UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

In re ApolloMD Data Breach Litigation,	No. 1:25-cv-05439-SEG **DEMAND FOR JURY TRIAL**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Lee Flint, Shawanna Townsend, Paul Bruni, Cathy O'Donnell, Cynthia Hall, Sarah Inman, Evelyn Adams, Ron Orton, Marion Wooten, Jerry Bossert, Lauren McEntee, Pamela Govan, Dominique Williams, and Carita Mathews ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint against Defendant ApolloMD Business Services, LLC ("ApolloMD" or "Defendant"), alleging the following upon personal knowledge as their own experiences and on information and belief upon their counsel's investigations and matters of public record.

INTRODUCTION

1. Plaintiffs and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted ApolloMD with sensitive Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively, "Private Information") that was impacted in a data breach (the "Data Breach" or the "Breach").

2. Plaintiffs' claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to them, and their accompanying responsibility to store and transfer that information securely.

3. Defendant ApolloMD is a physician practice management company based in Atlanta, Georgia that offers multispecialty business and health services to more than one hundred hospitals and health systems nationwide, including but not limited to Mercy Health Regional Medical Center, LLC d/b/a/ Mercy Health Lorain Hospital ("Mercy"), Rush Copley Medical Center ("Rush Copley"), Trinity Emergency Physicians ("Trinity"), Aurora Emergency Physicians, LLC ("Aurora Emergency"), Pensacola Hospitalist Physicians, LLC ("Pensacola Hospitalist"), and Baptist Health Care Inc. ("Baptist Health") (collectively, "Clients").

4. ApolloMD had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiffs and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. Between July 21, 2025, and September 11, 2025, ApolloMD notified its Clients of a data security incident that resulted in unauthorized access to and acquisition of information pertaining to patients of ApolloMD's Clients.

6. ApolloMD first became aware of the incident on May 22, 2025, after it detected unusual activity in its Information Technology ("IT") environment. Upon

learning of this, ApolloMD initiated an investigation to determine the nature and scope of the Data Breach.

7. ApolloMD's investigation determined that an unauthorized third-party accessed its IT environment between May 22, 2025 and May 23, 2025 and acquired files that contained information for patients treated by its Clients.

8. The following types of Private Information were compromised as a result of the Data Breach: names, dates of birth, addresses, diagnosis information, provider names, dates of service, medical and treatment information, health insurance information, and Social Security numbers.

9. On or around September 17, 2025, nearly four months after becoming aware of the Data Breach, ApolloMD began issuing notice letters to impacted individuals.

10. Five months later, in February 2026, ApolloMD confirmed that more than 626,000 people's Private Information was impacted by the Data Breach.[1]

11. ApolloMD failed to take precautions designed to keep Plaintiffs' and Class Members' Private Information secure.

12. ApolloMD owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

derived a benefit from the Private Information, yet breached their duty by failing to implement or maintain adequate security practices.

13. Defendant admit that information in their system was accessed by unauthorized individuals, though they provided little information regarding how the Data Breach occurred.

14. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiffs and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

15. Defendant failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information they maintained for Plaintiffs and Class Members, causing the exposure of Plaintiff and Class Members' Private Information.

16. As a result of Defendant's inadequate digital security and notice process, Plaintiffs and Class Members' Private Information was exposed to criminals. Plaintiffs and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of their personal and financial information.

17. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of ApolloMD's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. ApolloMD's conduct amounts to at least negligence and violates federal and state statutes.

18. Plaintiffs bring this action individually and on behalf of a Nationwide Class of similarly situated individuals against ApolloMD for: negligence; negligence *per se*; breach of third-party beneficiary contract, invasion of privacy, unjust enrichment, declaratory judgment, and fees and expenses under O.C.G.A. § 3-6-11.

19. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves, and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to ApolloMD's inadequate data security practice.

PARTIES

20. Plaintiff Lee Flint is a natural person, a citizen, and a resident of Lorain, Ohio, where she intends to remain.

21. Plaintiff Shawanna Townsend is a natural person, a citizen, and a resident of Yorkville, Illinois, where she intends to remain.

22. Plaintiff Paul Bruni is a natural person, a citizen, and a resident of Yorkville, Illinois, where he intends to remain.

23. Plaintiff Cathy Odonnell is a natural person, a citizen, and a resident of Pensacola, Florida, where she intends to remain.

24. Plaintiff Cynthia Hall is a natural person, a citizen, and a resident of Vestavia, Alabama, where she intends to remain.

25. Plaintiff Sarah Inman is a natural person, a citizen, and a resident of Birmingham, Alabama, where she intends to remain.

26. Plaintiff Evelyn Adams is a natural person, a citizen, and a resident of Hoover, Alabama, where she intends to remain.

27. Plaintiff Ron Orton is a natural person, a citizen, and a resident of Vincent, Alabama, where he intends to remain.

28. Plaintiff Marion Wooten is a natural person, a citizen, and a resident of Moody, Alabama, where she intends to remain.

29. Plaintiff Jerry Bossert is a natural person, a citizen, and a resident of Gulf Breeze, Florida, where he intends to remain.

30. Plaintiff Lauren McEntee is a natural person, a citizen, and a resident of Memphis, Tennessee, where she intends to remain.

31. Plaintiff Pamela Govan is a natural person, a citizen, and a resident of Memphis, Tennessee, where she intends to remain.

32. Plaintiff Dominique Williams is a natural person, a citizen, and a resident of Southaven, Mississippi, where she intends to remain.

33. Plaintiff Carita Mathews is a natural person, a citizen, and a resident of Atlanta, Georgia, where she intends to remain.

34. Defendant ApolloMD is a limited liability company formed under the laws of Georgia with its principal place of business at 5665 New Northside Drive, Atlanta, Georgia 30328.

JURISDICTION AND VENUE

35. This 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. There are over 100 putative Class Members, and most of the Plaintiffs are citizens of a different state than Defendant.[2]

36. This Court has personal jurisdiction over ApolloMD because ApolloMD is headquartered in this District, regularly conducts business in this District, and has sufficient minimum contacts in this District.

[2] Under the Class Action Fairness Act, "an unincorporated association shall be deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized." 28 U.S.C. § 1332(d)(10). Thus, as an LLC, Defendant ApolloMD is a citizen of Georgia (its state of formation and principal place of business).

37. Venue is proper in this Court because Defendant ApolloMD's principal place of business is located in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

ApolloMD Collected and Stored the Private Information of Plaintiffs and the Class

38. ApolloMD is a physician practice management company based in Atlanta, Georgia that offers multispecialty business and health services to its Clients, which are hospitals, health systems, and physician practices.[3]

39. As part of its business, ApolloMD receives and maintains the Private Information of hundreds of thousands of patients from its Clients.

40. In collecting, transferring, and maintaining the Private Information, ApolloMD agreed to safeguard the data in accordance with their internal policies, industry standards, state law, and federal law. Indeed, Plaintiffs and Class Members took reasonable steps to secure their Private Information that they possessed, but they had no ability to protect the information in ApolloMD's possession.

41. Under state and federal law, businesses like ApolloMD have duties to protect patients' Private Information and to promptly and accurately notify them about data breaches.

[3] *Home Page*, APOLLOMD, https://apollomd.com/.

Defendant's Data Breach

42. Between May 22, 2025, and May 23, 2025, cybercriminals targeted, accessed, and stole the Private Information from ApolloMD's systems in the Data Breach.[4]

43. Worryingly, ApolloMD admitted that:

a. "Between July 21, 2025 and September 11, 2025, ('ApolloMD') notified its affiliated physician practices of a data security incident that may have resulted in unauthorized access to / acquisition of information pertaining to some of their patients. ApolloMD first became aware of the incident on May 22, 2025, after it detected unusual activity in its Information Technology ('IT') environment. Upon learning of this, we initiated an investigation, took steps to secure our systems, engaged a third-party forensic firm to assist in the investigation, and notified law enforcement."[5]

b. "Our investigation determined that an unauthorized party accessed ApolloMD's IT environment between May 22, 2025

[4] *Notice of Data Security Incident*, APOLLOMD (Sept. 15, 2025) https://go.pardot.com/l/86652/2025-09-15/96sz4g/86652/1757967385wtBivHnU/ApolloMD_Substitute__Website__Notice.pdf (hereafter, "Notice").
[5] *Id*.

> and May 23, 2025. While in the IT environment, the unauthorized party may have accessed and/or acquired files that contain information for patients treated by ApolloMD's affiliated physicians and practices. The information involved varied by patient and includes names in combination with one or more of the following: dates of birth, addresses, diagnosis information, provider names, dates of service, treatment information, and/or health insurance information. For some individuals, the incident may have also involved their Social Security numbers."[6]

44. The Data Breach impacted patients (including Plaintiffs) from various healthcare providers, including: "PASSAIC HOSPITALIST SERVICES, LLC; PENSACOLA HOSPITALIST PHYSICIANS, LLC; BROAD RIVER PHYSICIANS GROUP, LLC; OLIVE BRANCH EMERGENCY PHYSICIANS, LLC; AURORA EMERGENCY PHYSICIANS, LLC; PASSAIC RIVER PHYSICIANS, LLC; THE BORTOLAZZO GROUP, LLC; METHODIST UNIVERSITY EMERGENCY PHYSICIANS, PLLC; TRINITY EMERGENCY PHYSICIANS, LLC; LORAIN EMERGENCY PHYSICIANS, LLC; and PENNSYLVANIA HOSPITALIST GROUP, LLC."[7]

[6] *Id.*
[7] *Id.*

45. According to ApolloMD's recent report to the U.S. Department of Health and Human Services, more than 600,000 people were impacted by the Data Breach.[8]

46. ApolloMD failed to comply with its duties to employ adequate security practices and to stop cybercriminals from accessing the Private Information, causing widespread injury and monetary damages.

47. Further, the Notice of Data Breach shows that ApolloMD cannot—or will not—determine the full scope of the Data Breach, as ApolloMD has been unable to determine precisely what information was stolen and when.

48. Because of the Data Breach, the sensitive Private Information of Plaintiffs and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class Members now and for years to come.

Qilin & the Dark Web

49. Reports indicate that the cybercriminals that obtained Plaintiffs' and Class Members' Private Information appear to be the notorious cybercriminal group

[8] U.S. Department of Health and Human Services, *HIPAA Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf (last visited Feb. 26, 2026).

"Qilin" which succeeded in exfiltrating 238 gigabytes of data (include the Private Information of Plaintiffs and Class Members).[9]

50. Thus, on information and belief, Plaintiffs' and the Class's stolen Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiffs' Experiences and Injuries

Plaintiff Lee Flint

51. Plaintiff Lee Flint is a patient of Mercy and received a Notice of Data Breach.

52. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff was injured by Defendant's Data Breach.

53. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

54. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained

[9] *ApolloMD*, BREACHSENSE (June 13, 2025) https://www.breachsense.com/breaches/apollomd-data-breach/.

and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

55. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

56. On information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

57. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

58. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

59. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls.

60. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach, which is compounded by Defendant's delay in notifying her of the Data Breach.

61. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

62. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

63. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

64. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

65. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

66. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Shawanna Townsend

67. Plaintiff Shawanna Townsend is a patient of Rush Copley and received a Notice of Data Breach.

68. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff was injured by Defendant's Data Breach.

69. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

70. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

71. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

72. On information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

73. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

74. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

75. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls.

76. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach, which is compounded by Defendant's delay in notifying her of the Data Breach.

77. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

78. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

79. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

80. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

81. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

82. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Paul Bruni

83. Plaintiff Paul Bruni is a patient of Rush Copley and received a Notice of Data Breach.

84. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff was injured by Defendant's Data Breach.

85. Plaintiff is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

86. Plaintiff provided his Private Information to Defendant through his medical provider and trusted that his Private Information would be protected

according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

87. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of his Private Information.

88. On information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

89. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

90. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

91. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages, emails, and phone calls.

92. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach, which is compounded by Defendant's delay in notifying him of the Data Breach.

93. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

94. Plaintiff suffered actual injury from the exposure and theft of his Private Information—which violates her rights to privacy.

95. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

96. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

97. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

98. Today, Plaintiff has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Cathy Odonnell

99. Plaintiff Cathy Odonnell is a current patient of Baptist Health and received a Notice of Data Breach.

100. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

101. Plaintiff was injured by Defendant's Data Breach.

102. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

103. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

104. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

105. On information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

106. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

107. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

108. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls. Plaintiff also had unauthorized charges on her credit card from a different country that were flagged by her bank, causing her to have to close her card.

109. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach, which is compounded by Defendant's delay in notifying her of the Data Breach.

110. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

111. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

112. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

113. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

114. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

115. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Cynthia Hall

116. Plaintiff Cynthia Hall has been a patient of Grandview Trinity Emergency Physicians since August of 2023 and was an employee of Trinity from 2008-2010.

117. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

118. Plaintiff was injured by Defendant's Data Breach.

119. Plaintiff disclosed to Defendant her name, date of birth, address, Social Security Number, health information, insurance information, contact information, driver's license number, financial information, and her husband's personal information as her emergency contact.

120. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

121. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

122. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

.

123. Thus, on information and belief, Plaintiff's Private Information likely will be published imminently—by cybercriminals on the Dark Web.

124. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

125. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft by calling her bank and contacting customer service. After all, Defendant directed Plaintiff to take those steps in its breach notice.

126. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls. Plaintiff also had multiple unauthorized charges on her credit card.

127. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

128. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

129. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

130. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

131. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

132. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

133. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Sarah Inman

134. Plaintiff Sarah Inman has been a patient of Grandview Trinity Emergency Physicians since around 2023.

135. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

136. Plaintiff was injured by Defendant's Data Breach.

137. Plaintiff disclosed to Defendant her name, phone number, email address, medical information and history, insurance information, financial information, and Social Security Number.

138. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

139. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

140. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information..

141. Thus, on information and belief, Plaintiff's Private Information likely will be published imminently—by cybercriminals on the Dark Web.

142. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

143. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

144. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls.

145. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

146. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

147. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

148. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

149. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because

Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

150. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

151. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Evelyn Adams

152. Plaintiff Evelyn Adams has been a patient of Grandview Trinity Emergency Physicians for the last 5 to 6 years and left the network in January in 2025.

153. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

154. Plaintiff was injured by Defendant's Data Breach.

155. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

156. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected

according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

157. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

158. Thus, on information and belief, Plaintiff's Private Information likely will be published imminently—by cybercriminals on the Dark Web.

159. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

160. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft by calling her bank and contacting customer service. Plaintiff believes she has already spent around 10 hours dealing with fraud. After all, Defendant directed Plaintiff to take those steps in its breach notice.

161. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls. Plaintiff believes she receives around 2-3 spam emails a day.

162. In May of 2025, Plaintiff's bank account was "drained," as a result of 16 payments of roughly $97 being made out of her account, leaving only $9. Plaintiff believes roughly $1,600 was taken from her bank account. Though Plaintiff's bank was able to refund her the money, it took several days to receive.

163. Plaintiff received invoices from a Toyota in South Carolina that matched the incremental payments of $97 out of her account. Plaintiff notes that she has never been to South Carolina. The invoices were sent to Plaintiff's personal email address; however, the invoices were addresses to an "Elizabeth," a name Plaintiff has never gone by.

164. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

165. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

166. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

167. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

168. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

169. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

170. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Ron Orton

171. Plaintiff Ron Orton is a patient of Trinity and received a Notice of Data Breach.

172. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff was injured by Defendant's Data Breach.

173. Plaintiff is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the

internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

174. Plaintiff provided his Private Information to Defendant through his medical provider and trusted that his Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

175. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of his Private Information.

176. On information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

177. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

178. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

179. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages, emails, and phone calls.

180. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach, which is compounded by Defendant's delay in notifying him of the Data Breach.

181. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

182. Plaintiff suffered actual injury from the exposure and theft of his Private Information—which violates her rights to privacy.

183. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

184. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

185. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

186. Today, Plaintiff has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Marion Wooten

187. Plaintiff Marion Wooten is a patient of Trinity.

188. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

189. Plaintiff was injured by Defendant's Data Breach.

190. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

191. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

192. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

193. Thus, on information and belief, Plaintiff's Private Information likely will be published imminently—by cybercriminals on the Dark Web.

194. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

195. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft.

196. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls.

197. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

198. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

199. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

200. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

201. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

202. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

203. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Jerry Bossert

204. Plaintiff Jerry Bossert is a patient of Baptist Health and Pensacola Hospitalist and received a Notice of Data Breach.

205. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff was injured by Defendant's Data Breach.

206. Plaintiff is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the

internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

207. Plaintiff provided his Private Information to Defendant through his medical provider and trusted that his Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

208. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of his Private Information.

209. On information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

210. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

211. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

212. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages, emails, and phone calls.

213. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach, which is compounded by Defendant's delay in notifying him of the Data Breach.

214. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

215. Plaintiff suffered actual injury from the exposure and theft of his Private Information—which violates her rights to privacy.

216. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

217. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

218. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

219. Today, Plaintiff has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Lauren McEntee

220. Plaintiff Lauren McEntee has been a long-time patient of Methodist University Hospital, having recently been treated in the emergency room on August 16th.

221. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

222. Plaintiff was injured by Defendant's Data Breach.

223. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

224. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal

duty and obligation to protect that Private Information from unauthorized access and disclosure.

225. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

226. Thus, on information and belief, Plaintiff's Private Information likely will be published imminently—by cybercriminals on the Dark Web.

227. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

228. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

229. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls regarding loans that she did not apply for. Plaintiff also had to close her bank account recently as a result of fraudulent charges.

230. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

231. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such

injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

232. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

233. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

234. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

235. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

236. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Pamela Govan

237. Plaintiff Pamela Govan has been a patient of Methodist University Hospital for the last ten years.

238. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

239. Plaintiff was injured by Defendant's Data Breach.

240. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

241. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

242. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

243. Thus, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

244. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

245. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

246. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls. Plaintiff believes she receives more than three spam calls a day.

247. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

248. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

249. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

250. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

251. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

252. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

253. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Dominique Williams

254. Plaintiff Dominique Williams has been an employee of Methodist University Hospital for the last five years.

255. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

256. Plaintiff was injured by Defendant's Data Breach.

257. Plaintiff disclosed to Defendant date of birth, address, diagnostic information, provider name, dates of service, treatment information, and health insurance information.

258. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the

internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

259. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

260. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information..

261. Thus, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

262. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

263. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Plaintiff even took time to sign up for the free credit monitoring service provided by Defendant

following the breach. After all, Defendant directed Plaintiff to take those steps in its breach notice.

264. And in the aftermath of the Data Breach, Plaintiff has noticed her medical bills with Methodist have increased but she does not know why.

265. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

266. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

267. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

268. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

269. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

270. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

271. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Carita Mathews

272. Plaintiff Carita Mathews was a patient of Wellstar Health System in July 2022.

273. Defendant obtained and maintained Plaintiff's Private Information, and Plaintiff received a Notice of Data Breach.

274. Plaintiff was injured by Defendant's Data Breach.

275. Plaintiff disclosed to Defendant her name, date of birth, address, medical history, health insurance information, financial information, treatment information, providers, contact information, and her MyChart account.

276. Plaintiff is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

277. Plaintiff provided her Private Information to Defendant through her medical provider and trusted that her Private Information would be protected

according to internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

278. Plaintiff reasonably understood that a portion of the funds paid for medical services would be used to pay for adequate cybersecurity and protection of her Private Information.

279. Thus, on information and belief, Plaintiff's Private Information will likely be published imminently by cybercriminals on the Dark Web.

280. Through its Data Breach, Defendant compromised Plaintiff's Private Information.

281. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

282. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls. Plaintiff believes she receives about 20 spam calls per day.

283. Plaintiff's debit and credit card have gotten alerts of unauthorized purchases on her account. She also received notice of attempted unauthorized transactions on her CashApp account, which is linked to her credit and debit account.

284. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

285. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

286. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

287. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

288. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

289. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

290. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Consumers Prioritize Data Security

291. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[10] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[11]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[12]

c. 89% of consumers stated that "I care about data privacy."[13]

[10] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).
[11] *Id*. at 3.
[12] *Id*.
[13] *Id*. at 9.

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[14]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[15]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[16]

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

292. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

[14] *Id.*
[15] *Id.*
[16] *Id.* at 11.

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

293. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.

294. The value of Plaintiffs and Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

295. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the Private Information far and wide.

296. One way that criminals profit from stolen Private Information is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen Private Information, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

297. The development of "Fullz" packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

298. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals 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. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

299. Defendant disclosed the Private Information of Plaintiffs and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

300. Defendant's failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

301. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

302. In 2024, a record 3,158 data breaches occurred—exposing approximately 1,350,835,988 sensitive records (i.e., 211% increase year over year).[17]

[17] *2024 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.

303. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[18]

304. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations have experienced cyberattacks.[19]

305. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

306. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

---

[18] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[19] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Sept. 11, 2023).

307. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[20] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

308. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

309. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

[20] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

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

311. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

312. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption (making data

unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

313. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

314. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation 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 all established standards in reasonable cybersecurity readiness.

315. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

316. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[21]

317. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information and PHI is properly maintained.[22]

318. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

[21] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[22] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

b. 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);

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

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. 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);

f. 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);

g. failing to identify and respond to suspected or known security incidents and 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 effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

319. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

320. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members ("Class Members") of the following nationwide class (the "Class"):

> All individuals residing in the United States whose Private Information was compromised in the Data Breach discovered by ApolloMD in May 2025, including all those individuals who received notice of the breach.

321. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

322. Plaintiffs reserve the right to amend the class definition.

323. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

324. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified the impacted individuals and sent them a data breach Notice.

325. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. The proposed Class includes at least 626,000 people.[23]

[23] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

326. Typicality. Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

327. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Her interests do not conflict with Class Members' interests. And Plaintiffs has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

328. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Private Information;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing Private Information;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's Private Information;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

329. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues

in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

330. Plaintiffs repeat and incorporate by reference the allegations in paragraphs 1-329 as if fully set forth herein.

331. Plaintiffs and the Class (or their third-party agents) entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their Private Information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

332. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Private Information in a data breach. And here, that foreseeable danger came to pass.

333. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if their Private Information was wrongfully disclosed.

334. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals

whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class Members' Private Information.

335. Defendant owed—to Plaintiffs and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

336. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

337. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

338. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

339. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class (or their third-party agents) entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

340. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant hold vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information —whether by malware or otherwise.

341. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private

Information of Plaintiffs and Class Members' and the importance of exercising reasonable care in handling it.

342. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

343. Defendant breached these duties as evidenced by the Data Breach.

344. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

345. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs and Class Members' injury.

346. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually

and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class Members' injuries-in-fact.

347. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

348. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

349. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

350. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence,

which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

351. Plaintiffs repeat and incorporate by reference the allegations in paragraphs 1-329 as if fully set forth herein.

352. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

353. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class Members' sensitive Private Information.

354. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

355. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with

applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

356. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

357. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class Members would not have been injured.

358. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

359. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class Members' PHI.

360. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

361. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

362. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and the Class)

363. Plaintiffs repeat and incorporate by reference the allegations in paragraphs 1-329 as if fully set forth herein.

364. On information and belief, Defendant entered into contracts to provide services to its Clients, which were made for the benefit of Plaintiffs and Class Members.

365. On information and belief, these contracts are virtually identical and were made expressly for the benefit of Plaintiffs and Class Members, as it was their

Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and Class Members was a direct and primary objective of the contracting parties.

366. Defendant knew that if it was to breach these contracts with its Clients, Plaintiffs and Class Members would be harmed.

367. Defendant breached the contracts with its Clients by failing to protect the Private Information it obtained pursuant to these contracts.

368. As a result, Plaintiffs and Class Members were harmed by the Data Breach when Defendant failed to use reasonable data security measures that could have prevented the Data Breach, and when it failed to timely notify Plaintiffs and Class Members regarding the breach, so that they could protect themselves.

369. As foreseen, Plaintiffs and Class Members were harmed by Defendants' failure to use reasonable data security measures to secure the Private Information from unauthorized access and failure to timely notify Plaintiffs and Class Members, which harms include, but are not limited to: (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) emotional distress due to their Private Information's publication on the dark web; (e) existing misuse of their

Private Information in the form of fraud, identity theft, and increased, unwanted spam communications; and (f) the continued and certainly increased risk to their Private Information, which remains in Defendants' possession in unencrypted form and subject to further unauthorized disclosures.

370. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

371. Plaintiffs repeat and incorporate by reference the allegations in paragraphs 1-329 as if fully set forth herein.

372. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

373. Defendant owed a duty to its current and former patients, including Plaintiffs and the Class, to keep this information confidential.

374. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' Private Information is highly offensive to a reasonable person.

375. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

376. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

378. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

379. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

380. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and the Class were stolen by a third

party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

381. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

382. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

383. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

384. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

385. Plaintiffs repeat and incorporate by reference the allegations in paragraphs 1-329 as if fully set forth herein.

386. This claim is pleaded in the alternative to the breach of implied contract claim.

387. Plaintiffs and Class Members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their Private Information to provide services, and (2) accepting payment.

388. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members.

389. Plaintiffs and Class Members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

390. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

391. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on

the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

392. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' (1) Private Information and (2) payment because Defendant failed to adequately protect their Private Information.

393. Plaintiffs and Class Members have no adequate remedy at law.

394. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

395. Plaintiffs repeat and incorporate by reference the allegations in paragraphs 1-329 as if fully set forth herein.

396. 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 has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

397. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and

belief, Plaintiffs alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

398. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class Members.

399. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

400. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

401. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class Members' injuries.

402. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

403. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class Members, and the public at large.

SEVENTH CAUSE OF ACTION
Expenses of Litigation, O.C.G.A. § 13-6-11
(On Behalf of Plaintiffs and the Class)

404. Plaintiffs repeat and incorporate by reference the allegations in paragraphs 1-329 as if fully set forth herein.

405. As alleged herein, ApolloMD acted in bad faith, was stubbornly litigious, or caused Plaintiffs and Class Members unnecessary trouble and expense with respect to the events underlying this litigation.

406. As alleged herein, ApolloMD harmed Plaintiffs and Class Members by failing to use reasonable measures to protect their Private Information and not complying with laws, regulations, and industry standards, requiring them to do so, including, but not limited to, the FTCA and HIPAA. ApolloMD's conduct was particularly unreasonable given the nature and amount of Private Information that it obtained, used, and stored and the foreseeable consequences of a data breach.

407. ApolloMD also has a duty under the Georgia Constitution which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its customers', beneficiaries', employees', agents', and other individuals' Private Information. The Constitution states "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

408. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) § 652A which specifically recognized four common law invasion of privacy claims in Georgia, which include (1) appropriation of likeness; (2) intrusion on solitude or seclusion; (3) public disclosure of private facts; and (4) false light.

409. ApolloMD's affirmative implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of

its responsibility to reasonably protect the Private Information of Plaintiffs and Class Members that it stored on its own servers and databases constitutes a violation of the Constitution and the Restatement of the Law of Torts (Second).

410. ApolloMD knew or should have known that it had a responsibility to protect the Private Information it stored, that it was entrusted with this Private Information, and that it was the only entity capable of adequately protecting the Private Information on its systems and databases.

411. Despite that knowledge, ApolloMD abdicated its duty to protect the Private Information that ApolloMD stored.

412. As a direct and proximate result of ApolloMD's actions, Plaintiffs' and Class Members' Private Information was accessed and stolen by cybercriminals. The Data Breach was a direct consequence of ApolloMD's abrogation of its data security responsibilities and its decision to employ knowingly deficient data security measures that knowingly left the Private Information unsecured. Had ApolloMD adopted reasonable data security measures, it could have prevented the Data Breach.

413. As further described above, Plaintiffs and Class Members have been injured and suffered losses directly attributable to the Data Breach.

414. Plaintiffs and Class Members therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and

that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all issues and claims so triable.

Date: February 26, 2026

Respectfully submitted,

/s/ Casondra Turner
Casondra Turner
(GA Bar No. 418426)
MILBERG, PLLC
260 Peachtree Street NW, Suite 2200
Atlanta, GA 30303
Tel: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

Jeff Ostrow (*pro hac vice*)
KOPELOWITZ OSTROW P.A.
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
ostrow@kolawyers.com

Interim Co-Lead Counsel for Plaintiffs and the Putative Class

Andrew J. Shamis
SHAMIS & GENTILE, P.A.
14 NE 1st Ave., Suite 705
Miami, FL 33132
Tel: 305-479-2299
Fax: 786-623-0915
ashamis@shamisgentile.com

Raina C Borrelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Tel: 872-263-1100
Fax: 872-263-1109
raina@straussborrelli.com

Additional Counsel for Plaintiffs and the Putative Class

**Pro hac vice forthcoming*

CERTIFICATE OF SERVICE

I, Casondra Turner, hereby certify that on February 26, 2026, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to all counsel of record.

DATED this 26th day of February, 2026.

/s/ Casondra Turner
Casondra Turner

ClassAction.org
