by jury for all issues triable by jury.

Dated: December 6, 2024

By: /s/ *Robert S. Stephen*

Robert S. Stephen, Esq. NHBA #10064
STEPHEN LAW GROUP
582 Chestnut Street
Manchester, NH 03104
Telephone: (603) 663-1007
Email: rob@stephenlaw.com

Dated: December 6, 2024

By: /s/ *Nicholas S. Guerrera*

Nicholas S. Guerrera, Esq. NHBA #6520
SHAHEEN, GUERRERA & O'LEARY, LLC
820A Turnpike Street
North Andover, MA 01845
Telephone: (978)689-0800
Email: nguerrera@sgolawoffice.com

Scott Edward Cole, Esq. (CA S.B. #160744)*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com

Bryan L. Bleichner, Esq.*
Phillip J. Krzeski, Esq.*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612)-336-2940

Email: bbleichner@chestnutcambronne.com
Email: pkrzeski@chestnutcambronne.com

Gary Klinger, Esq.*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: (866) 252-0878
Email: gklinger@milberg.com

Interim Co-Lead Class Counsel

Biron L. Bedard, Esq. NHBA #8758
RANSMEIER & SPELLMAN, P.C.
Meaghan A. Jepsen NHBA #266707
1 Capitol Street, P.O. Box 600
Concord, NH 03302-0600
Telephone: (603) 228-0477
Email: bbedard@ranspell.com
Email: mjepsen@ranspell.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borrelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109 (
Email: sam@straussborrelli.com
Email: raina@straussborrelli.com

Christopher C. Snook, Esq. NHBA #274093
SEUFERT LAW OFFICES, PA
59 Central Street
Franklin, NH 03235
Telephone: (603) 934-9837
Facsimile: (603) 934-9838
Email: CSnook@seufertlaw.com

Andrew J. Shamis, Esq.*
Leanna A. Loginov, Esq.*
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 400
Miami, FL 33132
Telephone: (305) 479-2299
Email: ashamis@shamisgentile.com
Email: lloginov@shamisgentile.com

Leigh S. Montgomery, Esq.*
EKSM, LLP
1105 Milford Street

Houston, Texas 77006
Telephone: (888) 350-3931
Facsimile: (888) 276-3455
Email: lmontgomery@eksm.com

Attorneys for Representative Plaintiffs and the Plaintiff Class

**Pro hac vice forthcoming*

CERTIFICATE OF SERVICE

Nicholas S. Guerrera, counsel of record for the plaintiffs, hereby certifies that on this date the foregoing document was served upon the defendant, Access Sports Medicine and Orthopaedics, PLLC, by regular mail at 1 Hampton Road, Suite 200, Exeter, New Hampshire 03833

Dated: December 6, 2024 By: /s/ *Nicholas S. Guerrera*
Nicholas S. Guerrera, Esq. NHBA #6520