Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

In re American Addictions Centers, Inc. Data Breach Litigation.	Case No. 3:24-cv-01505 Class Action Jury Demand Chief Judge William L. Campbell, Jr. Magistrate Judge Barbara D. Holmes

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Ethan Parker, Tracy Lee Jay, Nikolaos Skourtis, Mary Deboer, James Bouchereau, Courtney Cox, Samantha Rainey, Athena Luth, Anell Capellan, Jason Lanagan, Chris Kidder, Patricia Ellison, and Ron Pronsky ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class Members"), by and through the undersigned attorneys, bring this Consolidated Class Action Complaint against Defendant American Addiction Centers, Inc., ("AAC" or "Defendant"), and alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which is based on personal knowledge:

NATURE OF THE CASE

1. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard personally identifiable information ("PII") and personal health information ("PHI"), including patients' names, Social Security numbers, dates of birth, health insurance information, medical information, and phone numbers belonging to approximately 422,424 individuals, including Plaintiffs.

2. AAC provides medical treatment including drug and alcohol addiction along with

mental and behavioral health issues to individuals, including Plaintiffs and Class Members.[1]

3. According to a "Data Breach Notice" AAC provided, a data breach occurred on its network between September 23 and September 26, 2024 (the "Data Breach"). [2]

4. AAC reported that, on or around September 26, 2024, it detected suspicious activity on its computer network, indicating a data breach. Based on a subsequent forensic investigation, AAC determined that cybercriminals infiltrated its inadequately secured computer environment and thereby gaining access to its patients' data files. The investigation further determined that, through this infiltration, cybercriminals potentially accessed and copied files containing the sensitive personal information of 422,424 individuals.[3]

5. According to AAC, the private information accessed by cybercriminals involved a wide variety of PII and PHI, including names, dates of birth, addresses, phone numbers, Social Security numbers, medical record numbers and identifiers, and health insurance information (collectively, "Private Information").[4]

6. AAC[5] is a publicly traded for-profit addiction treatment chain and, along with its affiliated providers, AdCare (MA & RI), the Greenhouse (TX), Desert Hope Center (NV), Oxford Treatment Center (MS), Recovery First (FL), Sunrise House (NJ), River Oaks Treatment Center (FL), and Laguna Treatment Hospital (CA)[6] operates in locations across the country, including

---

[1] https://americanaddictioncenters.org/.
[2] Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ff8926f7-302d-4cbb-a554-9b03d6b32d03.html.
[3] *Id.*
[4] Steve Adler, *American Addiction Centers Ransomware Attack Affects Almost 411,000 Patients*, THE HIPAA JOURNAL (Dec. 27, 2024), https://www.hipaajournal.com/american-addiction-centers-ransomware-attack.
[5] AAC Holdings Inc. (AACH), the parent company of American Addiction Centers, is currently an over-the-counter listed stock. *See AAC (AACH) Stock Price, News & Analysis*, https://www.marketbeat.com/stocks/OTCMKTS/AACH/.
[6] *Id.*

California, Florida, Massachusetts, Mississippi, Nevada, Rhode Island and Texas.[7]

7. As part of its business, and to generate profit, Defendant obtains and stores Plaintiffs' and Class Members' Private Information.[8]

8. By taking possession and control of Plaintiffs' and Class Members' Private Information, Defendant assumed a duty to securely store and protect Plaintiffs' and Class Members' Private Information of.

9. Defendant breached this duty and betrayed Plaintiffs' and Class Members' trust by failing to properly safeguard and protect their Private Information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

10. The cyberattack was detected on or around September 26, 2024. At that time, Defendant retained experts who conducted a forensic investigation which confirmed that a threat actor had access to its systems between September 23 and September 24, 2024, and during that time, exfiltrated files that included patient information.[9]

11. However, despite apparently learning of the Data Breach on or about September 26, 2024, AAC did not inform Plaintiffs, Class Members or other current and former patients of the Data Breach until December 23, 2024.

12. Due to Defendant's data security failures which resulted in the Data Breach,

[7] https://americanaddictioncenters.org/.
[8] *See, e.g.*, *Privacy Policy*, https://americanaddictioncenters.org/privacy-policy (providing "[n]on-personally identifiable visitor information (including unique device identifiers) may be provided to other parties for marketing, advertising, or other uses. We may disclose your personal information to a potential or actual acquirer, successor, or assignee as part of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock.")
[9] *Id.*

cybercriminals were able to target Defendant's computer systems and exfiltrate Plaintiffs' and Class Members' highly sensitive PII and PHI. As a result of this Data Breach, Plaintiffs' and Class Members' Private Information remains in the hands of those cybercriminals.

13. The Rhysida ransomware group has claimed responsibility for the attack. Rhysida reported that it exfiltrated 2.8 terabytes of patient data representing approximately over 400,000 current and former patients.[10]

14. Rhysida has conducted many recent attacks on healthcare organizations including Prospect Medical, Lurie Children's Hospital, and Axis Health System.[11] Rhysida attempts to sell the stolen data if the ransom is not paid. If a buyer can't be found, the stolen data is leaked on the group's data leak site, as was the case with this attack.[12]

15. According to cyberattack news sources, the data obtained from the Data Breach has been made available publicly, indicating that Rhysida was unable to extort American Addiction Centers.[13]

16. This was the third largest reported data breach during November 2024. Hacking and other IT incident reports accounted for 82% of data breaches during November 2024.[14]

17. Though Defendant has not revealed the vulnerabilities that Rhysida exploited, such

---

[10] Ionut Arghire, *American Addiction Centers Data Breach Impacts 422,000 People*, SECURITY WEEK (Dec. 24, 2024), https://www.securityweek.com/american-addiction-centers-data-breach-impacts-422000-people/.

[11] Marianne Kolbasuk McGee, *Rhysida Hacking Group Strikes More Healthcare Providers*, GOVINFOSECURITY (Mar. 10, 2025), https://www.govinfosecurity.com/rhysida-hacking-group-strikes-more-healthcare-providers-a-27677.

[12] Steve Adler, *American Addiction Centers Ransomware Attack Affects Almost 411,000 Patients*, THE HIPAA JOURNAL (Dec. 27, 2024), https://www.hipaajournal.com/american-addiction-centers-ransomware-attack/.

[13] *Toll of American Addiction Centers Hack Surpasses 422K*, SC MEDIA (Dec. 26, 2024), https://www.scworld.com/brief/toll-of-american-addiction-centers-hack-surpasses-422k.

[14] Steve Adler, *November 2024 Healthcare Data Breach Report* THE HIPAA JOURNAL (Dec. 23, 2024), https://www.hipaajournal.com/november-2024-healthcare-data-breach-report/.

that Plaintiff cannot allege those specific details with discovery, the known facts make clear that Defendant's cybersecurity posture was woefully inadequate.

18. For example, Defendant apparently did not realize that Rhysida had infiltrated its systems until after the hacker group was able to exfiltrate a tremendous amount of data—2.8 terabytes. In other words, Rhysida was able to look for a way in to Defendant's information system; exploit that vulnerability and gain access to Defendant's information system; perform the necessary reconnaissance measures required for it to know where Defendant stored these valuable files; likely perform measures like installing additional malware that require administrative privileges (as these steps are standard for such hacker groups); and then download that data from Defendant's information systems all without being caught.

19. These measures are noisy and would have been identified as malicious activity if Defendant had implemented any serious systems designed to identify malicious activity—such as endpoint detection and response, extended detection and response, intrusion detection systems, anomaly detection systems, or centralized alerting systems.

20. If Defendant had taken even the minimal effort to employee some or all of these systems necessary to detect malicious activity, then it would have at least noticed when the hacker group walked out the door with a massive amount of data—indeed, it is hard to imagine how anyone can miss such a spike in network activity.

21. Defendant's misconduct, including failing to implement adequate and reasonable measures to protect Plaintiffs' and Class Members' Private Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Private Information, and failing to provide timely and adequate notice of the Data Breach – caused

substantial harm and injuries to Plaintiffs and Class Members across the United States.

22. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals, for decades to come.

23. For example, now that their Private Information has been released onto the dark web, Plaintiffs are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, and such risk may last for the rest of their lives. Consequently, Plaintiffs must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

24. Plaintiffs bring this class action lawsuit to hold Defendant responsible for its grossly negligent—indeed, reckless—failure to use statutorily required or reasonable industry cybersecurity measures to protect Class Members' Private Information.

25. Plaintiffs bring this action individually and on behalf of the Class and seeks actual damages and restitution. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

JURISDICTION AND VENUE

26. The Class Action Fairness Act (CAFA) confers diversity jurisdiction to a class action where (1) the "matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs," and (2) "*any* member of a class of Plaintiffs is a citizen of a State different from any defendant." 28 U.S.C. § 1332(d)(2) (emphasis added).

27. This Court has diversity jurisdiction over this action under CAFA, 28 U.S.C. § 1332(d), because this is a class action consisting of more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least one member of the Class is a citizen of a State that differs from any Defendant.

28. This Court has personal jurisdiction over the parties in this case. Defendant conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

29. Venue is proper in this District under 28 U.S.C. §1391(b) because AAC and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

Plaintiffs

30. Plaintiff Ethan Parker is a citizen and resident of Danville, Virginia. Plaintiff is a victim of the Data Breach.

31. Plaintiff Parker is an AAC patient and Defendant stored and handled his Private Information because of his dealings with Defendant.

32. On or about December 23, 2024, Plaintiff Parker was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

33. Plaintiff Tracy Lee Jay is an adult individual and, at all relevant times herein, a resident and citizen of Maryland, residing in Baltimore, Maryland. Plaintiff is a victim of the Data Breach.

34. Plaintiff Jay is an AAC patient and Defendant stored and handled her Private Information because of her dealings with Defendant.

35. On or about December 23, 2024, Plaintiff Jay was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

36. Plaintiff Nikolaos Skourtis is an adult individual and, at all relevant times herein, a resident and citizen of Fitchburg, Massachusetts. Plaintiff is a victim of the Data Breach.

37. Plaintiff Skourtis is an AAC patient and Defendant stored and handled his Private Information because of his dealings with Defendant.

38. On or about December 23, 2024, Plaintiff Skourtis was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

39. Plaintiff Mary Deboer is an adult individual and, at all relevant times herein, a resident and citizen of Waco, Texas. Plaintiff is a victim of the Data Breach.

40. Plaintiff Deboer is an AAC patient and Defendant stored and handled her Private Information because of her dealings with Defendant.

41. On or about December 23, 2024, Plaintiff Deboer was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

42. Plaintiff James Bouchereau is an adult individual and, at all relevant times herein, a resident and citizen of Longmeadow, Massachusetts. Plaintiff is a victim of the Data Breach.

43. Plaintiff Bouchereau is an AAC patient and Defendant stored and handled his Private Information because of his dealings with Defendant.

44. On or about December 23, 2024, Plaintiff Bouchereau was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

45. Plaintiff Courtney Cox is an adult individual and, at all relevant times herein, a resident and citizen of Middlesex, Massachusetts. Plaintiff is a victim of the Data Breach.

46. Plaintiff Cox is an AAC patient and Defendant stored and handled her Private

Information because of her dealings with Defendant.

47. On or about December 23, 2024, Plaintiff Cox was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

48. Plaintiff Samantha Rainey is an adult individual and, at all relevant times herein, a resident and citizen of Southhaven, Mississippi. Plaintiff is a victim of the Data Breach.

49. Plaintiff Rainey is an AAC patient and Defendant stored and handled her Private Information because of her dealings with Defendant.

50. On or about December 23, 2024, Plaintiff Rainey was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

51. Plaintiff Athena Luth is an adult individual and, at all relevant times herein, a resident and citizen of Kailua Kona, Hawaii. Plaintiff is a victim of the Data Breach.

52. Plaintiff Luth is an AAC patient and Defendant stored and handled her Private Information because of her dealings with Defendant.

53. On or about December 23, 2024, Plaintiff Luth was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

54. Plaintiff Anell Capellan is an adult individual and, at all relevant times herein, a resident and citizen of Lawrence, Massachusetts. Plaintiff is a victim of the Data Breach.

55. Plaintiff Capellan is an AAC patient and Defendant stored and handled her Private Information because of her dealings with Defendant.

56. On or about December 23, 2024, Plaintiff Capellan was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

57. Plaintiff Jason Lanagan is an adult individual and, at all relevant times herein, a resident and citizen of Massachusetts. Plaintiff is a victim of the Data Breach.

58. Plaintiff Lanagan is an AAC patient and Defendant stored and handled his Private Information because of his dealings with Defendant.

59. On or about December 23, 2024, Plaintiff Lanagan was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

60. Plaintiff Chris Kidder is an adult individual and, at all relevant times herein, a resident and citizen of Las Vegas, Nevada. Plaintiff is a victim of the Data Breach.

61. Plaintiff Kidder is an AAC patient and Defendant stored and handled his Private Information because of his dealings with Defendant.

62. On or about December 23, 2024, Plaintiff Kidder was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

63. Plaintiff Patricia Ellison is an adult individual and, at all relevant times herein, a resident and citizen of Baltimore, Maryland. Plaintiff is a victim of the Data Breach.

64. Plaintiff Ellison is an AAC patient and Defendant stored and handled her Private Information because of her dealings with Defendant.

65. On or about December 23, 2024, Plaintiff Ellison was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

Defendant American addiction Centers, Inc.

66. Defendant American Addiction Centers, Inc., is a Tennessee corporation with its principal place of business at 500 Wilson Pike Circle, Brentwood, Tennessee 37027.

67. 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 Plaintiffs.

68. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names

and capacities of the responsible parties when their identities become known.

FACTUAL BACKGROUND

A. American Addiction Centers, Inc. and the Services it Provides.

69. AAC represents itself as the "leading provider for addiction treatment nationwide, which specializes in evidence-based treatment and mental healthcare services."[15]

70. While administering its services, AAC receives and handles PHI/PII, which includes, *inter alia*, patients' full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

71. Plaintiffs are required to entrust their highly sensitive PHI/PII to Defendant to participate in the treatment services it provides. Each Plaintiff entrusted this information to AAC with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

72. By obtaining, collecting, and storing Plaintiffs' PHI/PII, AAC assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiffs' PHI/PII from unauthorized disclosure.

73. And, upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members. Defendant also uses Plaintiffs' PHI/PII to generate additional revenue and profits.[16]

B. American Addiction Centers, Inc. Knew the Risks of Storing Valuable PHI/PII and the Foreseeable Harm to its Patients.

[15] *Id.* at n.1, *supra*.
[16] *Id.* at n.7, *supra*.

74. At all relevant times, AAC knew it was storing sensitive PHI/PII and that, as a result, its system would be an attractive target for cybercriminals.

75. Upon information and belief, Defendant's HIPAA Notice of Privacy Practices ("Privacy Policy") is provided to every patient both prior to receiving treatment and upon request.[17] Defendant's Privacy Notice makes clear that it understands that its patients' Private Information is personal and must be protected by law.

76. Defendant's own published privacy policy states that, "We are required by law to maintain the privacy of your PHI; provide you with notice of our legal duties and privacy practices with respect to your PHI; and to notify you following a breach of unsecured PHI related to you."[18]

77. AAC also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PHI/PII was compromised, as well as intrusion into their highly private health information.

78. These risks are not theoretical. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[19] "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[20]

79. Defendant agreed to and undertook legal duties to maintain the protected health and personal information Plaintiffs and Class Members entrusted to it safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15

---

[17] *Id.* at n.8, *supra*.
[18] https://americanaddictioncenters.org/notice-of-privacy-practices.
[19] *The Healthcare Industry Is at Risk*, SWIVELSECURE https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Apr. 17, 2023).
[20] *Id.*

U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

80. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

81. Through its failure to properly secure Plaintiffs' and Class Members' Private Information, Defendant failed to meet its own promises of patient privacy.

82. Nevertheless, Defendant failed to spend sufficient resources on preventing external access, detecting outside infiltration, and training its employees to identify email-borne threats and defend against them.

83. The stolen Private Information at issue has great value to the hackers, due to the large number of individuals affected and the fact the sensitive information that was part of the data that was compromised.

C. The Data Breach

84. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

85. On or around September 26, 2024, AAC detected suspicious activity on its computer network, indicating a data breach. Based on a subsequent forensic investigation, AAC determined that cybercriminals infiltrated its inadequately secured computer environment and thereby gained access to its data files. The investigation further determined that, through this infiltration, cybercriminals potentially accessed and copied files containing the sensitive personal information of 422,424 individuals.[21]

[21] *Id.* at nn. 2, 4, 10, *supra*.

86. According to AAC, the Private Information accessed by cybercriminals involved a wide variety of PII and PHI, including names, dates of birth, addresses, phone numbers, Social Security numbers, medical record numbers and identifiers, and health insurance information.

87. Defendant notified Department of Health and Human Services ("HHS") of the Data Breach on or about November 25, 2024, listing thousands of individuals affected.[22] Moreover, upon information and belief, Plaintiffs' and Class Members' PHI/PII had already been published on the dark web[23] prior to the time that AAC began sending notices to its patients regarding the Data Breach.

88. Based on the notice letter sent to Plaintiffs on December 23, 2024, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiffs' Private Information was stolen in the Data Breach.

89. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Private Information and has engaged in (and will continue to engage in) misuse of the Private Information, including marketing and selling Plaintiffs' and Class Members' Private Information on the dark web.

90. Since the Data Breach, according to cybersecurity news sources, at least one ransomware group, Rhysida ransomware group has claimed responsibility for the attack. Rhysida reported that it exfiltrated 2.8 terabytes of patient data representing approximately over 400,000 current and former patients.[24]

91. Despite the breadth and sensitivity of the PHI/PII that was exposed, and the

[22] U.S. Dep't of Health & Human Servs., *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Apr. 8, 2025).
[23] *Id.* at nn. 10-14, *supra*.
[24] *Id.*

attendant consequences to patients as a result of the exposure, AAC failed to disclose the Data Breach for weeks. This inexplicable delay further exacerbated the harms to Plaintiffs and Class Members.

92. Presently, however, Defendant has provided no public information on the ransom demand or payment.

D. Defendant had an Obligation to Protect Private Information under the Law and the Applicable Standard of Care

93. Defendant is 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).

94. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[25] and protection of PII[26] which includes basic security standards applicable to all types of businesses.

95. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

[25] Fed. Trade Comm'n, *Start with Security: A Guide for Business*, (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[26] Fed. Trade Comm'n, *Protecting Private Information: A Guide for Business*, (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

96. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[27]

[27] Federal Trade Comm'n, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-

97. Defendant is further required by various states' laws and regulations to protect Plaintiffs' and Class Members' Private Information.

98. Defendant owed a duty to Plaintiffs and the Class to design, maintain, and test its computer and application systems to ensure that the Private Information in its possession was adequately secured and protected.

99. Defendant owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees (and others who accessed Private Information within its computer systems) on how to adequately protect Private Information.

100. Defendant owed a duty to Plaintiffs and the Class to implement processes that would detect a breach on its systems in a timely manner.

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

102. Defendant owed a duty to Plaintiffs and the Class 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 Private Information with Defendant.

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

104. Defendant owed a duty of care to Plaintiffs and the Class because it was a foreseeable victim of a data breach.

E. Defendant Failed to Comply with HIPAA Guidelines

---

security-enforcement.

105. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security 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.

106. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[28] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

108. 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.

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

110. "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.

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

a. Ensure the confidentiality, integrity, and availability of all electronic protected

[28] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

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.

112. 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." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA 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).

113. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

114. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also 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."[29]

[29] U.S. Dep't of Health & Human Services, *Breach Notification Rule*,

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

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

117. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[30] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR indicates "represent the industry standard for good business practices with respect to standards for securing e-PHI." U.S Department of Health & Human Services, Guidance on Risk Analysis.[31]

---

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

[30] U.S. Dep't of Health & Human Servs., *Security Rule Guidance Material*, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Apr. 8, 2025).

[31] U.S. Dep't of Health & Human Servs., *Guidance on Risk Analysis*, https//www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Apr. 8, 2025).

F. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security

118. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[32] Yahoo,[33] Marriott International,[34] Chipotle, Chili's, Arby's,[35] and others.[36]

119. Defendant should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

120. Defendant was also on notice of the importance of data encryption of Private Information. Defendant knew it kept Private Information in its systems and yet it appears Defendant did not encrypt these systems or the information contained within them.

121. In January 2023, nearly two years before the attack, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like Defendant of the severe threats posed by cybercriminal groups.[37] Within the healthcare industry, the risk of a

---

[32] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[33] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[34] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[35] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others.

[36] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[37] U.S. Dep't of Health & Human Servs., *Royal & BlackCat Ransomware: The Threat to the Health Sector* (Jan. 12, 2023), https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf.

cyberattack is well-known and preventable with adequate security systems in place.

122. On or about December 23, 2024, months after Defendant learned that the Class Members' Private Information was attacked by cybercriminals, Defendant's patients began receiving their notices of the Data Breach informing them that its investigation determined that their Private Information was accessed.

123. Defendant's notice letters list time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Also, Plaintiffs would have to affirmatively sign up for a call center number that victims may contact with questions. Defendant offered one year of credit monitoring for members of the class and Defendant offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, Defendant sent a similar generic letter to all other individuals affected by the Data Breach.

124. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

125. Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

126. Defendant had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

127. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

128. It is well known that PII and PHI, including Social Security numbers in particular,

is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Defendant, are well-aware of the risk of being targeted by cybercriminals.

129. Individuals place a high value on the privacy of their PII and PHI. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

130. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[38]

131. Individuals, like Plaintiffs and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing one's DNA for hacker's purposes.

132. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim

[38] U.S. Dep't of Justice, *Victims of Identity Theft, 2018*, (April 2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

of Social Security number misuse.

133. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[39]

134. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[40]

135. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches from 2020. Over the next two years, in a poll of security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable cases will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[41]

136. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

---

[39] U.S. Social Security Admin, *Identity Theft and Your Social Security Number*, Pub. No. 05-10064 (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[40] Bree Fowler, *Data Breaches Break Record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/.

[41] Chuck Brooks, *Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864.

137. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [42] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[43]

138. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII and PHI private and secure, Defendant failed to take appropriate steps to protect Plaintiffs' and the proposed Class' PII and PHI from being compromised.

G. Data Breaches are Rampant in Healthcare.

139. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

140. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were

[42] Fed. Bureau of Investigations, *Common Frauds and Scams*, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited Apr. 8, 2025).
[43] *Id.*

classified as hacking/IT incidents."[44]

141. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[45]

142. The HIPAA Journal article goes on to explain that patient records, like those stolen from Defendant, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[46]

143. Data breaches such as the one Defendant experienced have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

144. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[47]

145. HHS data shows more than 39 million patients' information was exposed in the first half of 2023 in nearly 300 incidents and that healthcare beaches have doubled between 2020

---

[44] Steve Adler, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[45] *Id.*
[46] *Id.*
[47] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack,* SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

and 2023, according to records compiled from HHS data by Health IT Security.[48]

146. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[49]

147. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant.

H. Plaintiffs' Experiences

Plaintiff Ethan Parker

148. Plaintiff Ethan Parker is and was an AAC patient at all times relevant to this Complaint and Defendant stored and Defendant stored and handled his Private Information as a result of his dealings with Defendant. Plaintiff is a victim of the Data Breach.

149. On or about December 23, 2024, Plaintiff Parker was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

150. Plaintiff Parker is careful to protect his Private Information. Indeed, he uses a password manager to ensure any credentials he uses online are protected, and he still changes those passwords frequently.

151. The Notice Letter that Plaintiff received does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his name, "date of birth, dates of service, medical record number, patient account number, medical

[48] Jill McKeon, *Biggest Healthcare Data Breaches Reported This Year, So Far* (June 26, 2023), https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far.
[49] Advent Health Univ., *5 Important Elements to Establish Data Security in Healthcare* (May 21, 2020), https://www.ahu.edu/blog/data-security-in-healthcare (last visited February 13, 2025).

treatment/diagnosis information, and health insurance policy number."

152. Plaintiff Parker is especially alarmed by the vagueness in the Notice Letter regarding his stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

153. Since the Data Breach, Plaintiff Parker has tried to mitigate the damage by changing his passwords, contacting the credit bureaus as Defendant instructed, and monitoring his financial accounts for about 2 and a half hours per week, and freezing his credit. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes his time as a result of Defendant's negligence, but it also causes him great anxiety.

154. Soon after the Data Breach, Plaintiff Parker began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to his stolen PHI/PII.

155. Plaintiff Parker is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

156. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

157. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PHI/PII has been or will be misused and from the loss of his privacy.

158. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive

information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

159. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

160. Plaintiff has a continuing interest in ensuring that his PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

161. Had Plaintiff Parker been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with his PII and PHI.

162. As a result of Defendant's conduct, Plaintiff Parker suffered actual damages including, without limitation, time related to monitoring his financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Tracy Lee Jay

163. Plaintiff Tracy Lee is and was an AAC patient at all times relevant to this Complaint and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

164. On or about December 23, 2024, Plaintiff Jay was notified of the Data Breach and

of the impact to her PHI/PII via letter from AAC.

165. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

166. Plaintiff Jay is especially alarmed by the vagueness in the Notice Letter regarding her stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

167. Since the Data Breach, Plaintiff Jay has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes her great anxiety.

168. Soon after the Data Breach, Plaintiff Jay began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PHI/PII.

169. Plaintiff Jay is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

170. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

171. Indeed, Plaintiff Tracy Lee Jay has already begun to see the impact of Defendant's

failures in that she experienced an attempt to charge $800 to her card and another attempt by a hacker to change her email password. This required her time necessary to set things straight, including by spending time on the phone to stop the $800 charge.

172. Together with the time spent attempting to mitigate the risk of harm with the time spent responding to actual fraudulent attempts (which is a response effort and not a mitigation effort), Plaintiff Tracy Lee Jay has to date spent more than twenty hours because of Defendant's failures and should be compensated for this time that would otherwise have spent on her own tasks.

173. Plaintiff has experienced anxiety and increased concerns arising from the fact that her PHI/PII has been or will be misused and from the loss of her privacy.

174. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

175. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

176. Plaintiff has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

177. Had Plaintiff Jay been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

178. As a result of Defendant's conduct, Plaintiff Jay suffered actual damages including,

without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Nikolaos Skourtis

179. Plaintiff Nikolaos Skourtis is and was an AAC patient at all times relevant to this Complaint and Defendant stored and Defendant stored and handled his Private Information as a result of his dealings with Defendant. Plaintiff is a victim of the Data Breach.

180. On or about December 23, 2024, Plaintiff Skourtis was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

181. The Notice Letter that Plaintiff received does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

182. Plaintiff Skourtis is especially alarmed by the vagueness in the Notice Letter regarding his stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

183. Since the Data Breach, Plaintiff Skourtis has tried to mitigate the damage by changing his passwords, contacting the credit bureaus as Defendant instructed, and monitoring his financial accounts for about 2 and a half hours per week, and placing a freeze on his Experian credit account. This is more time than she spent prior to learning of the Defendant's Data Breach.

Having to do this every week not only wastes his time as a result of Defendant's negligence, but it also causes him great anxiety.

184. Soon after the Data Breach, Plaintiff Skourtis began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to his stolen PHI/PII.

185. Plaintiff Skourtis is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

186. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

187. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PHI/PII has been or will be misused and from the loss of his privacy.

188. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

189. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

190. Plaintiff has a continuing interest in ensuring that his PHI/PII which, upon

information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

191. Had Plaintiff Skourtis been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with his PII and PHI.

192. As a result of Defendant's conduct, Plaintiff Skourtis suffered actual damages including, without limitation, time related to monitoring his financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Mary Deboer

193. Plaintiff Mary Deboer is and was an AAC patient at all times relevant to this Complaint and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

194. On or about December 23, 2024, Plaintiff Deboer was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

195. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

196. Plaintiff Deboer is especially alarmed by the vagueness in the Notice Letter regarding her stolen extremely private PHI/PII as among the breached data on Defendant's

computer system.

197. Since the Data Breach, Plaintiff Deboer has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes him great anxiety.

198. Soon after the Data Breach, Plaintiff Deboer began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PHI/PII.

199. Moreover, Plaintiff Deboer received an Experian notification that it was aware of an address change when she had not moved—thus implying that someone was using her identity. She also received alerts that someone was attempting to log in to one of her accounts.

200. Though Plaintiff Deboer was offered credit monitoring services from Defendant, she had not enrolled because she was unsure if it would constitute a waiver of her rights to sue, and the letter failed to inform her of the same.

201. Plaintiff Deboer is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

202. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

203. Plaintiff has experienced anxiety and increased concerns arising from the fact that

her PHI/PII has been or will be misused and from the loss of her privacy.

204. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

205. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

206. Plaintiff has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

207. Had Plaintiff Deboer been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

208. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff James Bouchereau

209. Plaintiff Bouchereau is and was an AAC patient at all times relevant to this

Complaint and Defendant stored and Defendant stored and handled his Private Information as a result of his dealings with Defendant. Plaintiff is a victim of the Data Breach.

210. On or about December 23, 2024, Plaintiff Bouchereau was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

211. The Notice Letter that Plaintiff received does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

212. Plaintiff Bouchereau is especially alarmed by the vagueness in the Notice Letter regarding his stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

213. Since the Data Breach, Plaintiff Bouchereau has tried to mitigate the damage by changing his passwords, contacting the credit bureaus as Defendant instructed, and monitoring his financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes his time as a result of Defendant's negligence, but it also causes him great anxiety.

214. Notwithstanding his efforts to mitigate the risk of harm, that risk has nevertheless come to fruition.

215. Plaintiff Bouchereau has had six credit cards opened his name. Moreover, someone tried to open a renter's insurance policy in his name. which cost him half a day to get it cancelled. Even further, someone tried to open a bank account in his name in November 2024, which cost him an additional ten to twelve hours of this time.

216. Because of the fraudulent activity Plaintiff has seen, he has had to spend the

equivalent of four to five days of his time setting things straight because of the time it takes to get the right person on the phone and rarely getting prompt customer service. This time spent is in additional to the time spent mitigating the risk of even more identity theft and fraud.

217. Soon after the Data Breach, Plaintiff Bouchereau began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to his stolen PHI/PII.

218. Plaintiff Bouchereau is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

219. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

220. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PHI/PII has been or will be misused and from the loss of his privacy.

221. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

222. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

223. Plaintiff has a continuing interest in ensuring that his PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

224. Had Plaintiff Bouchereau been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with his PII and PHI.

225. As a result of Defendant's conduct, Plaintiff Bouchereau suffered actual damages including, without limitation, time related to monitoring his financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Courtney Cox

226. Plaintiff Courtney Cox is and was an AAC patient at all times relevant to this Complaint and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

227. On or about December 23, 2024, Plaintiff Cox was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

228. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

229. Plaintiff Cox is especially alarmed by the vagueness in the Notice Letter regarding

her stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

230. Since the Data Breach, Plaintiff Cox has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes him great anxiety.

231. Soon after the Data Breach, Plaintiff Cox began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PHI/PII.

232. Plaintiff Cox is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

233. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

234. Plaintiff has experienced anxiety and increased concerns arising from the fact that her PHI/PII has been or will be misused and from the loss of her privacy.

235. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

236. Plaintiff further suffered actual injury in the form of damages to and diminution in

the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

237. Plaintiff has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

238. Had Plaintiff Cox been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

239. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Samantha Rainey

240. Plaintiff Samantha Rainey is and was an AAC patient at all times relevant to this Complaint and Defendant stored and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

241. On or about December 23, 2024, Plaintiff Rainey was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

242. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her

name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

243. Plaintiff Rainey is especially alarmed by the vagueness in the Notice Letter regarding her stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

244. Since the Data Breach, Plaintiff Rainey has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes him great anxiety.

245. Soon after the Data Breach, Plaintiff Rainey began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PHI/PII.

246. Plaintiff Rainey is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

247. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

248. Plaintiff has experienced anxiety and increased concerns arising from the fact that her PHI/PII has been or will be misused and from the loss of her privacy.

249. The risk is not hypothetical. Here, a known hacking group intentionally stole the

data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

250. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

251. Plaintiff has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

252. Had Plaintiff Rainey been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

253. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Athena Luth

254. Plaintiff Athena Luth is and was an AAC patient at all times relevant to this Complaint and Defendant stored and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

255. On or about December 23, 2024, Plaintiff Luth was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

256. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, address, phone number, "date of birth, medical record number or other identifier, social security number, treatment information, and health insurance information."

257. Plaintiff Luth is especially alarmed by the vagueness in the Notice Letter regarding her stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

258. Since the Data Breach, Plaintiff Luth has tried to mitigate the damage by changing her passwords and monitoring her financial accounts. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes her great anxiety.

259. Soon after the Data Breach, Plaintiff Luth began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PHI/PII.

260. Plaintiff Luth is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

261. Plaintiff Luth has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

262. Plaintiff Luth has experienced anxiety and increased concerns arising from the fact

that her PHI/PII has been or will be misused and from the loss of her privacy.

263. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

264. Plaintiff Luth further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

265. Plaintiff has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

266. Had Plaintiff Luth been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

267. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Anell Capellan

268. Plaintiff Anell Capellan is and was an AAC patient at all times relevant to this

Complaint and Defendant stored and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

269. On or about December 23, 2024, Plaintiff Capellan was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

270. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

271. Plaintiff Capellan is especially alarmed by the vagueness in the Notice Letter regarding her stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

272. Since the Data Breach, Plaintiff Capellan has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes him great anxiety.

273. Soon after the Data Breach, Plaintiff Capellan began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PHI/PII.

274. Plaintiff Capellan is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

275. Indeed, Plaintiff Capellan received an alert from Experian notifying her that it had

found her information on the dark web.

276. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

277. Plaintiff has experienced anxiety and increased concerns arising from the fact that her PHI/PII has been or will be misused and from the loss of her privacy.

278. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

279. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

280. Plaintiff has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

281. Had Plaintiff Capellan been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

282. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal

information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Jason Lanagan

283. Plaintiff Jason Lanagan is and was an AAC patient at all times relevant to this Complaint and Defendant stored and Defendant stored and handled his Private Information as a result of his dealings with Defendant.

284. On or about December 23, 2024, Plaintiff Lanagan was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC. Plaintiff is a victim of the Data Breach.

285. The Notice Letter that Plaintiff received does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

286. Plaintiff Lanagan is especially alarmed by the vagueness in the Notice Letter regarding his stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

287. Since the Data Breach, Plaintiff Lanagan has tried to mitigate the damage by changing his passwords, contacting the credit bureaus as Defendant instructed, and monitoring his financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes his time as a result of Defendant's negligence, but it also causes him great anxiety.

288. Soon after the Data Breach, Plaintiff Lanagan began receiving an excessive number

of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to his stolen PHI/PII.

289. Plaintiff Lanagan is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

290. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

291. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PHI/PII has been or will be misused and from the loss of his privacy.

292. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

293. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

294. Plaintiff has a continuing interest in ensuring that his PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

295. Had Plaintiff Lanagan been aware that Defendant's computer systems were not

secure, she would not have entrusted Defendant with his PII and PHI.

296. As a result of Defendant's conduct, Plaintiff Lanagan suffered actual damages including, without limitation, time related to monitoring his financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Chris Kidder

297. Plaintiff Chris Kidder is and was an AAC patient at all times relevant to this Complaint and Defendant stored and Defendant stored and handled his Private Information as a result of his dealings with Defendant. Plaintiff is a victim of the Data Breach.

298. On or about December 23, 2024, Plaintiff Kidder was notified of the Data Breach and of the impact to his PHI/PII via letter from AAC.

299. The Notice Letter that Plaintiff received does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

300. Plaintiff Kidder is especially alarmed by the vagueness in the Notice Letter regarding his stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

301. Since the Data Breach, Plaintiff Kidder has tried to mitigate the damage by changing his passwords, contacting the credit bureaus as Defendant instructed, and monitoring his

financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes his time as a result of Defendant's negligence, but it also causes him great anxiety.

302. Soon after the Data Breach, Plaintiff Kidder began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to his stolen PHI/PII.

303. Plaintiff Kidder is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

304. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

305. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PHI/PII has been or will be misused and from the loss of his privacy.

306. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

307. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

308. Plaintiff has a continuing interest in ensuring that his PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

309. Had Plaintiff Kidder been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with his PII and PHI.

310. As a result of Defendant's conduct, Plaintiff Kidder suffered actual damages including, without limitation, time related to monitoring his financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Patricia Ellison

311. Plaintiff is and was an AAC patient at all times relevant to this Complaint and Defendant stored and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

312. On or about December 23, 2024, Plaintiff Ellison was notified of the Data Breach and of the impact to her PHI/PII via letter from AAC.

313. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

314. Plaintiff Ellison is especially alarmed by the vagueness in the Notice Letter

regarding her stolen extremely private PHI/PII as among the breached data on Defendant's computer system.

315. Since the Data Breach, Plaintiff Ellison has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes him great anxiety.

316. Soon after the Data Breach, Plaintiff Ellison began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PHI/PII.

317. Plaintiff Ellison is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

318. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PHI/PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

319. Indeed, Plaintiff Ellison has already seen the risk of identity theft and fraud come to fruition. She has had two credit cards opened in her name that she did not authorize, she has had hard inquiries on her credit that she did not authorize, and other items have appeared on her credit that she had not requested or authorized. Moreover, she has seen a significant drop in her credit score of over 50 points.

320. Plaintiff has experienced anxiety and increased concerns arising from the fact that

her PHI/PII has been or will be misused and from the loss of her privacy, including significant anxiety because of the fraudulent activity, loss of sleep, and paranoia.

321. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

322. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

323. Plaintiff has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

324. Had Plaintiff Ellison been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

325. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

I. Cyber Criminals Will Use Plaintiffs' and Class Members' Private Information to Defraud Them

326. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

327. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[50] For example, with the Private Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[51] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

328. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[52]

329. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because there, victims can cancel or close credit and debit card accounts. The information

---

[50] Insurance Info. Inst., *Facts + Statistics: Identity Theft and Cybercrime*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[51] John Egan, *What Should I Do If My Driver's License Number is Stolen* (June 13, 2024), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[52] U.S. Gov't Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, (July 5, 2007), https://www.gao.gov/products/gao-07-737.

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

330. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[53]

331. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiffs' and the Class Members' Private Information on the dark web. The Private Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

332. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[54]

333. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[55]

334. As described above, identity theft victims must spend countless hours and large

---

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

[54] Ari Lazarus, *How fast will identity thieves use stolen info?*, (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[55] U.S. Gov't Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, (July 5, 2007), https://www.gao.gov/products/gao-07-737.

amounts of money repairing the impact to their credit.[56]

335. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

336. Data Breach victims, like Plaintiffs and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[57]

337. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

338. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

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

b. Improper disclosure of their Private Information;

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

[56] Fed. Trade Comm'n, *Guide for Assisting Identity Theft Victims*, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.
[57] *Id.*

already misused;

d. The imminent and certainly impending risk of having their Private Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

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

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

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

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

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

339. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standards and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiffs' and Class Members' Private Information.

340. Plaintiffs and Class Members are desperately trying to mitigate the damage that Defendant has caused them but, given the Private Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Private

Information,

341. Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives.

342. None of this should have happened. The Data Breach was preventable.

J. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' Private Information

343. It is important to that that data breaches are preventable.[58] 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."[59] 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 . . . ."[60]

344. "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."[61]

345. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

346. In 2016, the FTC updated its publication, Protecting Private Information: A Guide

[58] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[59] *Id.* at 17.
[60] *Id.* at 28.
[61] *Id.*

for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[62]

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

348. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

349. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. See, e.g., In the Matter of Labmd, Inc., A Corp, 2016-2 Trade Cas. (CCH)

[62] Fed. Trade Comm'n, *Protecting Private Information: A Guide for Business*, (Oct. 2016). https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

350. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

351. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

352. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

353. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiffs' and Class Members' Private Information.

354. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

355. Defendant was at all times fully aware of its obligation to protect the Private Information of Plaintiffs and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

356. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained and/or exchanged, unencrypted, in Defendant's systems and were maintained in a condition vulnerable to cyberattacks.

357. Defendant knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if Plaintiffs' and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach.

358. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' Private Information from those risks left that information in a dangerous condition.

359. Defendant disregarded the rights of Plaintiffs and Class Members by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts 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 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 Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

J. Plaintiffs' And Class Members' Common Injuries

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

361. Defendant offered only one year of credit monitoring services to class Members.

362. Defendant fails to offer any compensation to victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

363. Furthermore, Defendant's failure to safeguard Plaintiffs' and Class Members' Private Information, places the burden squarely on Plaintiffs and the Class, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts and omissions resulting in the Data Breach. Defendant merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

364. Plaintiffs and Class Members have been damaged by the compromise and exfiltration, by cyber-criminals, of their Private Information as a result of the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

365. Plaintiffs and Class Members were damaged in that their Private Information is now in the hands of cyber criminals being sold and potentially for sale for years into the future.

366. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft, especially in light of the actual fraudulent misuse of the Private Information that has already taken place, as alleged herein.

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

368. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility

bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

369. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

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

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

372. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

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

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

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

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

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

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

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

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

373. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in Defendant's possession, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

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

375. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed

notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach since September 26, 2024 and did not notify the victims until December 23, 2024. Yet Defendant offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increased the injuries to Plaintiffs and the Class.

CLASS ACTION ALLEGATIONS

376. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

377. Plaintiffs bring all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons whose Private Information was compromised because of the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about January 8, 2025 (the "Class" or "Class Members").

378. This proposed Class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the Class definition in an amended pleading or when they move for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

379. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

380. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

381. N**umerosity** – Fed. R. Civ. P. 23(a)(1): Plaintiff is informed and believes, and thereon alleges, that there are at minimum, over 400,000 members of the Class described above.

The exact size of the Class and the identities of the individual members are identifiable through AAC's records, including but not limited to the files implicated in the Data Breach.

382. **Commonality** – Fed. R. Civ. P. 23(a)(2): This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether AAC had a duty to protect Plaintiffs' and Class Members' PHI/PII;

b. Whether AAC was negligent in collecting and storing Plaintiffs' and Class Members' PHI/PII, and breached its duties thereby;

c. Whether AAC was unjustly enriched;

d.

e. Whether AAC entered a contract implied in fact with Plaintiffs and the Class;

f. Whether AAC breached that contract by failing to adequately safeguard Plaintiffs' and Class Members' PHI/PII;

g. Whether AAC breached its fiduciary duty to Plaintiffs and the Class;

h. Whether AAC violated its own Privacy Practices;

i. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class and the general public;

j. Whether Plaintiffs and Class Members are entitled to damages as a result of AAC's wrongful conduct; and

k. Whether Plaintiffs and Class Members are entitled to restitution as a result of AAC's wrongful conduct.

383. **Typicality** – Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs' and Class Members' claims are based on the same legal

theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in AAC's system, each having their PHI/PII exposed and/or accessed by an unauthorized third party.

384. **Adequacy of Representation** – Fed. R. Civ. P. 23(a)(3): Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex Class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

385. **Injunctive Relief**, Fed. R. Civ. P. 23(b)(2): Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

386. **Superiority**, Fed. R. Civ. P. 23(b)(3): A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for AAC. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and

protects the rights of each Class member.

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

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

a. Whether AAC failed to timely and adequately notify the public of the Data Breach;

b. Whether AAC owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PHI/PII;

c. Whether AAC's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether AAC's failure to institute adequate protective security measures amounted to negligence;

e. Whether AAC failed to take commercially reasonable steps to safeguard consumers' and employees' PHI/PII; and

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

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and Class Members)

390. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

391. Defendant required Plaintiff and Class Members to submit non-public personal information to obtain healthcare/medical services and/or employment.

392. By collecting and storing this data in Defendant's computer network and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer network—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

393. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

395. Defendant's duty to use reasonable security measures under HIPAA required

Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

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

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

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

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

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

d. Allowing unauthorized access to Class Members' Private Information;

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

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

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

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

401. Moreover, though Defendant has not publicly identified the vulnerability or vulnerabilities that were exploited, its complete failure to identify the malicious activity notwithstanding that the hackers walked out the door with a massive 2.8 terabytes of data shows that Defendant failed to get even the basics right—tools designed to at least identify malicious activity. Defendant's failure to do even the basics constitutes gross negligence.

COUNT TWO
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and Class Members)

402. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

403. Plaintiffs and the Class bring this claim in the alternative to all other claims and remedies at law.

404. Plaintiffs and Class Members conferred a benefit on AAC in the form of profits to render certain services, a portion of which was intended to have been used by AAC for data security measures to secure Plaintiffs' and Class Members' PHI/PII.

405. AAC enriched itself by saving the costs it reasonably should have expended on data

security measures to secure Plaintiffs' and Class Members' PHI/PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, AAC chose to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of AAC's failure to provide adequate security.

406. Under the principles of equity and good conscience, AAC should not be permitted to retain the full value of its profits resulting from its collection and storage of the Plaintiffs' and Class Members' PHI/PII, because AAC failed to implement appropriate data management and security measures that are mandated by industry standards.

407. If Plaintiffs and Class Members knew that AAC had not secured their PHI/PII, they would not have agreed to disclose their data to AAC's clients.

408. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with the entities that collected Plaintiffs' and the Class Members' Private Information, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiffs' and Class Members' Private Information.

409. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Private Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class Members.

410. Defendant failed to implement—or adequately implement—data security practices, procedures, and programs to secure sensitive Private Information, including without limitation

those industry standard data security practices, procedures, and programs discussed herein.

411. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiffs and Class Members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of Private Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

412. Defendant, upon information and belief, has therefore engaged in opportunistic and unethical conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and Class Members' interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

413. Accordingly, Plaintiffs and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

COUNT THREE
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and Class Members)

414. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

415. Plaintiffs and Class Members were required to provide Defendant with their Private Information in order to receive medical care and treatment.

416. When Plaintiffs and Class Members provided their Private Information to Defendant when seeking medical services, they entered into implied contracts in which Defendant

agreed to comply with its statutory and common law duties to protect their Private Information and to timely notify them in the event of a Data Breach.

417. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' Private Information, Defendant had an implied duty to safeguard their Private Information through the use of reasonable industry standards. This implied duty was reinforced by Defendant's representations in its Privacy Policy.

418. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant months to warn Plaintiffs and Class member of their imminent risk of identity theft. Defendant also failed to notify Plaintiffs and the Class Members whether or not their driver's license numbers were compromised, leaving Plaintiffs and Class Members unsure as to the extent of the information that was compromised.

419. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' Private Information.

420. Plaintiffs and Class Members were required to provide Defendant with their Private Information in order to receive treatment, pharmaceuticals and/or services.

421. When Plaintiffs and Class Members provided their Private Information to Defendant when seeking care or services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Private Information and to timely notify them in the event of a Data Breach.

422. Based on Defendant's representations, legal obligations, and acceptance of

Plaintiffs' and the Class Members' Private Information, Defendant had an implied duty to safeguard their Private Information through the use of reasonable industry standards. This implied duty was reinforced by Defendant's representations in its HIPAA disclosures.

423. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant weeks to warn Plaintiffs and Class Members of their imminent risk of identity theft. The vagueness of the breach notification also left Plaintiffs and Class Members unsure as to the extent of the information that was compromised.

424. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' Private Information.

COUNT FOUR
INVASION OF PRIVACY
(On Behalf of Plaintiffs and Class Members)

425. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

426. Plaintiffs and Class Members took reasonable and appropriate steps to keep their Private Information confidential from the public, yet Plaintiffs and Class Members still suffered an invasion of their privacy and an invasion of their right to control who had access to their Private Information because of Defendant's failure to properly protect the data it collected.

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

428. Defendant owed a duty to its clients, including Plaintiffs and the proposed Class Members, to keep their Private Information confidential.

429. The unauthorized release of Private Information, especially Social Security numbers and protected health information, is highly offensive to any reasonable person.

430. Plaintiffs' and Class Members' Private Information is not of legitimate concern to the public, and Defendant knew that Plaintiffs' and Class Members' Private Information was private and was to be kept confidential.

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

432. Indeed, the definition of publication is met regardless of the number of cybercriminals who gained access to the information because those cybercriminals are in a special relationship with Plaintiffs and the proposed Class in that they are the exact group of individuals that reasonable cybersecurity measures are intended to protect Plaintiffs and the proposed Class Members from.

433. Moreover, given that the practice of cybercriminals is to share stolen data amongst themselves for even further misuse, it is likely that Plaintiffs' and Class Members' Private Information is at present being proliferated amongst cybercriminals and other identity thieves to be exploited and misused.

434. Moreover, because of the ubiquitous nature of data breaches, Defendant was substantially certain that a failure to protect Private Information would lead to its disclosure to

unauthorized third parties, including the thousands of waiting identity thieves who are in a special relationship to Plaintiffs and the proposed Class Members. Thus, the definition of intent under Section 8A of the Restatement was met here.

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

COUNT FIVE
DECLARATORY/INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and Class Members)

436. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

437. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the Private Information it collected from Plaintiffs and the Class.

438. Defendant owes a duty of care to Plaintiffs and Class Members that requires it to adequately secure Private Information.

439. Defendant still possess Private Information regarding Plaintiffs and Class Members.

440. Since the Data Breach, Defendant has announced few if any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and go undetected for months

and, thereby, prevent further attacks.

441. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

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

443. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

444. Plaintiffs, therefore, seeks a declaration that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security and that to comply with its contractual obligations and duties of care, Defendant must implement and maintain additional security measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such

other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

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

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

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

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

v. Ordering that Defendant cease transmitting Private Information via unencrypted email;

vi. Ordering that Defendant cease storing Private Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably

secure manner customer data not necessary for its provisions of services;

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

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

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

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

DEMAND FOR JURY TRIAL

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

J. Gerard Stranch, IV (BPR 023045)
Grayson Wells (BPR 039658)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801

gstranch@stranchlaw.com
gwells@stranchlaw.com

Interim Class Counsel

Marc H. Edelson
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
Tel: (215) 867-2399
medelson@edelson-law.com

Eduard Korsinsky
LEVI & KORSINSKY, LLP
55 Broadway, 10th Floor
New York, NY 10006
Tel: (212) 363-7500
ek@zlk.com

Mark Svensson
LEVI & KORSINSKY, LLP
33 Whitehall Street
17th Floor
New York, NY 10004
212-363-7500
msvensson@zlk.com

Lynn A. Toops
Amina A. Thomas
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
(317) 636-6481
ltoops@cohenmalad.com
athomas@cohenmalad.com

Leigh S. Montgomery
ELLZEY & ASSOCIATES, PLLC
1105 Milford Street
Houston, TX 77006
Tel: (888) 350-3931
leigh@ellzeylaw.com

Philip J. Krzeski
CHESTNUT CAMBRONNE PA
100 Washington Ave. South, Ste. 1700

Minneapolis, MN 55401
Tel: (612) 339-7300
bbleichner@chestnutcambronne.com

Andrew J. Shamis
SHAMIS & GENTILE, PA
14 NE 1st Avenue, Suite 1205
Miami, FL 33132
Tel: (305) 479-2299
ashamis@shamisgentile.com

A. Brooke Murphy
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
abm@murphylegalfirm.com

Daniel Srourian
SROURIAN LAW FIRM, P.C.
468 N. Camden Drive, Suite 200
Beverly Hills, CA 90210
Tel: (213) 747-3800
daniel@slfla.com

R. Scott Pietrowski
SIRI & GLIMSTAD LLP
4780 I-55 North, Suite 100
Jackson, MS 39211
Tel: (601) 274-4252
spietrowski@sirillp.com

Tyler J. Bean
Sonjay Singh
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: (212) 532-1091
ssingh@sirillp.com
tbean@sirillp.com

Alexandra M. Honeycutt
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Tel: 865-247-0080

ahoneycutt@milberg.com

Mariya Weekes
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (954) 647-1866
mweekes@milberg.com

Jeff Ostrow
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
1 W Las Olas Boulevard, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

William B. Federman
Tanner Hilton
FEDERMAN & SHERWOOD
10205 N Pennsylvania Avenue
Oklahoma City, OK 73120
Tel: (405) 235-1560
wbf@federmanlaw.com
trh@federmanlaw.com

Gary S. Graifman
Melissa R. Emert
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Road, Suite 200
Chestnut Ridge, NY 10977
Tel: (845) 356-2570
memert@kgglaw.com
ggraifman@kgglaw.com

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that the foregoing Motion to Consolidate and Appoint Interim Class Counsel was filed and served via the court's CM/ECF electronic filing system on this 21st day of April 2025, and to the following:

Alan S. Bean
STARNES DAVIS FLORIE, LLP
3000 Meridian Blvd.
Ste. 350
Franklin, TN 37067-6673
Phone: 615-905-7200
Fax: 615-807-4802
Email: abean@starneslaw.com