UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

IN RE ANNE ARUNDEL DATA BREACH LITIGATION	**Case No.: 1:25-cv-02274**
	DEMAND FOR JURY TRIAL

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Natalia Correa, Peyton Sulkowski, Jennifer Longwell, Shemika Jones, Brice Farris, Michael Straw, Barbara Buracker, Paul Gale, Earl Beville Jr., Steven Boehm, Paul Madigan, Heidi Shell, Troy Botteon, Richard Bernard, Jason Tyson, Crystal Hall, Terri Wilson, Raven Martin, Jacqueline Smith, and Alunda Mitchell, on behalf of J.D., a minor, Diana Wilson, and George Tyler (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Anne Arundel Dermatology, P.A. ("AAD" or "Defendant") based on personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against AAD for its failure to properly secure and safeguard from criminal hackers Plaintiffs' and other similarly situated AAD patients' personally identifiable information ("PII") and protected health information ("PHI"), including, *inter alia*, names, addresses, date(s) of birth, patient ID, medical record numbers, health history, and insurance information (collectively, "Private Information").

2. AAD, based in Linthicum Heights, Maryland, is a network of dermatological clinics that offers a wide variety of medical, surgical, and cosmetic dermatology treatments. AAD serves thousands of patients in the Mid-Atlantic and Southeastern regions.

3. On or about July 11, 2025, AAD filed an official notice of a hacking incident with the Office of the Texas Attorney General.[1] Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or about the same date, AAD also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiffs and "Class Members" (defined below), after detecting unusual activity on some of its computer systems, Defendant launched an investigation, which determined that an unauthorized cybercriminal had gained *three months* of unfettered access to a gold mine of highly sensitive patient data. Specifically, the unauthorized access occurred from between February 14, 2025 to May 13, 2025 (referred to herein as the "Data Breach").

6. As a result of the Data Breach, Plaintiffs and Class Members were, and continue to be, at significant risk of identity theft and various other forms of personal and social harm.

7. Armed with the Private Information accessed in the Data Breach (and a months-long head start), data thieves have already committed a wide variety of fraudulent acts and identity theft against Plaintiffs and Class Members, including in the form of, *e.g.*, unauthorized charges to their payment cards, opening unauthorized accounts in their names, and carrying out fraudulent attempts to access their online accounts.

[1] *See Data Security Breach Reports*, ATT'Y GEN. OF TEX., https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (keyword: ANNE ARUNDEL) (last visited Dec. 10, 2025).

8. There has been no assurance from AAD that all personal data or copies of data have been recovered or destroyed or that AAD has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

9. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiffs bring this class action lawsuit to address AAD's inadequate safeguarding of Plaintiffs' and Class Members' Private Information, and AAD's failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed by cybercriminals without their knowledge or consent.

11. Because the potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to AAD, AAD was on notice that its failure to properly secure Plaintiffs' and Class Members' Private Information left it vulnerable to an attack.

12. Upon information and belief, AAD failed to properly monitor or implement security practices as to the computer network and systems that housed the Private Information. Had AAD properly secured or monitored its networks, it would have discovered the Data Breach sooner or prevented it altogether.

13. Because of AAD's negligent conduct, Plaintiffs' and Class Members' Private Information that AAD collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all others similarly situated whose Private Information was accessed and/or compromised during the Data Breach.

II. PARTIES

15. Plaintiff Natalia Correa is, and at all times mentioned herein was, an individual citizen of the State of Florida.

16. Plaintiff Peyton Sulkowski is, and at all times mentioned herein was, an individual citizen of the State of Georgia

17. Plaintiff Jennifer Longwell is, and at all times mentioned herein was, an individual citizen of the State of Florida.

18. Plaintiff Shemika Jones is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

19. Plaintiff Brice Farris is, and at all times mentioned herein was, an individual citizen of the Commonwealth of Pennsylvania.

20. Plaintiff Michael Straw is, and at all times mentioned herein was, an individual citizen of the State of Tennessee.

21. Plaintiff Barbara Buracker is, and at all times mentioned herein was, an individual citizen of the State of North Carolina.

22. Plaintiff Paul Gale is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

23. Plaintiff Earl Beville, Jr. is, and at all times mentioned herein was, an individual citizen of the State of Tennessee.

24. Plaintiff Steven Boehm is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

25. Plaintiff Paul Madigan is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

26. Plaintiff Heidi Shell is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

27. Plaintiff Troy Botteon is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

28. Plaintiff Richard Bernard is, and at all times mentioned herein was, an individual citizen of the State of Georgia.

29. Plaintiff Jason Tyson is, and at all times mentioned herein was, an individual citizen of the State of North Carolina.

30. Plaintiff Crystal Hall is, and at all times mentioned herein was, an individual citizen of the State of Tennessee.

31. Plaintiff Terri Wilson was an individual citizen of the State of Tennessee up and until November 29, 2024, upon which time she relocated and became, and remains a citizen of, the Commonwealth of Kentucky.

32. Plaintiff Raven Martin is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

33. Plaintiff Jacqueline Smith is, and at all times mentioned herein was, an individual citizen of the State of North Carolina.

34. Plaintiff Alunda Mitchell, on behalf of J.D., a minor, is, and at all times mentioned herein was, an individual citizen of the State of Georgia.

35. Plaintiff Diana Wilson is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

36. Plaintiff George Tyler is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

37. Defendant AAD is a network of dermatological clinics with its principal place of business at 1306 Concourse Drive, Suite 201, Linthicum Heights, Maryland 21090, in Anne Arundel County.

III. JURISDICTION AND VENUE

38. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from AAD. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

39. This Court has general jurisdiction over AAD because AAD is incorporated in the State of Maryland and maintains its headquarters in this District.

40. This Court has specific personal jurisdiction over AAD because AAD has availed itself of the rights and benefits of the State of Maryland, including by (1) providing services in this District, (2) conducting substantial business in this District, and (3) perpetuating unlawful acts in this District.

41. Venue is proper in this District under 28 U.S.C. § 1391(a)–(d) because a substantial part of the events giving rise to this action occurred in this District, and Defendant caused harm to Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. AAD's Business and Collection of Plaintiffs' and Class Members' Private Information

42. Founded in 1974, AAD maintains over 60 locations led by 155 clinicians and advertises itself as "[o]ne of the largest and most well-established dermatology practices in the Mid-Atlantic and Southeastern states."[2] AAD's services include medical dermatology, surgical dermatology, cosmetic services, and dermatopathology, which it provides to thousands of patients in Florida, Georgia, Maryland, North Carolina, Pennsylvania, Tennessee and Virginia.[3] AAD employs more than 450 people and generates approximately $151.9 million in annual revenue.[4]

43. As a condition of receiving dermatological services, AAD requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from AAD, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

44. The first line of AAD's Notice of Privacy Practices states: **"We have a legal duty to safeguard your protected health information."**[5] AAD's Notice of Privacy Practices also describes specific duties held by AAD with regards to patient's Private Information, including the limited circumstances under which AAD is permitted to disclose patient Private Information without written authorization (none of which are relevant here), and AAD's duty to notify patients of a breach of their Private Information.[6]

---

[2] *Homepage*, ANNE ARUNDEL DERMATOLOGY, https://aadermatology.com/ (last visited Dec. 10, 2025).
[3] *Id.*; *Locations*, ANNE ARUNDEL DERMATOLOGY, https://aadermatology.com/locations/ (last visited Dec. 10, 2025).
[4] *Anne Arundel Dermatology*, ROCKETREACH, https://rocketreach.co/anne-arundel-dermatology-profile_b5eb07d8f42e7bc4 (last visited Dec. 10, 2025).
[5] *Notice of Privacy Practices*, ANNE ARUNDEL DERMATOLOGY, https://aadermatology.com/hipaa-privacy-notice/ (last visited Aug. 26, 2025).
[6] *Id.*

45. Upon information and belief, AAD's Notice of Privacy Practices is provided to all patients, including Plaintiffs and Class Members, prior to their receipt of services from AAD and upon their requests.

46. Thus, due to the highly sensitive and personal nature of the patient information AAD acquires and stores, AAD, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security; comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

47. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, AAD assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

48. Plaintiffs and Class Members relied on AAD to keep their Private Information confidential and securely maintained and to only make authorized disclosures of their Private Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members

49. According to Defendant's Notice, unauthorized access to its computer systems lasted for three long months: from February 14, 2025 and May 13, 2025.

50. Indeed, through the Data Breach, the unauthorized cybercriminal(s) acquired three months of unfettered access to highly sensitive Private Information, including, *inter alia*, names,

addresses, dates of birth, patient ID, medical record numbers, health history, and insurance information of almost two million individuals.

51. On or about July 11, 2025, approximately four months after Plaintiffs' and Class Members' Private Information was first accessed by cybercriminals, AAD finally began notifying patients their Private Information was involved in the Data Breach by delivering Notices to Plaintiffs and Class Members.

52. Omitted from the Notice are crucial details including the root cause of the Data Breach, the vulnerabilities exploited, the remedial measures undertaken to terminate the Data Breach and steps taken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

53. Thus, AAD's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

54. In addition, the Notice provides no substantive steps to assist victims like Plaintiffs and Class Members in protecting themselves other than providing two year(s) of credit monitoring—an offer that is woefully inadequate considering the heightened risk of fraud and identity theft Plaintiffs and Class Members now face as a result of the Data Breach.

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

56. Plaintiffs and Class Members provided their Private Information to AAD with the reasonable expectation and mutual understanding that AAD would comply with its obligations to keep such Private Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

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

58. AAD knew or should have known that its electronic records would be targeted by cybercriminals.

59. Instead, AAD failed to abide by its own Notice of Privacy Practices and other legal obligations.

60. Further, AAD's own Notice sent to Plaintiffs and Class Members demonstrates that AAD:

a. failed to adequately encrypt, redact, and protect Plaintiffs' and Class Members' Private Information;[7]

b. failed to maintain adequate tools to detect network intrusions;[8]

c. failed to maintain adequate tools to log network access;[9]

d. failed to maintain adequate tools to log file access and data exfiltration;[10] and

[7] *See* https://ago.vermont.gov/sites/ago/files/documents/2025-07-11%20Anne%20Arundel%20Dermatology%20Data%20Breach%20Notice%20to%20Consumers.pdf (admitting that "certain data files were accessible to the unauthorized third party" during the Data Breach).

[8] *Id.* (admitting that the unauthorized access begun around February 14, 2025, but AAD did not discover it until sometime around May 13, 2025, *nearly three months later*).

[9] *Id.* (admitting that AAD was unable to determine exactly when the unauthorized access began and could determine only that the unauthorized access "*may* have begun on February 14, 2025") (emphasis added).

[10] *Id.* (admitting that after over a month of analysis, AAD could not determine for certain "whether the third party actually viewed or exfiltrated [] information").

e. was able to implement reasonable safeguards that would have prevented or mitigated the effects of the Data Breach but failed to do so.[11]

61. Further, the cybersecurity company, Strobes, reports that the Data Breach likely occurred due to compromised remote desktop credentials or an unpatched vulnerability, which resulted in a ransomware attack.[12]

62. Strobes further reports that the "lack of network segmentation and endpoint monitoring allowed the attackers to operate undetected. Implementing [Endpoint Detection and Response] tools, network segmentation, and regular vulnerability scanning would have reduced the attack surface and limited lateral movement."

63. Upon information and belief, Plaintiffs' and the Class's stolen Private Information has now been published by cybercriminals to the Dark Web as that is the modus operandi of ransomware attackers.[13] Indeed, as the Harvard Business Review notes, "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[14]

---

[11] *Id.* (admitting that after its discovery of the Data Breach, AAD was able to take "immediate action to… secure [its] systems").

[12] https://strobes.co/blog/top-6-data-breaches-in-july-2025/ ("Ransomware operators infiltrated the provider's network, likely via compromised RDP credentials or an unpatched vulnerability. Once inside, they moved laterally to escalate privileges, exfiltrating and encrypting sensitive data.").

[13] https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware (Typically, in a ransomware attack, the criminal actor will not only encrypt the victim's system and block access until a ransom is paid but also exfiltrate data and threaten to release it to the dark web if a ransom is not paid. This scheme is known as a double-extortion attack. This scheme is used because many "organizations overcome the threat of file encryption with a simple up-to-date backup system.").

[14] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

C. The Healthcare Sector Is Particularly Susceptible to Data Breaches

64. AAD was on notice that companies in the healthcare industry are especially susceptible targets for data breaches. Given its role in handling sensitive patient data, Defendant was well aware at all relevant times that the Private Information it obtains, collects, stores, uses, and derives a benefit from is highly sensitive and of significant value to those who seek to use it for wrongful purposes.

65. Defendant also knew that a breach of its computer systems and the resulting exposure of the information stored therein would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised as well as intrusion into their highly private health information.

66. In August 2014, after a cyberattack on Community Health Systems, Inc., the Federal Bureau of Investigation ("FBI") warned companies in the healthcare industry that they were being targeted by hackers. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[15]

67. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[16]

---

[15] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Dec. 10, 2025).

[16] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on Dec. 10, 2025).

68. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[17] In 2022, the largest growth in compromises occurred in the healthcare sector.[18]

69. These risks are not theoretical; high-profile breaches at healthcare providers and related service companies in recent years include: Change Healthcare, Inc. (affecting 190 million individuals in 2024); Anthem, Inc. (affecting 78.8 million individuals in 2015); American Medical Collection Agency (affecting more than twenty-six million individuals in 2019); Welltok, Inc. (affecting 14.7 million individuals in 2023); Premera Blue Cross (affecting eleven million individuals in 2015); CareSource (affecting more than three million individuals in 2023); Perry Johnson & Associates, Inc. (affecting 9.3 million people in 2023); Excellus Health Plan, Inc. (affecting ten million individuals in 2015); and many more.[19]

70. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. In 2023, there were 6,077 recorded data breach incidents, exposing seventeen billion records. The United States specifically saw a 19.8% year-over-year increase in data breaches as compared to 2022.[20]

71. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2019, roughly 3.5 million people

[17] IDENTITY THEFT RES. CTR., *2018 End-of-Year Data Breach Report*, /www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-EOY-BREACH-REPORT-KEY-FINDINGS.pdf (last visited Dec. 10, 2025).
[18] IDENTITY THEFT RES. CTR., *2022 End-of-Year Data Breach Report*, https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited Dec. 10, 2025).
[19] HIPAA J., *Healthcare Data Breach Statistics* (July 15, 2025), www.hipaajournal.com/ healthcare-data-breach-statistics.
[20] *2024 Global Threat Intelligence Report*, FLASHPOINT (Feb. 29, 2024), https://go.flashpoint.io/2024-global-threat-intelligence-report-download.

reported some form of identity theft, fraud, or other consumer complaint, compared to 5.4 million people in 2023.[21]

72. 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."[22] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that were developed to work on specific—and now obsolete—operating systems and cannot be transferred to supported operating systems."[23]

73. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2023, 5,887 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights. Those breaches have resulted in the exposure of 519,935,970 healthcare records, a number that equates to 1.5x the population of the United States.[24]

74. In fact, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights,

[21] *Facts + Statistics: Identity theft and cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Key%20Facts (last visited July 24, 2025).
[22] *The Healthcare Industry is at Risk*, SWIVELSECURE, www.swivelsecure.com/ solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks (last visited July 24, 2025).
[23] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA J. (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[24] *Healthcare Data Breach Statistics*, HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited July 24, 2025).

beating the record of 720 healthcare security breaches set the previous year."[25] In 2023 alone, about one-third of Americans were affected by health-related data breaches.[26]

75. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to medical fraud, identity theft, tax fraud, credit and bank fraud, and more.

76. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that, to restore healthcare coverage, victims were often forced to pay out-of-pocket costs for healthcare they did not receive.[27]

77. Almost 50 percent of the victims lost their healthcare coverage because of the incident; nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[28]

78. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other

[25] Steve Alder, *Security Breaches in Healthcare in 2023*, HIPAA J. (Jan. 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.
[26] Ken Alltucker, *Health Care Data Breaches Hit 1 in 3 Americans Last Year: Is Your Data Vulnerable?*, USA TODAY (Feb. 19, 2024), https://www.usatoday.com/story/news/health/2024/02/18/health-data-breaches-hit-new-record-2023/72507651007/.
[27] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.
[28] *Id*.

organization, including credit bureaus, have so much monetizable information stored in their data centers."[29]

79. As a healthcare provider, AAD knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on AAD's patients as a result of a breach. AAD failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. AAD Failed to Comply with HIPAA

80. Title II of HIPAA contains what are known as the Administrative Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that HHS create rules to streamline the standards for handling PHI similar to the types of data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

81. AAD's Data Breach resulted from a combination of insufficiencies that indicate AAD failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from AAD's Data Breach that AAD either failed to implement or inadequately implemented information security policies or procedures to protect Plaintiffs' and Class Members' Private Information.

82. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by C.F.R. § 160.103.

[29] *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGIT. HEALTH (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

83. 45 C.F.R. § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

84. 45 C.F.R. § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

85. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 C.F.R. § 164.402.

86. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 C.F.R., Subpart E, as a result of the Data Breach.

87. Based upon Defendant's Notice to Plaintiffs and Class Members, AAD reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 C.F.R., Subpart E, as a result of the Data Breach.

88. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 C.F.R., Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

89. AAD reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 C.F.R., Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

90. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 C.F.R., Subpart E as a result of the Data

Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

91. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 C.F.R., Subpart E as a result of the Data Breach.

92. AAD reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 C.F.R., Subpart E as a result of the Data Breach.

93. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 C.F.R., Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

94. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 C.F.R., Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

95. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 C.F.R. § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members, to believe that future harm (including medical identity theft) is real and imminent and to take steps necessary to mitigate that risk of future harm.

96. In addition, AAD's Data Breach could have been prevented if AAD had implemented HIPAA-mandated, industry-standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

97. AAD's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information AAD creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 C.F.R. § 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. §§ 164.502, *et seq.*

98. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414 also required AAD 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***" (emphasis added).

99. While monetary relief may cure some of Plaintiffs' and Class Members' injuries, AAD's failure to comply with HIPAA means injunctive relief is also necessary to ensure AAD's approach to information security is adequate and appropriate going forward. AAD still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of future data breaches.

E. AAD Failed to Comply with FTC Guidelines

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

101. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision

making. Indeed, the FTC has concluded (and a federal appellate court agreed) that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

102. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[30] 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 into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

104. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and

[30] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 10, 2025).

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. §§ 45, *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

105. Such FTC enforcement actions include those against businesses that fail to adequately protect customer data, like AAD here. *See, e.g.*, *In re LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 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.").

106. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like AAD of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of AAD's duty in this regard.

107. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[31]

108. As evidenced by the Data Breach, AAD failed to properly implement basic data security practices. AAD's failure to employ reasonable and appropriate measures to protect against

[31] FTC Comm'r Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

109. AAD was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. AAD Failed to Comply with Industry Standards

110. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

111. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[32]

112. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

[32] *The 18 CIS Critical Security Controls*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/cis-controls-list (last visited Dec. 10, 2025).

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

113. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[33]

[33] *Shields Up: Guidance for Organizations*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Dec. 10, 2025).

114. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

G. AAD Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

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

116. AAD breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. AAD's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect patients' Private Information;

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

d. Failing to sufficiently train its employees regarding the proper handling of its patients' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

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

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

117. AAD negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

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

119. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with AAD.

H. Plaintiffs and Class Members Are at a Significantly Increased and Substantial Risk of Fraud and Identity Theft as a Result of the Data Breach.

120. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such

as data breaches or unauthorized disclosure of data.[34] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

121. Any victim of a data breach is exposed to serious risks and injuries regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities to engage in illegal financial transactions under the victims' names.

122. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as their login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

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

[34] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, FTC (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves because they allow them to access users' other accounts.

124. Thus, even if certain information was purportedly not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

125. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

126. Cybercriminals can cross-reference two sources of Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

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

128. As a result of the Data Breach, upon information and belief, Plaintiffs and other Class Members' stolen Private Information is being misused and consolidated into such Fullz packages right now. It is undeniable that Plaintiffs' and Class Members' Private Information is

being misused and that such misuse is fairly traceable to the Data Breach.

129. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[35] But these steps do not guarantee protection from identity theft; they can only mitigate identity theft's long-lasting negative impacts.

130. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, or bank fraud.

131. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[36] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77 percent experienced financial-related problems;
- 29 percent experienced financial losses exceeding $10,000;
- 40 percent were unable to pay bills;
- 28 percent were turned down for credit or loans;
- 37 percent became indebted;
- 87 percent experienced feelings of anxiety;
- 67 percent experienced difficulty sleeping; and
- 51 percent suffered from panic or anxiety attacks.[37]

[35] *See IdentityTheft.gov,* FTC, https://www.identitytheft.gov/Steps (last visited Dec. 10, 2025).
[36] *2023 Consumer Impact Report*, IDENTITY THEFT RES. CTR. (Jan. 2024), https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf.
[37] *Id.* at pp 21–25.

132. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[38]

133. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

134. While credit card information and associated PII can sell for as little as $1–$2 on the black market, PHI can sell for as much as $363, according to the Infosec Institute.[39]

135. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing hackers to purchase and resell medical equipment or gaining access to prescriptions for illegal use or resale.

136. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, Executive Director of the World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[40]

[38] *Warning Signs of Identity Theft*, FTC, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Dec. 10, 2025).
[39] *Data Breaches: In the Healthcare Sector,* CTR. FOR INTERNET SEC., https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Dec. 10, 2025).
[40] Michael Ollove, "*The Rise of Medical Identity Theft in Healthcare*," KAISER HEALTH NEWS (Feb. 7, 2014), https://kffhealthnews.org/news/rise-of-indentity-theft/.

137. The ramifications of AAD's failure to keep its patients' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

138. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates that the Private Information compromised here has considerable market value.

139. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has 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. [41]

140. PII and PHI are such valuable commodities to identity thieves that, once the information has been compromised, criminals often trade the information on the dark web for years.

141. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future and have no choice but to vigilantly monitor their accounts for years to come.

[41] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

I. Plaintiffs' and Class Members' Damages

Plaintiff Natalia Correa's Experience and Injuries

142. Plaintiff Natalia Correa is a patient of Defendant.

143. As a condition of obtaining medical services, Plaintiff Correa was required to supply Defendant with her PII/PHI—including her name, address, phone number, Social Security number, email, date of birth, financial account information, insurance provider, and other medical information.

144. Defendant was in possession of Plaintiff Correa's PII/PHI before, during, and after the Data Breach.

145. Plaintiff Correa received a Notice from Defendant informing her that her PII/PHI was compromised as a result of the Data Breach.

146. Plaintiff Correa reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Correa would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI, if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

147. Plaintiff Correa greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Longwell is now concerned about identity theft and fraud as a result of the Data Breach.

148. Plaintiff Correa is very careful about sharing her sensitive PII/PHI. Plaintiff Correa takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Correa would not have

entrusted her PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

149. As a result of the Data Breach, Plaintiff Correa has taken reasonable efforts to mitigate the impact of the Data Breach, such as monitoring her accounts for suspicious activity.

150. The Data Breach has caused Plaintiff Correa to suffer fear, and anxiety, and stress, which has been compounded by the fact that she finds it extremely nerve-wracking to know that someone has access to her personal information.

151. Plaintiff Correa will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

153. As a direct and traceable result of the Data Breach, Plaintiff Correa suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her Bank account for suspicious activity; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (d) emotional distress because identity thieves now possess her PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Correa, and (g) other economic and non-economic harm.

Plaintiff Peyton Sulkowski's Experience and Injuries

154. Plaintiff Peyton Sulkowski is a patient of Anne Arundel Dermatology.

155. As a condition of obtaining medical services, Plaintiff Sulkowski was required to supply Defendant with her PII/PHI—including her name, address, phone number, email, date of birth, insurance provider, and other medical information.

156. Defendant was in possession of Plaintiff Sulkowski's PII/PHI before, during, and after the Data Breach.

157. Plaintiff Sulkowski received a Notice from Defendant informing her that her PII/PHI was compromised as a result of the Data Breach.

158. Plaintiff Sulkowski reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Sulkowski would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

159. Plaintiff Sulkowski greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Sulkowski is now concerned about identity theft and fraud as a result of the Data Breach.

160. Plaintiff Sulkowski is very careful about sharing her sensitive PII/PHI. Plaintiff Sulkowski takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Sulkowski would not have entrusted her PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

161. As a result of the Data Breach, Plaintiff Sulkowski has spent multiple hours researching the Data Breach and monitoring her accounts for suspicious activity. This is valuable time that Plaintiff Sulkowski spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

162. As a consequence of and following the Data Breach, Plaintiff Sulkowski has experienced unauthorized login attempts on her email account, which required her to change her password.

163. The Data Breach has caused Plaintiff Sulkowski to suffer fear, anxiety, and stress, as she is worried about its repercussions.

164. Plaintiff Sulkowski will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

166. As a direct and traceable result of the Data Breach, Plaintiff Sulkowski suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts for suspicious activity and researching the Data Breach; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (d) emotional distress because identity thieves now possess her PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen and likely published on the dark web; (f) diminution in

the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Sulkowski, and (g) other economic and non-economic harm.

Plaintiff Jennifer Longwell's Experience and Injuries

167. Plaintiff Jennifer Longwell is a patient of Defendant.

168. As a condition of obtaining medical services, Plaintiff Longwell was required to supply Defendant with her PII/PHI—including her name, address, phone number, Social Security number, email, date of birth, financial account information, medical and health insurance information.

169. Defendant was in possession of Plaintiff Longwell's PII/PHI before, during, and after the Data Breach.

170. Plaintiff Longwell received a Notice from Defendant informing her that her PII/PHI was compromised as a result of the Data Breach.

171. Plaintiff Longwell reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Longwell would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI, if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

172. Plaintiff Longwell greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Longwell is now concerned about identity theft and fraud as a result of the Data Breach.

173. Plaintiff Longwell is very careful about sharing her sensitive PII/PHI. Plaintiff Longwell takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Longwell

would not have entrusted her PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

174. As a result of the Data Breach, Plaintiff Longwell has taken reasonable efforts to mitigate the impact of the Data Breach, such as monitoring her accounts for suspicious activity.

175. The Data Breach has caused Plaintiff Longwell to suffer fear, anxiety, and stress, which has been compounded by the fact that she finds it extremely nerve-wracking to know that someone has access to her personal information.

176. Plaintiff Longwell will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

178. As a direct and traceable result of the Data Breach, Plaintiff Longwell suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her Bank account for suspicious activity; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (d) emotional distress because identity thieves now possess her PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Longwell, and (g) other economic and non-economic harm.

Plaintiff Shemika Jones' Experience and Injuries

179. Plaintiff Shemika Jones is a patient of Defendant.

180. As a condition of obtaining medical services, Plaintiff Jones was required to supply Defendant with her PII/PHI—including her name, address, phone number, Social Security number, email, date of birth, financial account information, insurance provider, and other medical information.

181. Defendant was in possession of Plaintiff Jones' PII/PHI before, during, and after the Data Breach.

182. Plaintiff Jones received a Notice from Defendant informing her that her PII/PHI was compromised as a result of the Data Breach.

183. Plaintiff Jones reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Jones would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

184. Plaintiff Jones greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Jones is now concerned about identity theft and fraud as a result of the Data Breach.

185. Plaintiff Jones is very careful about sharing her sensitive PII/PHI. Plaintiff Jones takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Jones would not have entrusted her PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

186. As a result of the Data Breach, Plaintiff Jones has spent several hours researching the Data Breach, monitoring and investigating her accounts for suspicious activity, contacting major credit bureaus to freeze her credit, and contacting banks, credit card companies, and other vendors about fraudulent and suspicious activity, as well as making other necessary mitigation efforts. This is valuable time that Plaintiff Jones spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

187. As a consequence of and following the Data Breach, Plaintiff Jones has experienced a significant uptick in spam calls, text messages, and emails to the same phone number and email provided to AAD, in addition to unauthorized charges and attempted charges affecting her financial accounts, including credit cards, debit cards, and bank accounts.

188. The Data Breach has caused Plaintiff Jones to suffer fear, anxiety, and stress, which has been compounded by the fact that she is very concerned about identity theft.

189. Plaintiff Jones will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

191. As a direct and traceable result of the Data Breach, Plaintiff Jones suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her financial accounts and credit reports for fraudulent and suspicious activity; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (d) emotional distress because identity thieves now possess her

PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Jones, and (g) other economic and non-economic harm.

Plaintiff Brice Farris's Experience and Injuries

192. Plaintiff Brice Farris is a patient of Defendant.

193. As a condition of obtaining medical services, Plaintiff Farris was required to supply Defendant with his PII/PHI—including his name, address, phone number, Social Security number, email, date of birth, financial account information, insurance provider, and other medical information.

194. Defendant was in possession of Plaintiff Farris's PII/PHI before, during, and after the Data Breach.

195. Plaintiff Farris received a Notice from Defendant informing him that his PII/PHI was compromised as a result of the Data Breach.

196. Plaintiff Farris reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Farris would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

197. Plaintiff Farris greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Farris is now concerned about identity theft as a result of the Data Breach.

198. Plaintiff Farris is very careful about sharing his sensitive PII/PHI. Plaintiff Farris takes proactive steps to ensure that his PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Farris would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

199. As a result of the Data Breach, Plaintiff Farris has spent several hours researching the Data Breach, monitoring and investigating his accounts for suspicious activity, contacting major credit bureaus to freeze his credit, and contacting banks, credit card companies, and other vendors about fraudulent and suspicious activity, as well as making other necessary mitigation efforts. This is valuable time that Plaintiff Farris spent at Defendant's direction, and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

200. As a consequence of and following the Data Breach, Plaintiff Farris has experienced a significant uptick in spam calls, text messages, and emails to the same phone number and email provided to AAD, as well as fraudulent attempted charges on his financial accounts. He also had his Social Security number appear on public websites, which he has been unable to remove from the Internet.

201. The Data Breach has caused Plaintiff Farris to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing him of the fact that his Social Security number was acquired by criminals as a result of the Data Breach.

202. Plaintiff Farris will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

204. As a direct and traceable result of the Data Breach, Plaintiff Farris suffered actual injury and damages after his PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his financial accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Farris, and (g) other economic and non-economic harm.

Plaintiff Michael Straw's Experience and Injuries

205. Plaintiff Michael Straw is a patient of Defendant.

206. As a condition of obtaining medical services, Plaintiff Straw was required to supply Defendant with his PII/PHI—including his name, address, phone number, Social Security number, email, date of birth, financial account information, insurance provider, and other medical information.

207. Defendant was in possession of Plaintiff Straw's PII/PHI before, during, and after the Data Breach.

208. Plaintiff Straw received a Notice from Defendant informing him that his PII/PHI was compromised as a result of the Data Breach.

209. Plaintiff Straw reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Straw would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

210. Plaintiff Straw greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Straw is now concerned about identity theft as a result of the Data Breach.

211. Plaintiff Straw is very careful about sharing his sensitive PII/PHI. Plaintiff Straw takes proactive steps to ensure that his PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Straw would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

212. As a result of the Data Breach, Plaintiff Straw has spent several hours researching the Data Breach, monitoring and investigating his accounts for suspicious activity, contacting major credit bureaus to freeze his credit, as well as making other necessary mitigation efforts. This is valuable time that Plaintiff Straw spent at Defendant's direction, and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

213. As a consequence of and following the Data Breach, Plaintiff Straw has experienced a significant uptick in spam calls, text messages, and emails to the same phone number and email provided to AAD.

214. The Data Breach has caused Plaintiff Straw to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing him of the fact that his PII/PHI was acquired by criminals as a result of the Data Breach.

215. Plaintiff Straw will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the data breach.

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

217. As a direct and traceable result of the Data Breach, Plaintiff Straw suffered actual injury and damages after his PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his financial accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Straw, and (g) other economic and non-economic harm.

Plaintiff Barbara Buracker's Experience and Injuries

218. Plaintiff Barbara Buracker is a patient of Defendant.

219. As a condition of obtaining medical services, Plaintiff Buracker was required to supply Defendant with her PII/PHI—including her name, address, phone number, Social Security

number, email, date of birth, financial account information, insurance provider, and other medical information.

220. Defendant was in possession of Plaintiff Buracker's PII/PHI before, during, and after the Data Breach.

221. Plaintiff Buracker received a Notice from Defendant informing her that her PII/PHI was compromised as a result of the Data Breach.

222. Plaintiff Buracker reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Buracker would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

223. Plaintiff Buracker greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Buracker is now concerned about identity theft and fraud, as a result of the Data Breach.

224. Plaintiff Buracker is very careful about sharing her sensitive PII/PHI. Plaintiff Buracker takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Buracker would not have entrusted her PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

225. As a result of the Data Breach, Plaintiff Buracker has spent several hours researching the Data Breach, investigating and monitoring her financial and bank accounts for fraudulent and suspicious activity, contacting her bank and other financial institutions regarding fraudulent charges, driving more than an hour and thirty minutes to her bank incurring gas

expenses to address these issues, and undertaking other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

226. As a consequence of and following the Data Breach, Plaintiff Buracker has experienced multiple fraudulent access attempts and charges affecting her Wells Fargo bank account, which has been hacked twice.

227. Furthermore, as a consequence of and following the Data Breach, Plaintiff Buracker had her Cash App account hacked and, despite her efforts to address and resolve the issue, she did not receive full reimbursement of the money taken from her account.

228. The Data Breach has resulted in the Plaintiff Buracker experiencing heightened fear, anxiety, and stress, further exacerbating the financial challenges stemming from her limited income, which she relies on to pay her bills.

229. Plaintiff Buracker will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

231. As a direct and traceable result of the Data Breach, Plaintiff Buracker suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her bank and other financial accounts for fraudulent activity; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (d) emotional distress because identity thieves now possess her

PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Buracker, and (g) other economic and non-economic harm.

Plaintiff Paul Gale's Experience and Injuries

232. Plaintiff Paul Gale is a patient of Defendant.

233. As a condition of obtaining medical services, Plaintiff Gale was required to supply Defendant with his PII/PHI—including his name, address, phone number, Social Security number, date of birth, financial account information, and other medical information.

234. Defendant was in possession of Plaintiff Gale's PII/PHI before, during, and after the Data Breach.

235. Plaintiff Gale received a Notice from Defendant informing him that his PII/PHI was compromised as a result of the Data Breach.

236. Plaintiff Gale reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Gale would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

237. Plaintiff Gale greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Gale is now concerned about identity theft and fraud as a result of the Data Breach.

238. Plaintiff Gale is very careful about sharing his sensitive PII/PHI. Plaintiff Gale takes proactive steps to ensure that his PII/PHI is kept safe and secure and would never knowingly

transmit unencrypted sensitive information over the internet. Thus, Plaintiff Gale would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

239. As a result of the Data Breach, Plaintiff Gale has spent several hours researching the incident, contacting his bank and credit card companies regarding fraudulent activity and suspicious information, making necessary changes to his credit and bank account information, and filing police reports, which required traveling to the police station. Plaintiff Gale has also enrolled in and is paying for a monthly credit monitoring protection service through Norton 360, in addition to taking other reasonable mitigation efforts. This is valuable time and money that Plaintiff Gale spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

240. As a consequence of and following the Data Breach, a perpetrator used an ID in Plaintiff Gale's name to fraudulently purchase a vehicle. Plaintiff Gale discovered the fraud when a letter addressed to his parents from TD Auto Finance, the financing company, arrived at his parents' address. Plaintiff Gale promptly contacted the car dealership and filed a police report. The perpetrator was subsequently arrested, and a criminal case associated with the matter is pending in Yonkers, New York. Plaintiff Gale, on his own, has had to jump through numerous hoops with the auto company to get the incident cleared from his credit. Despite these efforts, Plaintiff Gale's credit was still negatively impacted.

241. Furthermore, since the Data Breach, Plaintiff Gale has identified multiple unrecognized hard inquiries on his credit report from unknown individuals applying for credit through Nissan Motor Acceptance Company, Sam Tanner Consumer USA, Capital One Auto Finance, Ally Financial, and a Walmart AT&T Plan, all of which were denied or resolved. Plaintiff

Gale also experienced multiple unauthorized charges to his Green Dot Corporation account, including five unrecognized charges to platforms such as Google and YouTube, which remain unresolved.

242. The incidents mentioned above, triggered by the Data Breach and Defendant's actions, have led Plaintiff Gale to purchase cameras for both his house and his parents' house due to fears of their addresses being compromised by cybercriminals. The Data Breach has also caused Plaintiff Gale to suffer from additional anxiety and stress, which has led to disruptions in both his marital and work life.

243. Plaintiff Gale will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

245. As a direct and traceable result of the Data Breach, Plaintiff Gale suffered actual injury and damages after his PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity, and addressing a criminal incident involving a fraudulent car purchase made with his ID ; (b) loss of privacy due to his PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of his PII/PHI, a form of

intangible property that Defendant obtained from Plaintiff Gale, and (g) other economic and non-economic harm.

Plaintiff Earl Beville, Jr. Experience and Injuries

246. Plaintiff Earl Beville, Jr. is a patient of Defendant.

247. As a condition of obtaining medical services, Plaintiff Beville's was required to supply Defendant with his PII/PHI—including his name, address, phone number, Social Security number, date of birth, financial account information, and other medical information.

248. Defendant was in possession of Plaintiff Beville's PII/PHI before, during, and after the Data Breach.

249. Plaintiff Beville received a Notice from Defendant informing him that his PII/PHI was compromised as a result of the Data Breach.

250. Plaintiff Beville reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Beville would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

251. Plaintiff Beville greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Beville is now concerned about identity theft and fraud, as a result of the Data Breach.

252. Plaintiff Beville is very careful about sharing his sensitive PII/PHI. Plaintiff Beville has taken proactive steps, such as enrolling in a credit monitoring service, to ensure that his PII/PHI is kept safe and secure. He would never knowingly transmit unencrypted sensitive information

over the internet. Thus, Plaintiff Beville would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

253. As a consequence of and following the Data Breach, Plaintiff Beville has experienced a significant uptick in spam calls, text messages, and emails to the same phone number and email provided to AAD.

254. Furthermore, Plaintiff Beville has been notified that his Social Security Number, financial information, Medical Records, and other PHI/PII have been compromised as a result of the Data Breach. As a consequence of and following the Data Breach, Plaintiff Beville has also been notified that his PII/PHI has been found on the dark web. Subsequently, Plaintiff Beville has been forced to look for a new medical provider because he no longer trusts Defendant because of Defendant's inability to safeguard his PII/PHI from cybercriminals.

255. The Data Breach has caused Plaintiff Beville to suffer constant fear, anxiety, and stress, especially because his PHI has been implicated due to Defendant's actions.

256. Plaintiff Beville will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

258. As a direct and traceable result of the Data Breach, Plaintiff Beville suffered actual injury and damages after his PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) loss of privacy due to his PII/PHI being accessed and stolen by cybercriminals; (b) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent

and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen and published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Beville, and (g) other economic and non-economic harm.

Plaintiff Steven Boehm's Experience and Injuries

259. Plaintiff Steven Boehm is a patient of Defendant.

260. As a condition of obtaining medical services, Plaintiff Boehm was required to supply Defendant with his PII/PHI—including his name, address, phone number, household size, Social Security number, email, date of birth, financial account information, insurance provider, and other medical information.

261. Defendant was in possession of Plaintiff Boehm's PII/PHI before, during, and after the Data Breach.

262. Plaintiff Boehm received a Notice from Defendant informing him that his PII/PHI was compromised as a result of the Data Breach.

263. Plaintiff Boehm reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Boehm would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

264. Plaintiff Boehm greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Boehm is now concerned about identity theft and fraud, as a result of the Data Breach.

265. Plaintiff Boehm is very careful about sharing his sensitive PII/PHI. Plaintiff Boehm has taken proactive steps, such as enrolling in a credit monitoring service, to ensure that his PII/PHI is kept safe and secure. He would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Boehm would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

266. As a result of the Data Breach, Plaintiff Boehm has spent multiple hours researching the Data Breach, monitoring his credit report, and investigating his financial accounts for fraudulent and suspicious activity. This is valuable time that Plaintiff Boehm spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

267. As a consequence of, and following, the Data Breach, Plaintiff Boehm received a fraud alert for attempted use of his debit card this past summer, which, on information and belief, was likely the same debit card Plaintiff Boehm had used at Anne Arundel previously for his medical visits. Plaintiff Boehm was forced to have the debit card cancelled and reissued due to the incident.

268. As a consequence of, and following the Data Breach, Plaintiff Boehm has experienced a significant uptick in spam calls, text messages, and emails to the same phone number and email provided to AAD. Plaintiff Boehm has also received notice from Norton that his PII/PHI has been found on the dark web. Plaintiff Boehm subsequently had to pay Norton to get his PII/PHI removed.

269. The incidents mentioned above, triggered by the Data Breach, have caused Plaintiff Boehm to suffer anxiety and stress.

270. Plaintiff Boehm will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

272. As a direct and traceable result of the Data Breach, Plaintiff Boehm suffered actual injury and damages after his PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his financial accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Boehm, and (g) other economic and non-economic harm.

Plaintiff Paul Madigan's Experience and Injuries

273. Plaintiff Paul Madigan is a patient of Defendant.

274. As a condition of obtaining medical services, Plaintiff Madigan was required to supply Defendant with his PII/PHI—including his address, phone number, household size, email, date of birth, insurance provider, and other medical information.

275. Defendant was in possession of Plaintiff Madigan's PII/PHI before, during, and after the Data Breach.

276. Plaintiff Madigan received a Notice from Defendant informing him that his PII/PHI was compromised as a result of the Data Breach.

277. Plaintiff Madigan reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Madigan would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

278. Plaintiff Madigan greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Madigan is now concerned about identity theft and fraud, as a result of the Data Breach.

279. Plaintiff Madigan is very careful about sharing his sensitive PII/PHI. Plaintiff Madigan has taken proactive steps, such as enrolling in a credit monitoring service, to ensure that his PII/PHI is kept safe and secure. He would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Madigan would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

280. As a result of the Data Breach, Plaintiff Madigan has spent several hours researching the Data Breach, monitoring his accounts for suspicious activity. This is valuable time that Plaintiff Madigan spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

281. Defendant offered Plaintiff Madigan free credit monitoring. However, when Plaintiff Madigan attempted to use the code provided by Defendant for free monitoring, it did not work.

282. As a consequence of and following the Data Breach, Plaintiff Madigan has experienced a significant uptick in spam calls, and text messages to the same phone number and email supplied to AAD.

283. As a consequence of the Data Breach, Plaintiff Madigan was notified three months ago that his PII/PHI had been found on the dark web.

284. The Data Breach has caused Plaintiff Madigan to suffer from anxiety and stress over the fear of potential damage to his credit.

285. Plaintiff Madigan will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

287. As a direct and traceable result of the Data Breach, Plaintiff Madigan suffered actual injury and damages after his PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts for fraudulent activity; (b) loss of privacy due to his PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen and published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Madigan, and (g) other economic and non-economic harm.

Plaintiff Heidi Shell's Experience and Injuries

288. Plaintiff Heidi Shell is a patient of Defendant.

289. As a condition of obtaining medical services, Plaintiff Shell was required to supply Defendant with her PII/PHI—including her name, address, email, phone number, household information, date of birth, insurance provider, and other medical information.

290. Defendant was in possession of Plaintiff Shell's PII/PHI before, during, and after the Data Breach.

291. Plaintiff Shell received a Notice from Defendant informing her that her PII/PHI was compromised as a result of the Data Breach.

292. Plaintiff Shell reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Shell would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

293. Plaintiff Shell greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI.

294. Plaintiff Shell is very careful about sharing her sensitive PII/PHI. Plaintiff Shell has taken proactive steps, such as enrolling in a credit monitoring service, to ensure that her PII/PHI is kept safe and secure. She would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Shell would not have entrusted her PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

295. As a result of the Data Breach, Plaintiff Shell has spent multiple hours researching the Data Breach, monitoring/investigating her financial accounts, and contacting her bank and

credit card companies about potential fraudulent and suspicious activity. This is valuable time that Plaintiff Shell spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

296. Plaintiff Shell will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

298. As a direct and traceable result of the Data Breach, Plaintiff Shell suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts for fraudulent activity; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (d) emotional distress because identity thieves now possess her PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Shell, and (g) other economic and non-economic harm.

Plaintiff Troy Botteon's Experience and Injuries

299. Plaintiff Troy Botteon is a patient of Defendant.

300. As a condition of obtaining medical services, Plaintiff Botteon was required to supply Defendant with his PII/PHI—including his name, address, phone number, email, Social Security number, date of birth, insurance provider, and other medical information.

301. Defendant was in possession of Plaintiff Botteon's PII/PHI before, during, and after the Data Breach.

302. Plaintiff Botteon received a Notice from Defendant informing him that his PII/PHI was compromised as a result of the Data Breach.

303. Plaintiff Botteon reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Botteon would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

304. Plaintiff Botteon greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Botteon is now concerned about identity theft and fraud, as a result of the Data Breach.

305. Plaintiff Botteon is very careful about sharing his sensitive PII/PHI. Plaintiff Botteon has taken proactive steps, such as enrolling in a credit monitoring service, to ensure that his PII/PHI is kept safe and secure. He would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Botteon would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

306. As a result of the Data Breach, Plaintiff Botteon has spent several hours researching the Data Breach, monitoring his accounts for suspicious/fraudulent activity, contacting CashApp, Robinhood, and other financial institutions, and addressing the resulting card and account number changes. This is valuable time that Plaintiff Botteon spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

307. As a consequence of and following the Data Breach, Plaintiff Botteon was notified of multiple fraudulent attempts to access his private online accounts. He received repeated notifications of fraudulent attempts to access his Cash App account, a financial services platform. An unauthorized individual also successfully accessed his Microsoft account, and Plaintiff Botteon later discovered multiple fraudulent addresses and names on his Credit Karma account.

308. As a consequence of and following the Data Breach, Plaintiff Botteon has experienced a significant uptick in spam calls, text messages, and emails to the same phone number and email provided to AAD.

309. The Data Breach has caused Plaintiff Botteon to suffer from anxiety and stress, stemming from the fear of future fraud. To ease those concerns, Plaintiff Botteon avoids keeping funds in his checking account. Instead, before each purchase, he transfers just enough money from his brokerage account and then pays with his credit card. This process is time-consuming and inconvenient, but Plaintiff Botteon has found it necessary to manage the constant anxiety and stress stemming from the Data Breach.

310. Plaintiff Botteon will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

312. As a direct and traceable result of the Data Breach, Plaintiff Botteon suffered actual injury and damages after his PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts for fraudulent activity; (b) loss of privacy due to his PII/PHI being accessed and stolen by cybercriminals; (c)

loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Botteon, and (g) other economic and non-economic harm.

Plaintiff Richard Bernard's Experience and Injuries

313. Plaintiff Richard Bernard is a patient of Defendant.

314. As a condition of obtaining medical services, Plaintiff Bernard was required to supply Defendant with his PII/PHI—including his name, address, phone number, household size, Social Security number, email, date of birth, financial account information, insurance provider, and other medical information.

315. Defendant was in possession of Plaintiff Bernard's PII/PHI before, during, and after the Data Breach.

316. Plaintiff Bernard received Notice from Defendant that his PII/PHI was compromised as a result of the Data Breach.

317. Plaintiff Bernard reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Bernard would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

318. Plaintiff Bernard greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Bernard is now concerned about identity theft and fraud, because of the Data Breach.

319. As a Systems Engineer for the Department of Defense, Plaintiff Bernard's work is directly tied to data security. Accordingly, Plaintiff Bernard is highly aware of the importance of protecting sensitive information, is very careful when sharing his PII/PHI, and takes proactive steps such as enrolling in credit monitoring services to keep it safe and secure. He would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Bernard would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

320. As a result of the Data Breach, Plaintiff Bernard has spent several hours researching the Data Breach, monitoring and investigating his accounts for fraudulent/suspicious activity, and undertaking other necessary mitigation efforts. This is valuable time that Plaintiff Bernard spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

321. As a consequence of and following the Data Breach, Plaintiff Bernard has received an alert that his name, email, address, and phone number were compromised.

322. As a result of the Data Breach, Plaintiff Bernard has endured anxiety stemming from the fear of the unknown happening with respect to his PII/PHI.

323. Plaintiff Bernard will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

325. As a direct and traceable result of the Data Breach, Plaintiff Bernard suffered actual injury and damages after his PII/PHI was compromised in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts reports for fraudulent activity; (b) loss of privacy due to his PII/PHI being accessed and by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen and likely published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Bernard, and (g) other economic and non-economic harm.

Plaintiff Jason Tyson's Experience and Injuries

326. Plaintiff Jason Tyson is a patient of Defendant.

327. As a condition of obtaining medical services, Plaintiff Tyson was required to supply Defendant with his PII/PHI—including his name, address, phone number, Social Security number, email, date of birth, and other medical information.

328. Defendant was in possession of Plaintiff Tyson's PII/PHI before, during, and after the Data Breach.

329. Plaintiff Tyson received Notice from Defendant that his PII/PHI was compromised as a result of the Data Breach.

330. Plaintiff Tyson reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Tyson would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

331. Plaintiff Tyson greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Tyson is now concerned about identity theft and fraud, as a result of the Data Breach.

332. Plaintiff Tyson is very careful about sharing his sensitive PII/PHI. Plaintiff Tyson has taken proactive steps, such as enrolling in multiple credit monitoring services, to ensure that his PII/PHI is kept safe and secure. He would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Tyson would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

333. As a result of the Data Breach, Plaintiff Tyson has spent multiple hours researching the Data Breach, monitoring his accounts for suspicious activity, and changing his passwords. This is valuable time that Plaintiff Tyson spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

334. As a consequence of and following the Data Breach, Plaintiff Tyson has experienced a significant uptick in spam text messages to the same phone number and email provided to AAD. Specifically, Plaintiff Tyson has received several spam messages claiming fraudulent activity has been detected in his bank account and other financial accounts.

335. The Data Breach has caused Plaintiff Tyson to suffer fear, anxiety, and stress stemming from the advent of his PII/PHI being leaked and exposed.

336. Plaintiff Tyson will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

338. As a direct and traceable result of the Data Breach, Plaintiff Tyson suffered actual injury and damages after his PII/PHI was compromised in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts for fraudulent activity; (b) loss of privacy due to PII/PHI being accessed and compromised by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her his/PHI has been compromised and likely published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Tyson, and (g) other economic and non-economic harm.

Plaintiff Crystal Hall's Experience and Injuries

339. Plaintiff Crystal Hall is a patient of Defendant.

340. As a condition of obtaining medical services, Plaintiff Hall was required to supply Defendant with her PII/PHI—including her name, address, email, phone number, Social Security number, date of birth, financial account information, insurance provider, and other medical information.

341. Defendant was in possession of Plaintiff Hall's PII/PHI before, during, and after the Data Breach.

342. Plaintiff Hall received a Notice from Defendant informing her that her PII/PHI was compromised as a result of the Data Breach.

343. Plaintiff Hall reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Hall would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

344. Plaintiff Hall greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Hall is now concerned about identity theft and fraud, as a result of the Data Breach.

345. Plaintiff Hall is very careful about sharing her sensitive PII/PHI. Plaintiff Hall takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Hall would not have entrusted her PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

346. As a result of the data breach, Plaintiff Hall has devoted several hours to researching the incident and has been monitoring all her accounts for suspicious activity for an hour every day. This is valuable time that Plaintiff Hall spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

347. As a consequence of and following the Data Breach, Plaintiff Hall received a notice that her date of birth, medical record number, health history, and insurance information had been compromised.

348. The Data Breach has caused Plaintiff Hall to suffer fear, anxiety, and stress, which has been compounded by the worry that cybercriminals will misuse Plaintiff Hall's PII/PHI to steal her money and or identity.

349. Plaintiff Hall will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

351. As a direct and traceable result of the Data Breach, Plaintiff Hall suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts for fraudulent activity; (b) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (c) emotional distress because identity thieves now possess her PII/PHI; (d) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen and likely published on the dark web; (e) diminution in the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Hall, and (f) other economic and non-economic harm.

Plaintiff Terri Wilson's Experience and Injuries

352. Plaintiff Terri Wilson is a patient of Defendant.

353. As a condition of obtaining medical services, Plaintiff Wilson was required to supply Defendant with her PII/PHI—including her name, address, phone number, Social Security number, email, date of birth, insurance provider, and other medical information.

354. Defendant was in possession of Plaintiff Wilson's PII/PHI before, during, and after the Data Breach.

355. Plaintiff Wilson received Notice from Defendant that her PII/PHI was compromised as a result of the Data Breach.

356. Plaintiff Wilson reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Wilson would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

357. Plaintiff Wilson greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Wilson is now concerned about identity theft and fraud, as a result of the Data Breach.

358. As a Software Implementation and Accounting Consultant, Plaintiff Wilson represents numerous business clients and thus has to safeguard their confidential and/or proprietary information, including, but not limited to, client Social Security Numbers and bank records. Accordingly, Plaintiff Wilson is highly aware of the importance of protecting her own and others' sensitive information. Plaintiff Wilson takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Wilson would not have entrusted her PII/PHI to Defendant if Defendant had been transparent about its negligent data security practices.

359. As a result of the Data Breach, Plaintiff Wilson has spent multiple hours researching the Data Breach, monitoring and investigating her accounts for fraudulent/suspicious activity, and undertaking other necessary mitigation efforts. This is valuable time that Plaintiff

Wilson spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

360. As a consequence of and following the Data Breach, Plaintiff Wilson has experienced a substantial increase in spam text messages to the same phone number and email provided to AAD. These messages have caused daily annoyance for Plaintiff Wilson and have consistently interrupted her work and personal time by distracting her into checking whether the text is from a client or a friend.

361. As a consequence of and following the Data Breach, Plaintiff Wilson received a notice that her PII/PHI, including but not limited to her financial information, date of birth, and medical record number, may have been compromised.

362. Plaintiff Wilson will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

364. As a direct and traceable result of the Data Breach, Plaintiff Wilson suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts for fraudulent activity; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen; (f) diminution in the value of her PII/PHI, a form of intangible

property that Defendant obtained from Plaintiff Wilson; and (g) other economic and non-economic harm.

Plaintiff Raven Martin's Experience and Injuries

365. Plaintiff Raven Martin is a patient of Defendant.

366. As a condition of obtaining medical services, Plaintiff Martin was required to supply Defendant with his PII/PHI—including his name, address, phone number, Social Security number, email, date of birth, and other medical information.

367. Defendant was in possession of Plaintiff Martin's PII/PHI before, during, and after the Data Breach.

368. Plaintiff Martin received Notice from Defendant that his PII/PHI was compromised as a result of the Data Breach.

369. Plaintiff Martin reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Martin would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

370. Plaintiff Martin greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Martin is now concerned about identity theft and fraud, as a result of the Data Breach.

371. Plaintiff Martin is very careful about sharing his sensitive PII/PHI. Plaintiff Martin has taken proactive steps, such as enrolling in multiple credit monitoring services, to ensure that his PII/PHI is kept safe and secure. He would never knowingly transmit unencrypted sensitive

information over the internet. Thus, Plaintiff Martin would not have entrusted his PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

372. As a result of the Data Breach, Plaintiff Martin has spent multiple hours researching the Data Breach, monitoring his accounts for suspicious activity and changing his passwords. This is valuable time that Plaintiff Martin spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

373. As a consequence of and following the Data Breach, Plaintiff Martin has experienced a significant uptick in spam text messages to the same phone number and email provided to AAD.

374. The Data Breach has caused Plaintiff Martin to suffer fear, anxiety, and stress stemming from the advent of his PII/PHI being leaked and exposed.

375. Plaintiff Martin will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

377. As a direct and traceable result of the Data Breach, Plaintiff Martin suffered actual injury and damages after his PII/PHI was compromised in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts for fraudulent activity; (b) loss of privacy due to PII/PHI being accessed and compromised by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (d) emotional distress because identity thieves now possess his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her his/PHI has been

compromised and likely published on the dark web; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Martin; and (g) other economic and non-economic harm.

Plaintiff Jacqueline Smith's Experience and Injuries

378. Plaintiff Jacqueline Smith is a patient of Defendant.

379. As a condition of obtaining medical services, Plaintiff Smith was required to supply Defendant with her PII/PHI—including her name, address, phone number, Social Security number, email, date of birth, financial account information, medical and health insurance information.

380. Defendant was in possession of Plaintiff Smith's PII/PHI before, during, and after the Data Breach.

381. Plaintiff Smith received a Notice from Defendant informing her that her PII/PHI was compromised as a result of the Data Breach.

382. Plaintiff Smith reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Smith would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI, if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

383. Plaintiff Smith greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Smith is now concerned about identity theft and fraud as a result of the Data Breach.

384. Plaintiff Smith is very careful about sharing her sensitive PII/PHI. Plaintiff Smith takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Smith would not have

entrusted her PII/PHI to Defendant if Defendant was transparent about its negligent data security practices.

385. As a result of the Data Breach, Plaintiff Smith has taken reasonable efforts to mitigate the impact of the Data Breach, such as monitoring her accounts for suspicious activity.

386. As a consequence of and following the Data Breach, in July 2025, an unidentified individual attempted to open a Chase Freedom account in Plaintiff Smith's name. Plaintiff Smith also experienced a notable increase in the number of spam calls, messages, and emails after the Breach.

387. The Data Breach has caused Plaintiff Smith to suffer fear, anxiety, and stress, which has been compounded by the fact that she finds it extremely nerve-wracking to know that someone has access to her personal information.

388. Plaintiff Smith will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

390. As a direct and traceable result of the Data Breach, Plaintiff Smith suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her Bank account for suspicious activity; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (d) emotional distress because identity thieves now possess her PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been

stolen and likely published on the dark web; (f) diminution in the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Smith, and (g) other economic and non-economic harm.

Plaintiff Alunda Mitchell, on behalf of J.D., a minor.

391. Plaintiff was a patient of Defendant.

392. In order to receive services from Defendant, Plaintiff provided Defendant with her minor child's PII/PHI, including her name, date of birth, Social Security number, email address, physical address, phone number, financial account information, and medical insurance information.

393. Defendant was in possession of Plaintiff's minor child's PII/PHI before, during, and after the Data Breach.

394. Plaintiff received Notice from Defendant that her minor child's PII/PHI was compromised as a result of the Data Breach.

395. As a result of the Data Breach, Plaintiff's minor child's PII/PHI has been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's minor child's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff's minor child will have to worry about when and how her sensitive information may be shared or used to her detriment.

396. As a result of the Data Breach, Plaintiff spent hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice, self-monitoring her accounts, reviewing credit reports, and mitigating fraud and identity theft. This time has been lost forever and cannot be recaptured.

397. Additionally, Plaintiff is very careful about not sharing her sensitive PII/PHI. He has never knowingly transmitted unencrypted sensitive PII/PHI over the internet or any other unsecured source.

398. Plaintiff stores any documents containing her sensitive PII/PHI in safe and secure locations or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for his various online accounts.

399. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of her privacy.

400. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

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

Plaintiff Diana Wilson's Experience and Injuries

402. Plaintiff Diana Wilson is a patient of Defendant.

403. As a condition of obtaining medical services, Plaintiff Wilson was required to supply Defendant with her PII/PHI—including her name, address, phone number, Social Security number, email, date of birth, insurance provider, and other medical information.

404. Defendant was in possession of Plaintiff Wilson's PII/PHI before, during, and after the Data Breach.

405. Plaintiff Wilson received Notice from Defendant that her PII/PHI was compromised as a result of the Data Breach.

406. Plaintiff Wilson reasonably understood and expected that Defendant would safeguard her PII/PHI and timely and adequately notify her in the event of a data breach. Plaintiff Wilson would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII/PHI if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

407. Plaintiff Wilson greatly values the privacy of her PII/PHI and takes reasonable steps to maintain the confidentiality of her PII/PHI. Plaintiff Wilson is now concerned about identity theft and fraud as a result of the Data Breach.

408. Plaintiff Wilson takes proactive steps to ensure that her PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Wilson would not have entrusted her PII/PHI to Defendant if Defendant had been transparent about its negligent data security practices.

409. As a result of the Data Breach, Plaintiff Wilson has spent multiple hours researching the Data Breach, monitoring and investigating her accounts for fraudulent/suspicious activity, and undertaking other necessary mitigation efforts. This is valuable time that Plaintiff Wilson spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

410. Furthermore, Plaintiff Wilson received a notice that her PII/PHI, including but not limited to her date of birth, medical information, and other sensitive information was compromised as a result of the Data Breach.

411. Plaintiff Wilson will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

413. As a direct and traceable result of the Data Breach, Plaintiff Wilson suffered actual injury and damages after her PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts for fraudulent activity; (b) loss of privacy due to her PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII/PHI has been stolen; (f) diminution in the value of her PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Wilson; and (g) other economic and non-economic harm.

Plaintiff George Tyler's Experience and Injuries

414. Plaintiff George Tyler was a patient of Defendant.

415. As a condition of obtaining medical services, Plaintiff Tyler was required to supply Defendant with his PII/PHI—including his name, address, phone number, Social Security number, email, date of birth, insurance provider, and other medical information.

416. Defendant was in possession of Plaintiff Tyler's PII/PHI before, during, and after the Data Breach.

417. On July 12, 2025, Plaintiff Tyler received email notice from Defendant that his PII/PHI was compromised as a result of the Data Breach.

418. Furthermore, Plaintiff Tyler received a notice that his PII/PHI, including but not limited to his "date of birth, patient ID, medical record number, health history, financial information, insurance information, and appointment history" was compromised as a result of the Data Breach.

419. Plaintiff Tyler reasonably understood and expected that Defendant would safeguard his PII/PHI and timely and adequately notify him in the event of a data breach. Plaintiff Tyler would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII/PHI if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

420. Plaintiff Tyler greatly values the privacy of his PII/PHI and takes reasonable steps to maintain the confidentiality of his PII/PHI. Plaintiff Tyler is now concerned about identity theft and fraud as a result of the Data Breach.

421. Plaintiff Tyler takes proactive steps to ensure that his PII/PHI is kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Tyler would not have entrusted his PII/PHI to Defendant if Defendant had been transparent about its negligent data security practices.

422. As a result of the Data Breach, Plaintiff Tyler has spent time researching the Data Breach, monitoring and investigating his accounts for fraudulent/suspicious activity, and undertaking other necessary mitigation efforts. This is valuable time that Plaintiff Tyler spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

423. Plaintiff Tyler will continue to face a present and ongoing increased risk of identity theft and fraud for years to come due to the harm caused by the Data Breach.

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

425. As a direct and traceable result of the Data Breach, Plaintiff Tyler suffered actual injury in the form of difficulties accessing his personal online accounts due to unusual activity flagged as suspicious, involving the same email address that had been disclosed without authorization in the Data Breach.

426. As a direct and traceable result of the Data Breach, Plaintiff Tyler suffered actual injury and damages after his PII/PHI was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts for fraudulent activity; (b) loss of privacy due to his PII/PHI being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his PII/PHI; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII/PHI has been stolen; (f) diminution in the value of his PII/PHI, a form of intangible property that Defendant obtained from Plaintiff Tyler; and (g) other economic and non-economic harm.

427. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

428. Plaintiffs and Class Members entrusted their Private Information to Defendant to receive Defendant's services.

429. Plaintiffs' and Class Members' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which resulted from Defendant's inadequate data security practices.

430. As a direct and proximate result of AAD's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names.

431. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have also been forced to devote time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

432. 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.

433. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out targeted schemes against Plaintiffs and Class Members.

434. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted, fraudulent schemes against Plaintiffs and Class Members.

435. Plaintiffs and Class Members also lost the benefit of the bargain they made with AAD. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid

to AAD was intended to be used by AAD to fund adequate security of AAD's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

436. Additionally, 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. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[42] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[43]

437. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

438. Finally, Plaintiffs and Class Members have suffered or will suffer injury as a direct and proximate result of the Data Breach 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.

---

[42] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM REC., https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/ (last visited Dec. 10, 2025).

[43] *Frequently Asked Questions*, NIELSEN COMPUT. & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Dec. 10, 2025).

439. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of AAD, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

440. As a direct and proximate result of AAD's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

441. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

442. Specifically, Plaintiffs propose the following Nationwide Class and Maryland Subclass definitions (collectively, the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Maryland Subclass**
>
> All residents of the state of Maryland whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

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

444. Plaintiffs reserve the right to modify or amend the definition of the proposed Nationwide Class and/or Maryland Subclass, as well as add additional subclasses, if necessary, before the Court determines whether certification is appropriate.

445. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

446. ***Numerosity.*** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members have yet to be confirmed by Defendant, the most recent data that is publicly available suggests the Class consists of at least 1,905,000 current and former patients of AAD.[44] The identities of Class Members are ascertainable through AAD's records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether AAD engaged in the conduct alleged herein;

b. Whether AAD's conduct violated the FTCA and HIPAA;

c. When AAD learned of the Data Breach;

d. Whether AAD's response to the Data Breach was adequate;

e. Whether AAD unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

[44] *See Breach Portal*, U.S. DEP'T OF HEALTH & HUM. SERVS. OFF., for C.R., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Sept. 4, 2025).

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

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

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

i. Whether AAD owed a duty to Class Members to safeguard their Private Information;

j. Whether AAD breached its duty to Class Members to safeguard their Private Information;

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

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

m. Whether AAD breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

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

o. What damages Plaintiffs and Class Members suffered as a result of AAD's misconduct;

p. Whether AAD's conduct was negligent;

q. Whether AAD's conduct was negligent *per se*;

r. Whether AAD was unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

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

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

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

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

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

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

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

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

454. Plaintiffs restate and reallege all factual allegations stated above as if fully set forth herein.

455. AAD knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

456. AAD's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

457. AAD knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. AAD was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

458. AAD owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. AAD's duties included, but were not limited to, the following:

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

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

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

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

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

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

459. AAD's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

460. AAD's duty also arose because Defendant was bound by industry standards to protect its patients' confidential Private Information.

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

462. AAD, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within AAD's possession.

463. AAD, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

464. AAD, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

465. AAD breached its duties, and thus was 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. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

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

e. Failing to comply with the FTCA;

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

g. 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.

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

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

468. AAD's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

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

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

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

472. AAD also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

473. As a direct and proximate result of AAD's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

474. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

475. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

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

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

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

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

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

480. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

481. AAD breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

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

483. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures

to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of AAD's duty in this regard.

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

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

486. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and AAD's failure to comply with both constitutes negligence *per se*.

487. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to AAD's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

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

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

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

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

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

492. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to AAD in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

493. AAD's Notice of Privacy Practices memorialized the rights and obligations of AAD and its patients. This document was provided to Plaintiffs and Class Members in a way it became part of the agreement for services.

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

495. Plaintiffs and Class Members fully performed their obligations under their contracts with AAD.

496. But AAD did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information and therefore breached its contracts with Plaintiffs and Class Members.

497. AAD allowed third parties to access, copy, and exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, AAD breached the Privacy Policy with Plaintiffs and Class Members.

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

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

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

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

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

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

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

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

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

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

507. AAD accepted payment and/or possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

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

509. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor

authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

510. Plaintiffs and Class Members would not have entrusted their Private Information to AAD in the absence of such an implied contract.

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

512. As a provider of healthcare, AAD recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

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

514. Additionally, AAD breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

515. AAD also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1).

516. AAD further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

517. AAD further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii).

518. AAD further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2).

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

520. AAD further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 C.F.R. § 164.306(a)(94).

521. AAD further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. §§ 164.502, *et seq*.

522. AAD further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical

administrative safeguards to reasonably safeguard protected health information, in violation of 45 C.F.R. § 164.530(c).

523. AAD further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

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

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

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

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

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

528. Plaintiffs and Class Members conferred a benefit on AAD by turning over their Private Information to Defendant and by paying for products and/or services that should have included cybersecurity protection sufficient to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

529. Upon information and belief, AAD funds its data security measures entirely from its general revenue, including from payments made to it by or on behalf of Plaintiffs and Class Members.

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

531. AAD has retained the benefits of its unlawful conduct, including the amounts of payment received from or on behalf of Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

532. AAD knew that Plaintiffs and Class Members conferred these benefits upon it, which AAD accepted. AAD profited from these transactions and used Plaintiffs' and Class Members' Private Information for business purposes, while failing to use such benefits to implement adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

533. Had Plaintiffs and Class Members known that AAD had not adequately secured their Private Information, they would not have agreed to provide such Private Information to AAD and would have selected a different healthcare provider.

534. Due to AAD's conduct alleged herein, it would be unjust and inequitable under the circumstances to permit AAD to retain the benefit of its wrongful conduct.

535. As a direct and proximate result of AAD's conduct, Plaintiffs and Class Members have suffered and/or are at a continued, imminent risk of suffering, injuries in fact that include but are not limited to: (i) the actual misuse of their Private Information; (ii) ongoing loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private

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

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

537. Because Plaintiffs and Class Members may not have an adequate remedy at law against AAD, they plead this claim for unjust enrichment in addition to or in the alternative to other claims pleaded herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

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

539. In light of the special relationship between AAD and its patients, whereby AAD became a guardian of Plaintiffs' and Class Members' Private Information (including highly

sensitive, confidential, personal, and other PHI), AAD was a fiduciary and thus had fiduciary duties to act primarily for the benefit of its patients, including Plaintiffs and Class Members. These duties included: (1) safeguarding Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of where AAD's patients' Private Information was and is stored.

540. AAD had a fiduciary duty to act for the benefit of Plaintiffs and the Class on matters within the scope of its provider–patient relationships, particularly keeping their Private Information secure.

541. AAD breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected and notify them within a reasonable and practicable period.

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

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

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

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

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

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

548. AAD breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3).

549. AAD breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure that its workforce complied with HIPAA security-standard rules, in violation of 45 C.F.R. § 164.306(a)(94).

550. AAD breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that was, is, and remains accessible to unauthorized persons, in violation of 45 C.F.R. §§ 164.502, *et seq.*

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

COUNT VII
INVASION OF PRIVACY/INTRUSION UPON SECLUSION
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

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

553. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties by applicable laws set forth herein, including but not limited to state and federal privacy and consumer protection statutes and Maryland common law.

554. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

555. Defendant violated Plaintiffs' and the Class Members' right to privacy by failing to implement adequate data security measures, failing to resolve vulnerabilities and deficiencies, and abdicating its responsibility to reasonably protect data it required Plaintiffs and the Class to provide and store on its own servers.

556. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Private Information is highly offensive to a reasonable person. It constitutes an invasion of privacy both by disclosure of nonpublic facts and by intrusion upon seclusion.

557. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' Private Information constitutes an intentional interference of a kind that would be highly offensive to a reasonable person with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns.

558. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

559. Defendant knowingly failed to notify Plaintiffs and Class Members in a timely manner about the Data Breach.

560. Defendant had notice, as described herein, of its privacy violations and knew that its inadequate cybersecurity practices would injure Plaintiffs and the Class.

561. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' Private Information was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

562. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members since their Private Information is still maintained by Defendant and subject to its still-inadequate cybersecurity system and policies.

563. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their Private Information. A judgment for monetary damages will not remedy Defendant's inability to safeguard Plaintiffs' and Class Members' Private Information, which remains in its possession.

564. Plaintiffs and Class Members seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of their Private Information.

565. Plaintiffs and Class Members seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant; the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest; and costs.

COUNT VIII
VIOLATIONS OF THE MARYLAND CONSUMER PROTECTION ACT AND MARYLAND PERSONAL INFORMATION PROTECTION ACT (ON BEHALF OF "MARYLAND PLAINTIFFS" AND THE MARYLAND SUBLASS)

566. Plaintiffs Jones, Gale, Boehm, Madigan, Shell, Botteon, Martin, D. Wilson, and Tyler (the "Maryland Plaintiffs") restate and reallege the factual allegations in the preceding paragraphs as if fully set forth herein and bring this claim on behalf of themselves and the Maryland Subclass pursuant to the Maryland Consumer Protection Act, §§ 13-101, *et seq*. and the Maryland Personal Information Protection Act, §§ 14-3501, *et seq*.

567. The purpose of the Maryland Consumer Protection Act is "to set certain minimum statewide standards for the protection of consumers across the State [of] [Maryland]." The Maryland Personal Information Protection Act was implemented to, among other things, "protect personal information from unauthorized access, use, modification, or disclosure . . . of an individual residing in the State [of] [Maryland]."

568. A violation of the Maryland Personal Information Protection Act "is an unfair or deceptive trade practice."

569. AAD violated the Maryland Personal Information Protection Act by its failure to provide timely (within 45 days) and adequate (via direct mail) notice of the Data Breach in accordance with § 14-3504. Specifically, AAD delayed over 45 days to send notice of the Data Breach *via email*, which is only permissible if expressly consented to by the individual. *See* Md. Comm. Code § 14-3504(e)(2)(i). AAD also failed to provide its telephone number in the notices provided, in further violation of the statute. *See* Md. Comm. Code § 14-3504(g)(2).

570. Independently, AAD violated the Maryland Consumer Protection Act by engaging in the unfair and deceptive practices alleged herein. Pursuant to HIPAA (42 U.S.C. §§ 1302d, *et seq.*), the FTCA, and Maryland law—including, without limitation, Maryland's Personal

Information Protection Act—AAD was required, but failed, to protect Maryland Plaintiffs' and Maryland Subclass Members' Private Information and maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of such information and notify impacted individuals of a security breach thereof. These failures constitute violations of Maryland's Consumer Protection Act.

571. The damages suffered by the Maryland Plaintiffs and Maryland Subclass Members, as alleged herein, were directly and proximately caused by Defendant's deceptive, misleading, and unfair practices described above.

572. The Maryland Plaintiffs and Maryland Subclass Members seek declaratory judgment that Defendant's data security practices were not reasonable or adequate and caused the cyberattack under the Maryland CPA, as well as injunctive relief enjoining the above-described wrongful acts and practices of Defendant and requiring Defendant to employ and maintain industry accepted standards for data management and security. The Maryland Plaintiffs also seek attorneys' fees, as authorized by Maryland Code, Commercial Law § 13-408(b).

COUNT IX
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

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

574. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court also has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

575. AAD owes a duty of care to Plaintiffs and Class Members that required it to adequately secure their Private Information.

576. AAD still possesses Plaintiffs' and Class Members' Private Information.

577. AAD's data security measures remain inadequate. Further, Plaintiffs continue to suffer injury because of the compromise of their Private Information, and the risk remains that further compromises of their Private Information will occur in the future.

578. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. AAD owes a legal duty to secure its patients' Private Information and to timely notify them of a data breach under the common law, HIPAA, and the FTCA;

b. AAD's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patients' Private Information; and

c. AAD continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

579. This Court should also issue corresponding prospective injunctive relief requiring AAD to employ adequate security protocols consistent with legal and industry standards to protect patients' Private Information, including the following:

a. Order AAD to provide credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, AAD must implement and maintain reasonable security measures, including, but not limited to:

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

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of AAD's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting 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

vii. meaningfully educating its patients about the threats they face regarding the security of their Private Information as well as the steps they should take to protect themselves.

580. If the Court does not issue an injunction, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at AAD. The risk of another such breach is real, immediate, and substantial. If another breach at AAD occurs, Plaintiffs will

not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

581. The hardship to Plaintiffs absent an injunction exceeds the hardship to AAD that an injunction might cause. Whereas, absent an injunction, Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages, the cost to AAD of complying with an injunction requiring reasonable prospective data security measures is relatively minimal, and AAD has a pre-existing legal obligation to employ such measures.

582. Issuing the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at AAD, thus preventing future injury to Plaintiffs and other patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

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

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: December 12, 2025

Respectfully submitted,

/s/ Gary E. Mason
Gary E. Mason, Bar No. 15033
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
E: gmason@masonllp.com

James P. Ulwick, Bar No. 00536
KRAMON & GRAHAM, P.A.
750 East Pratt Street, Suite 1100
Baltimore, Maryland 21202
Phone: 410-752-6030
Fax: 410-539-1269
E: julwick@kg-law.com

Interim Co-Liaison Counsel

James J. Pizzirusso, Bar No. 20817
HAUSFELD LLP
1201 17th Street N.W., Suite 600
Washington, D.C. 20036
Tel: 202.540.7200
E: jpizzirusso@hausfeld.com

Gary Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
E: gklinger@milberg.com

Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com

Interim Co-Lead Class Counsel