INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT
	) SS:	
COUNTY OF MARION	)	CAUSE NO. 49D01-2207-PL-024807

IN RE: INDIANAPOLIS NEUROSURGICAL GROUP, P.C., d/b/a GOODMAN CAMPBELL BRAIN AND SPINE DATA INCIDENT LITIGATION	)	JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Joshua Ham, Rhonda Hensley-Johnson, Julianne Smallwood, Karrin Spencer, Mary Rebecca Hostetter, Victoria Powers, Ricky Perdue, Connie Goff, and Brittany Gilland, on behalf of herself, and her three minor children, A.G., B.G., and C.G.[1] (collectively, "Plaintiffs"), bring this action on behalf of themselves, and all others similarly situated, against Defendant Indianapolis Neurosurgical Group, P.C., d/b/a Goodman Campbell Brain & Spine ("Goodman" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and allege as follows:

NATURE OF THE ACTION

1. Defendant Goodman, an Indiana-based neurosurgical medical practice established in 1972, lost control over its former and current patients' and employees' highly sensitive personal and medical information to cybercriminals (the "Data Breach").

2. As of the date of this Consolidated Amended Complaint, the exact number of Data Breach victims remains unknown but is believed to be at least 362,833.[2] Goodman has yet to complete and/or share the results of its Data Breach investigations, the scope of which Goodman continues to change over time.

3. On information and belief, the Data Breach occurred on May 20, 2022. It remains unclear when Goodman first became aware of the Data Breach.

[1] The minors' names have been pseudonymously abbreviated to protect their privacy.
[2] *See* Office of the Maine Attorney General Data Breach Notifications, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/95f7ef39-de73-4165-806c-ad11b2e661dd.shtml (last accessed Apr. 10, 2023).

4. On or around June 3, 2022, Goodman posted a statement on its website acknowledging the Data Breach ("Website Notice").[3] At the time, Goodman did not identify what type of information was stolen; however, the Website Notice warned that Goodman's "initial analysis indicate[d] that both . . . patient and employee data has been accessed by an unauthorized party."

5. Goodman stated that cyber criminals gained unauthorized access to current and former patients' and current and former employees' confidential personally identifying information and/or protected health information (together "PHI").[4] Goodman did not disclose what specific PHI was included in the Data Breach, leaving Plaintiffs and Class Members guessing.

6. On June 17, 2022, Goodman updated its Website Notice to inform patients and employees that cybercriminals responsible for the Data Breach had posted certain sensitive patient and business information on the dark web, including patients' and employees' PHI.

7. At this point, Goodman still did not disclose what specific PHI was involved, but ominously warned patients and employees to be vigilant in reviewing their banking/financial account statements for fraudulent activity.

8. On July 19, 2022, Goodman once again updated its Website Notice. This time, Goodman informed patients and employees that the information involved in the Data Breach included medical, financial, and demographic information related to patients. Specifically, the PHI

---

[3] *See* Goodman's Website, https://www.goodmancampbell.com/2022/06/important-update/ (last accessed Apr. 8, 2023).

[4] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. A "covered entity" is further defined as, *inter alia*, a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. *Id. Covered entity*. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed July 14, 2022). Goodman is clearly a "covered entity" and some of the data compromised in the Data Breach that this action arises out of is "protected health information", subject to HIPAA.

impacted included: names, dates of birth, addresses, telephone numbers, email addresses, medical record numbers, patient account numbers, diagnosis and treatment information, physician information, insurance information, date(s) of service, and Social Security numbers.

9. Written notification about the Data Breach event was finally sent to impacted individuals on or about the same day (July 19, 2022).

10. The written notification stated that information acquired by the attacker was made available on the dark web for approximately ten days.[5]

11. On August 11, 2022, Goodman updated its Website Notice for the fourth time. This time, Goodman alerted patients and employees that despite conveying to patients and employees that PHI acquired by the attacker was made available on the dark web for approximately ten days, Goodman learned from forensic experts and law enforcement officials that patient and employee PHI posted to the dark web had been reactivated by the attacker."[6]

12. Goodman has still refused to transparently share the full results of its investigations despite having knowledge of published PHI on the dark web and the imminent harm facing each Data Breach victim.

13. Goodman knew or should have known that each victim of the Data Breach deserved prompt, efficient, and accurate notice of the Data Breach as well as assistance in mitigating the effects of fraud and identity theft.

14. On information and belief, cyber criminals were able to breach Goodman's systems because Goodman did not maintain reasonable security safeguards or protocols to protect its patients' and employees' PHI, leaving the PHI as an unguarded target for theft and misuse.

15. Goodman's failures to timely detect and notify Data Breach victims violate Indiana law and has made affected patients and employees vulnerable to identity theft for the rest of their lives.

16. Plaintiffs and Class Members have suffered injuries from Goodman's conduct, including: (i) the lost or diminished value of their PHI; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive PHI.

[5] *See* Exhibit 1, Goodman Campbell – Breach Notification Letter for Adults.
[6] *See* Website Notice.

17. Plaintiffs and Class Members are victims of Defendant's failure to abide by its data security promises and inadequate cyber security measures. Specifically, Plaintiffs and Class Members trusted Defendant with their PHI. Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

18. Accordingly, Plaintiffs and Class Members bring this lawsuit seeking damages and relief for Defendant's actions.

PARTIES

19. Plaintiff Joshua Ham is a natural person and citizen of Indiana. Plaintiff Ham's PHI was compromised by the Data Breach, which he confirmed by calling the toll free number provided by Goodman and being told that he was in fact a breach victim and that his notice letter had been sent to the wrong address.

20. Plaintiff Rhonda Hensley-Johnson is a natural person and citizen of Indiana. Plaintiff Hensley-Johnson's PHI was compromised by the Data Breach.

21. Plaintiff Julianne Smallwood is a natural person and citizen of Indiana. Plaintiff Smallwood's PHI was compromised by the Data Breach.

22. Plaintiff Karrin Spencer is a natural person and citizen of Indiana. Plaintiff Spencer's PHI was compromised by the Data Breach.

23. Plaintiff Mary Rebecca Hostetter is a natural person and citizen of Indiana. Plaintiff Hostetter's PHI was compromised by the Data Breach.

24. Plaintiff Victoria Powers is a natural person and citizen of Indiana. Plaintiff Powers's PHI was compromised by the Data Breach.

25. Plaintiff Ricky Perdue is a natural person and citizen of Indiana. Plaintiff Perdue's PHI was compromised by the Data Breach.

26. Plaintiff Connie Goff is a natural person and citizen of Indiana. Plaintiff Goff's PHI was compromised by the Data Breach.

27. Plaintiff Brittany Gilland is a natural person and citizen of Indiana, and the mother of A.G., B.G., and C.G. Plaintiff Gilland's and her children's PHI was compromised by the Data Breach.

28. Defendant Goodman is an Indiana corporation with its principal place of business at 13345 Illinois Street, Carmel, Indiana 46032.

JURISDICTION AND VENUE

29. This Court has jurisdiction over Goodman because Goodman is a citizen of this State.

30. Preferred venue lies in Marion County because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this County.

FACTUAL ALLEGATIONS

A. Goodman's Failure to Safeguard Patients' and Employees' PHI

31. Plaintiffs and Class Members are Goodman's current and former patients and current and former employees.

32. As a prerequisite of receiving treatment, Goodman requires its patients to provide their PHI.

33. On information and belief, Goodman maintains records of its patients' information such as its patients' full names, Social Security Numbers, financial account information, credit-card information, dates of birth, prescription information, diagnosis information, treatment information, treatment providers, health insurance information, medical information, and Medicare/Medicaid ID numbers, in the ordinary course of business. These records are stored on Goodman's computer systems.

34. As a prerequisite of employment with Goodman, Goodman requires its employees to provide their PHI.

35. On information and belief, Goodman maintains records of its employees' information such as employees' full names, Social Security Numbers, financial account information, dates of birth, health insurance information, and medical information in the ordinary course of business. These records are stored on Goodman's computer systems.

36. When Goodman collects this sensitive information, it promises to use reasonable measures to safeguard the PHI from theft and misuse.

37. Goodman represents to its patients and employees that their PHI would be secure. Plaintiffs and Class Members relied on such representations when they agreed to provide their PHI to Goodman.

38. Despite its alleged commitments to securing sensitive patient and employee data, Goodman does not follow industry standard practices in securing patients' and employees' PHI.

39. In May 2022, hackers bypassed Goodman's security safeguards and infiltrated its systems, giving the hackers unfettered access to patients' and employees' PHI.

40. As described above, Goodman has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

41. On information and belief, Goodman does not adequately implement cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

42. Goodman's conduct caused the Data Breach. Goodman violated its obligation to implement best practices and comply with industry standards concerning computer system security. Goodman failed to comply with security standards and allowed its patients' and employees' PHI to be accessed and stolen by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach.

43. Through its Website Notice, Goodman recognizes the actual imminent harm and injury that flowed from the Data Breach. Goodman encourages Data Breach victims to "be vigilant in reviewing banking/financial account statements and credit reports for fraudulent or irregular activity."

44. Despite discovering the Data Breach in May 2022, Goodman did not offer any credit monitoring or other support services to victims of the Data Breach until at least July 19, 2022. In its original notices to victims, Goodman provided general instructions to victims to mitigate the consequences of Goodman's conduct in allowing the Data Breach to occur. Now, despite the substantial PHI involved in the Data Breach, Goodman is offering Plaintiffs and Class Members only twelve months of single bureau credit monitoring services. This offer is wholly insufficient given the severity of the Data Breach and the consequences of Plaintiffs' and proposed Class Members' PHI being readily available on the dark web.

B. Plaintiffs' Experiences

Plaintiff Ham

45. Plaintiff Ham is a former Goodman patient.

46. As a condition of receiving Goodman's medical treatment and services, Goodman required Plaintiff Ham to provide it with his PHI.

47. Upon information and belief, Plaintiff Ham's PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

48. Plaintiff Ham believed, as part of the payments to Goodman for medical treatment and services, that those payments included amounts for adequate data security. Had Plaintiff Ham known that Goodman did not utilize reasonable data security measures, he would have paid less for his treatments and services or would not have provided Goodman with his PHI.

49. Plaintiff Ham will have to spend considerable time and effort over the coming years monitoring his accounts to protect himself from identity theft resulting from his PHI being posted to the dark web.

50. Indeed, Plaintiff Ham has already suffered damages in the form of identity theft resulting from the Data Breach. Plaintiff Ham experienced fraudulent activities on his personal financial accounts within weeks of the Data Breach. Cybercriminals have already used Plaintiff Ham's credit card to make fraudulent purchases and have even attempted to withdraw money from his personal bank account.

51. Additionally, Plaintiff Ham received notice of an unauthorized attempt to open a new credit card account in his name. Plaintiff Ham's financial apps have also been compromised since the Data Breach.

52. Plaintiff Ham's sensitive PHI remains in Goodman's possession without adequate protection against known threats, exposing Plaintiff Ham to the prospect of additional harm in the event Goodman suffers another data breach.

53. Plaintiff Ham is very careful about sharing his PHI. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

54. Plaintiff Ham stores any documents containing his PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

55. Plaintiff Ham suffered actual injury in the form of damages to and diminution in the value of his PHI—a form of intangible property that Plaintiff Ham entrusted to Defendant for the purpose of medical care, which was compromised in and as a result of the Data Breach.

56. Plaintiff Ham suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

57. Plaintiff Ham is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PHI, especially his Social Security number and sensitive

medical information, in combination with his name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PHI.

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

Plaintiff Hensley-Johnson

59. Plaintiff Hensley-Johnson is a former Goodman patient who began receiving medical treatment from Goodman in or around 2021.

60. As a condition of receiving Goodman's medical treatment and services, Goodman required Plaintiff Hensley-Johnson to provide it with her PHI.

61. Upon information and belief, Plaintiff Hensley-Johnson's PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

62. Plaintiff Hensley-Johnson believed, as part of the payments to Goodman for medical treatment and services, that those payments included amounts for adequate data security. Had Plaintiff Hensley-Johnson known that Goodman did not utilize reasonable data security measures, she would have paid less for her treatments and services or would not have provided Goodman with her PHI.

63. Plaintiff Hensley-Johnson will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft resulting from her PHI being posted to the dark web.

64. Indeed, Plaintiff Hensley-Johnson has already suffered damages in the form of identity theft and fraud. On August 16, 2022, after the Data Breach and as a direct and proximate cause of the Data Breach, Plaintiff Hensley-Johnson was flagged during a credit check and subsequently denied services as a result of the credit check. Plaintiff Hensley-Johnson had never previously been flagged for a credit check. During this process, Plaintiff Hensley-Johnson was also required to prove her identity via documentation in addition to the documents initially submitted for the credit check. Plaintiff Hensley-Johnson spent time and effort resolving this credit issue.

65. Plaintiff Hensley-Johnson has also received several phone calls from a company demanding she pay an outstanding balance for CBD oil purchased using her information, including her name, address, and phone number. Plaintiff Hensley-Johnson has never purchased CBD oil. Upon information and belief, this identity theft is a direct and proximate injury resulting from the Data Breach.

66. Plaintiff Hensley-Johnson's sensitive PHI remains in Goodman's possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm in the event Goodman suffers another data breach.

67. Plaintiff Hensley-Johnson is very careful about sharing her PHI. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

68. Plaintiff Hensley-Johnson stores any documents containing her PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

69. Plaintiff Hensley-Johnson suffered actual injury in the form of damages to and diminution in the value of her PHI—a form of intangible property that Plaintiff Hensley-Johnson entrusted to Defendant for the purpose of medical care, which was compromised in and as a result of the Data Breach.

70. Plaintiff Hensley-Johnson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

71. Plaintiff Hensley-Johnson is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PHI, especially her Social Security number and sensitive medical information, in combination with her name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PHI.

72. Plaintiff Hensley-Johnson has a continuing interest in ensuring that her PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Smallwood

73. Plaintiff Smallwood is a former Goodman patient.

74. As a condition of receiving Goodman's medical treatment and services, Goodman required Plaintiff Smallwood to provide it with her PHI.

75. Upon information and belief, Plaintiff Smallwood's PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

76. Plaintiff Smallwood believed, as part of the payments to Goodman for medical treatment and services, that those payments included amounts for adequate data security. Had Plaintiff Smallwood known that Goodman did not utilize reasonable data security measures, she would have paid less for her treatments and services or would not have provided Goodman with her PHI.

77. Plaintiff Smallwood will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft resulting from her PHI being posted to the dark web.

78. Plaintiff Smallwood's sensitive PHI remains in Goodman's possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm in the event Goodman suffers another data breach.

79. Plaintiff Smallwood is very careful about sharing her PHI. She has never knowingly transmitted unencrypted PHI over the internet or any other unsecured source.

80. Plaintiff Smallwood stores any documents containing her PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

81. Plaintiff Smallwood suffered actual injury in the form of damages to and diminution in the value of her PHI—a form of intangible property that Plaintiff Smallwood entrusted to Defendant for the purpose of medical care, which was compromised in and as a result of the Data Breach.

82. Plaintiff Smallwood suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

83. Plaintiff Smallwood is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PHI, especially her Social Security number and

sensitive medical information, in combination with her name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PHI.

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

Plaintiff Spencer

85. Plaintiff Spencer is a former Goodman patient.

86. As a condition of receiving Goodman's medical treatment and services, Goodman required Plaintiff Spencer to provide it with her PHI.

87. Upon information and belief, Plaintiff Spencer's PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

88. Plaintiff Spencer believed, as part of the payments to Goodman for medical treatment and services, that those payments included amounts for adequate data security. Had Plaintiff Spencer known that Goodman did not utilize reasonable data security measures, she would have paid less for her treatments and services or would not have provided Goodman with her PHI.

89. Plaintiff Spencer will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft resulting from her PHI being posted to the dark web.

90. Plaintiff Spencer's sensitive PHI remains in Goodman's possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm in the event Goodman suffers another data breach.

91. Plaintiff Spencer is very careful about sharing her PHI. She has never knowingly transmitted unencrypted PHI over the internet or any other unsecured source.

92. Plaintiff Spencer stores any documents containing her PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

93. Plaintiff Spencer suffered actual injury in the form of damages to and diminution in the value of her PHI—a form of intangible property that Plaintiff Ham entrusted to Defendant for the purpose of medical care, which was compromised in and as a result of the Data Breach.

94. Plaintiff Spencer suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

95. Plaintiff Spencer is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PHI, especially her Social Security number and sensitive medical information, in combination with her name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PHI.

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

Plaintiff Hostetter

97. Plaintiff Hostetter is a former Goodman patient.

98. As a condition of receiving Goodman's medical treatment and services, Goodman required Plaintiff Hostetter to provide it with her PHI.

99. Upon information and belief, Plaintiff Hostetter's PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

100. Plaintiff Hostetter believed, as part of the payments to Goodman for medical treatment and services, that those payments included amounts for adequate data security. Had Plaintiff Hostetter known that Goodman did not utilize reasonable data security measures, she would have paid less for her treatments and services or would not have provided Goodman with her PHI.

101. Plaintiff Hostetter will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft resulting from her PHI being posted to the dark web.

102. Indeed, Plaintiff Hostetter and her husband have spent approximately twelve hours monitoring her accounts and records for fraudulent or suspicious charges. Plaintiff Hostetter

changed her banking and credit card passwords, recognizing the real and immediate risk of identity theft and fraud stemming from the Data Breach and her PHI being placed on the dark web.

103. Plaintiff Hostetter's sensitive PHI remains in Goodman's possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm in the event Goodman suffers another data breach.

104. Plaintiff Hostetter is very careful about sharing her PHI. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

105. Plaintiff Hostetter stores any documents containing her PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

106. Plaintiff Hostetter suffered actual injury in the form of damages to and diminution in the value of her PHI—a form of intangible property that Plaintiff Hostetter entrusted to Defendant for the purpose of medical care, which was compromised in and as a result of the Data Breach.

107. Plaintiff Hostetter suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

108. Plaintiff Hostetter is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PHI, especially her Social Security number and sensitive medical information, in combination with her name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PHI.

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

Plaintiff Powers

110. Plaintiff Powers is a former Goodman patient.

111. As a condition of receiving Goodman's medical treatment and services, Goodman required Plaintiff Powers to provide it with her PHI.

112. Upon information and belief, Plaintiff Powers' PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

113. Plaintiff Powers believed, as part of the payments to Goodman for medical treatment and services, that those payments included amounts for adequate data security. Had Plaintiff Powers known that Goodman did not utilize reasonable data security measures, she would have paid less for her treatments and services or would not have provided Goodman with her PHI.

114. Plaintiff Powers will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft resulting from her PHI being posted to the dark web. Plaintiff Powers frequently monitors her accounts and statements to identify fraudulent and suspicious charges.

115. Plaintiff Powers has already suffered from identity theft and fraud resulting from the Data Breach. In reviewing her credit card statement, Plaintiff Powers discovered a fraudulent charge from an unfamiliar business. Plaintiff Powers spent resources contacting her credit card company to dispute the charge.

116. Plaintiff Powers' sensitive PHI remains in Goodman's possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm in the event Goodman suffers another data breach.

117. Plaintiff Powers is very careful about sharing her PHI. She has never knowingly transmitted unencrypted PHI over the internet or any other unsecured source.

118. Indeed, since the Data Breach, Plaintiff Powers has activated credit monitoring theft protection services to protect herself from further unauthorized use of her PHI. Plaintiff Powers also placed a freeze on her credit.

119. Plaintiff Powers stores any documents containing her PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts and changes the passwords regularly.

120. Plaintiff Powers suffered actual injury in the form of damages to and diminution in the value of her PHI—a form of intangible property that Plaintiff Powers entrusted to Defendant for the purpose of medical care, which was compromised in and as a result of the Data Breach.

121. Plaintiff Powers suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

122. Plaintiff Powers is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PHI, especially her Social Security number and sensitive medical information, in combination with her name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PHI.

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

Plaintiff Perdue

124. Plaintiff Perdue first visited Defendant's facility for medical care in July 2021 and last visited Defendant's facility in August of 2021. As a condition of receiving medical care, Plaintiff was required to provide, without limitation, his name, date of birth, address, telephone number, email addresses, medical record number, patient account number, diagnosis and treatment information, physician name, insurance information, date(s) of service, and Social Security number.

125. Upon information and belief, Plaintiff Perdue's PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

126. On or around July 26, 2022, Plaintiff Perdue received a Notice of Data Breach from Defendant. The letter was dated July 19, 2022 and stated that Plaintiff Perdue's information was compromised in the Data Breach.

127. As a result of the Data Breach, Plaintiff Perdue spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, time spent attempting to file police reports with his local police department, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, attempting to enroll and enrolling in the credit monitoring and identity theft protection services offered by Defendant, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

128. Plaintiff Perdue has suffered actual damages in the form of identity theft. Since the Data Breach, Mr. Perdue has received text messages from PayPal stating that his account has been frozen. Mr. Perdue does not have a PayPal account.

129. Further, Plaintiff Perdue has experienced an uptick in phone calls alleging to be from doctors' offices in his area and asking Plaintiff Perdue to verify information about his insurance, home address, and other personal, sensitive information. Plaintiff Perdue's PHI is more than likely still unlawfully in the hands of third-parties.

130. Plaintiff Perdue is very careful about sharing his PHI. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

131. Plaintiff Perdue stores any documents containing his PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

132. Plaintiff Perdue suffered actual injury in the form of damages to and diminution in the value of his PHI—a form of intangible property that Plaintiff Perdue entrusted to Defendant for the purpose of medical care, which was compromised in and as a result of the Data Breach.

133. Plaintiff Perdue suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

134. Plaintiff Perdue has also suffered an increase in spam calls, texts, and emails. These spam calls/texts/emails and phishing attempts have become so frequent and incessant that Plaintiff Perdue has considered changing his phone number.

135. Plaintiff Perdue is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PHI, especially his Social Security number and sensitive medical information, in combination with his name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PHI.

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

Plaintiff Goff

137. Plaintiff Goff is a former Goodman patient.

138. As a condition of receiving Goodman's medical treatment and services, Goodman required Plaintiff Goff to provide it with her PHI.

139. Upon information and belief, Plaintiff Goff's PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

140. Plaintiff Goff believed, as part of the payments to Goodman for medical treatment and services, that those payments included amounts for adequate data security. Had Plaintiff Goff known that Goodman did not utilize reasonable data security measures, she would have paid less for her treatments and services or would not have provided Goodman with her PHI.

141. Plaintiff Goff will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft resulting from her PHI being posted to the dark web.

142. Plaintiff Goff purchased Identity Guard for roughly $200 due to her information being on the Dark Web as a result of the Data Breach.

143. Plaintiff Goff made other reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, an/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Goff spent roughly 5 hours on mitigation efforts and will continue to spend valuable time monitoring her accounts for suspicious activity.

144. Plaintiff Goff's sensitive PHI remains in Goodman's possession without adequate protection against known threats, exposing her to the prospect of additional harm in the event Goodman suffers another data breach.

145. Plaintiff Goff is very careful about sharing her PHI. She has never knowingly transmitted unencrypted PHI over the internet or any other unsecured source.

146. Plaintiff Goff stores any documents containing her PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

147. Plaintiff Goff suffered actual injury in the form of damages to and diminution in the value of her PHI—a form of intangible property that Plaintiff Goff entrusted to Defendant for

the purpose of medical care from Defendant, which was compromised in and as a result of the Data Breach.

148. Plaintiff Goff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

149. Plaintiff Goff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PHI, especially her Social Security number and sensitive medical information, in combination with her name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PHI.

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

Plaintiff Gilland

151. Plaintiff Gilland has visited Goodman facilities for medical evaluation and treatment of her three minor children, referred to herein as A.G., B.G., and C.G., since at least 2013.

152. As a condition of receiving Goodman's medical treatment and services, Goodman required Plaintiff Gilland to provide it with both her and her children's PHI.

153. Upon information and belief, Plaintiff Gilland's and her children's PHI was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

154. Plaintiff Gilland believed, as part of the payments to Goodman for medical treatment and services, that those payments included amounts for adequate data security. Had Plaintiff Gilland known that Goodman did not utilize reasonable data security measures, she would have paid less for her treatments and services or would not have provided Goodman with her or her children's PHI.

155. Plaintiff Gilland will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself and her children from identity theft resulting from her and their PHI being posted to the dark web.

156. Indeed, Plaintiff Gilland has already suffered damages in the form of identity theft resulting from the Data Breach. Plaintiff Gilland experienced fraudulent activity on her PayPal account in early July 2022. Plaintiff Gilland was notified that someone was attempting to transfer money from her account. Plaintiff called PayPal and spent significant time attempting to halt the transfers.

157. Further, after receiving Goodman's notice of the Data Breach on or about July 19, 2022, Plaintiff Gilland began receiving threatening debt collection notices for accounts and transactions she had no involvement with, and Plaintiff Gilland was forced to take time to contest these fraudulent debt collection attempts. Plaintiff Gilland also received a substantially similar notice from Goodman for each of her three children, A.G., B.G., and C.G.

158. Plaintiff Gilland made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letters, including but not limited to researching the Data Breach and offered credit monitoring, reviewing her records from Goodman, contacting PayPal to halt the fraudulent transfers, and researching and contesting the fraudulent debt collection notices she received as a consequence of the Data Breach.

159. Plaintiff Gilland has spent roughly 10 hours on activity related to the Data Breach and she will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

160. Plaintiff Gilland's and her children's sensitive PHI remains in Goodman's possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm in the event Goodman suffers another data breach.

161. Plaintiff Gilland is very careful about sharing her PHI and the PHI of her children. She has never knowingly transmitted unencrypted PHI over the internet or any other unsecured source.

162. Plaintiff Gilland stores any documents containing her and her children's PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

163. Plaintiff Gilland suffered actual injury in the form of damages to and diminution in the value of her PHI—a form of intangible property that Plaintiff Gilland entrusted to Defendant for the purpose of medical care, which was compromised in and as a result of the Data Breach.

164. Plaintiff Gilland suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

165. Plaintiff Gilland and her children are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PHI, especially her and her children's Social Security numbers and sensitive medical information, in combination with their names, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's and her children's PHI.

166. Plaintiff Gilland has a continuing interest in ensuring that her and her children's PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

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

167. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PHI that can be directly traced to Defendant.

168. The ramifications of Defendant's failure to keep Plaintiffs' and the Class's PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

169. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[7]

170. As a result of Defendant's failure to prevent—and to timely detect—the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PHI is used;

[7] Anne Saita, *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

b. The diminution in value of their PHI;

c. The compromise and continuing publication of their PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PHI; and

h. The continued risk to their PHI, which remains in the possession of Goodman and is subject to further breaches so long as Goodman fails to undertake the appropriate measures to protect the PHI in their possession.

171. Stolen PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to $1,000.00 depending on the type of information obtained.[8]

172. The value of Plaintiffs' and the proposed Class's PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

173. It can take victims years to spot identity theft, giving criminals plenty of time to milk stolen PHI for cash.

174. One such example of criminals using PHI for profit is the development of "Fullz" packages.[9]

---

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

[9] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule

175. Cyber-criminals can cross-reference multiple sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

176. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI 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 members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

177. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

178. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and the Class that their PHI had been stolen.

179. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

180. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their

---

account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecurity.com/tag/fullz/.

reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

181. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

182. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[10]

183. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[11] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[12]

184. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[13] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

---

[10] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

[11] *Start With Security, A Guide for Business*, FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[12] *Id.*

[13] *See* Taking Charge, What to Do If Your Identity is Stolen, FED. TRADE COMM'N 3 (2012), https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

185. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Goodman thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PHI.

186. The healthcare industry is a prime target for data breaches.

187. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[14] The next year, that number increased by nearly 45%.[15] The following year, the healthcare sector was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach.[16]

---

[14] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"] (last accessed June 10, 2022).

[15] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, ITRC (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"] (last accessed June 10, 2022).

[16] *2018 End-of-Year Data Breach Report*, ITRC (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

188. Data breaches within the healthcare industry continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[17]

189. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[18] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[19] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[20]

190. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers."[21]

191. Charged with handling highly sensitive PHI including healthcare information, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the PHI that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's patients and employees as a result of a breach. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[17] *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), https://bit.ly/3LJqUr6.

[18] *2018 End-of-Year Data Breach Report*, *supra* note 14.

[19] Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), https://cnet.co/33uiV0v.

[20] *Id.*

[21] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08.

192. Defendant disclosed the PHI of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PHI of Plaintiffs and members of the proposed Class 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 PHI.

193. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PHI of Plaintiffs and members of the proposed Class to unscrupulous operators, con artists and outright criminals.

194. Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' and Class members' injuries by depriving them of the earliest ability to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

D. Goodman Failed to Adhere to HIPAA

195. 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.[22]

196. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.[23]

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

---

[22] 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.

[23] *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).

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);

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 Goodman'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).

E. Goodman Failed to Adhere to FTC Guidelines

198. According to the FTC, the need for data security should be factored into all business decision-making.[24] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Goodman, should employ to protect against the unlawful exposure of Personal Information.

[24] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed June 10, 2022).

199. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[25] The guidelines explain that businesses should:

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.

200. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

201. The FTC recommends that companies not maintain PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

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

203. Goodman's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient and employees' PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

204. Plaintiffs bring this action on behalf of themselves, and all members of the proposed Class (the "Class") as defined as:

> All citizens of the State of Indiana whose PHI was accessed without authorization in the Data Breach.

---

[25] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed June 10, 2022).

[26] *See Start with Security*, *supra* note 22.

205. The following people are excluded from the Class: (1) any judge or magistrate residing over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

206. The Class defined above is identifiable through Defendant's business records.

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

208. This action is properly maintainable as a class action under Indiana Rules of Trial Procedure 23(A) and (B)(3).

209. **Numerosity.** Plaintiffs are representative of the proposed Class, consisting of thousands of members, far too many to join in a single action.

210. **Commonality.** There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether Defendant breached its contractual promises to safeguard Plaintiffs' and Class members' PHI;

b. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PHI;

c. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiffs' and members of the Class's PHI from unauthorized release and disclosure;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

e. Whether Defendant's delay in informing Plaintiffs and members of the Class of the Data Breach was unreasonable;

f. Whether Defendant's method of informing Plaintiffs and other members of the Class of the Data Breach was unreasonable;

g. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PHI violated applicable state laws;

h. Whether Plaintiffs and members of the Class were injured as a proximate cause or result of the Data Breach;

i. Whether Plaintiffs and members of the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiff and members of the Class

j. What the proper measure of damages is; and

k. Whether Plaintiffs and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

211. **Typicality**. Plaintiffs' claims are typical of the claims of other members of the Class in that Plaintiffs, and the members of the Class sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiffs and members of the Class sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

212. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiffs.

213. **Superiority of Class Action**. A class action is also a fair and efficient method of adjudicating the controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale,

and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

214. A class action is therefore superior to individual litigation because:

a. The amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

215. The litigation of the claims brought herein is manageable. Goodman's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

216. Adequate notice can be given to Class members directly using information maintained in Goodman's records.

217. **Predominance.** Pursuant to Rule 23(B)(3), the issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include but are not limited to the questions identified above.

218. This proposed class action does not present any unique management difficulties.

FIRST CAUSE OF ACTION
Negligence
(on behalf of Plaintiffs and the Class)

219. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

95. Defendant collected, and maintained Plaintiffs' and the Class's PHI for the purpose of providing medical treatment to Plaintiffs and the Class. Defendant is a for profit corporation, thereby deriving revenue directly from its ability to provide medical services to patients.

96. Plaintiffs and the Class are a well-defined, foreseeable, and probable group who Defendant was aware, or should have been aware, could be injured by inadequate data security measures. The nature of Defendant's business requires patients to disclose PHI to receive adequate care, including, but not limited to, medical histories, dates of birth, addresses, phone numbers, and medical insurance information. Thus, for Defendant to provide its services, it must use, handle, gather, and store the PHI of Plaintiffs and the Class and, additionally, solicit and create records containing Plaintiffs' and the Class's sensitive information.

97. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or should have known that, given its repository of a host of PHI for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiffs and the Class of inadequate data security created a duty to act reasonably and safeguard the PHI.

98. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their PHI in its possession from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

99. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiffs' and the Class's PHI was adequately protected and secured. Defendant further had a duty to implement processes that would detect a breach of their security system in a timely manner.

100. Defendant also had a duty to timely disclose to Plaintiffs and the Class that their PHI had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that, among other things, Plaintiffs and the Class could take appropriate measures to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts, and take any other appropriate precautions, including those recommended by Defendant.

101. The Indiana Data Breach Notification Statute requires Defendant to notify affected individuals and the Attorney General of a data breach without unreasonable delay, but no later than forty-five (45) days after discovery of the breach.[27] Ind. Code 24-4.9-3-3 (July 1, 2022).

102. Additionally, HIPAA creates industry standards for maintaining the privacy of health-related data. Defendant knew or should have known it had a legal obligation to secure and protect Plaintiffs' and the Class's sensitive information and that failing to do so is a serious violation of HIPAA.

103. Defendant also should have known that, given the PHI it held, Plaintiffs and the Class would be harmed should it suffer a Data Breach. Defendant knew or should have known that their systems and technologies for processing and securing Plaintiffs' and the Class's PHI had security vulnerabilities susceptible to cyber-attacks.

104. Despite that knowledge, Defendant implemented unreasonable data security measures that allowed cybercriminals to successfully breach Defendant's network and data environments, reside there undetected for a significant period of time, and access or steal a host of personal and healthcare information on thousands of Defendants' patients.

105. Defendant, through its actions and/or omissions, failed to provide reasonable security for the data in its possession.

106. Defendant breached is duty to Plaintiffs and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their PHI, allowing unauthorized access to Plaintiffs' and the Class's PHI, and failing to recognize the Data Breach in a timely manner. Defendant further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class's PHI.

107. But for Defendant's wrongful and negligent breach of its duties, their PHI would not have been accessed and exfiltrated by unauthorized persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

108. As a result of Defendant's negligence, Plaintiffs and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely

[27] Indiana passed HB 1351 in March 2022, amending Indiana's data breach notification law to include the "but not more than forty-five (45) days after the discovery of the breach" language.

to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; irrecoverable financial losses due to fraud; loss of value of their PHI; overpayment for Defendant's services; and the value of identity protection services made necessary by the Data Breach.

SECOND CAUSE OF ACTION
Negligence *Per Se* (15 U.S.C. § 45)
(on behalf of Plaintiffs and the Class)

109. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

110. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PHI. Various FTC publications and orders also form the basis of Defendant's duty.

111. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's PHI and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PHI it obtained and stored and the foreseeable consequences of a data breach.

112. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

113. Plaintiffs and the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

114. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the proposed Class.

115. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have been injured as described herein and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Negligence *Per Se* (HIPPA, 45 C.F.R. § 160.102)
(on behalf of Plaintiffs and the Class)

116. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

117. Defendant required Plaintiffs and the Class to provide nonpublic PHI to obtain medical services. During the provision of those services, Defendant created and stored even more PHI.

118. As a healthcare provider, Defendant is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

119. HIPAA, 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information."

120. Per 45 C.F.R. § 164.306, HIPAA "standards, requirements and implementation specifications" apply to covered entities, such as Defendant. HIPAA standards are mandatory.

121. HIPAA requires Defendant to "ensure the confidentiality, integrity, and availability of all electronic protected health information" it receives and to protect against any "reasonably anticipated threats or hazards to the security or integrity" of the Sensitive Information. 45 C.F.R. § 164.306.

122. Defendant violated HIPAA by failing to adhere to and meet the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

123. Additionally, HIPAA requires timely notice of data breaches to each impacted consumer and defines timely as "in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. § 164.404. The notice must include certain minimum information, including, but not limited to a description of what the entity is doing to investigate the breach and mitigate harm. *Id.*

124. Defendant breached its HIPAA's notification duty by failing to give timely and complete notice. Defendant waited approximately two months from the date it was made aware of

the Data Breach to begin sending notices to victims and the notices did not include any explanation of what the company was doing to mitigate harm.

125. Defendant violated HIPAA by failing to use reasonable measures to protect the PHI of Plaintiffs and Class. Defendant's conduct was especially unreasonable given the nature of the PHI and the number of patients it serves, some of which are minors or patients who live below the federal poverty level, who may not have the means to expend significant amounts of time and money to fully mitigate the fallout of the Data Breach.

126. Defendant's violation of HIPAA constitutes negligence *per se*. Plaintiffs and the Class are within the group of individuals HIPAA was designed to protect and the harm to these individuals is a result of the Data Breach.

127. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members suffered and continue to suffer injuries and are entitled to damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Breach of an Implied Contract
(On Behalf of Plaintiffs and the Class)

128. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

129. Defendant offered to provide goods and services to Plaintiffs and members of the Class in exchange for payment and/or offered to provide employment to certain members of the Class.

130. Defendant required Plaintiffs and the members of the Class to provide Defendant with their PHI in order to receive medical treatment and services.

131. Defendant required its current and former employees to provide Defendant with their PHI in order to receive employment.

132. In turn, Defendant agreed it would not disclose the PHI it collects from patients and employees to unauthorized persons. Defendant also promised to maintain safeguards to protect its patients' and employees' PHI.

133. Plaintiffs and the members of the Class accepted Defendant's offer by providing PHI to Defendant in exchange for receiving Defendant's goods and services and then by paying

for and receiving the same, and Defendant's current and former employees in the Class accepted Defendant's offer by providing PHI to Defendant in exchange for employment.

134. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their PHI.

135. Plaintiffs and the members of the Class would not have entrusted their PHI to Defendant in the absence of such agreement with Defendant.

136. Defendant materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its e-mail systems that compromised such information. Defendant further breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's PHI;
b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and
c. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

137. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

138. Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

139. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

140. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

141. Defendant had an implied duty to reasonably safeguard and protect the PHI of Plaintiffs and Class members from unauthorized disclosure or uses.

142. Additionally, Defendant implicitly promised to retain this PHI only under conditions that kept such information secure and confidential.

143. Plaintiffs and Class members fully performed their obligations under the implied contract with Defendant. Defendant did not. Plaintiffs and Class members would not have provided their confidential PHI to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PHI for uses other than medical treatment, billing, and benefits from Defendant.

144. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

145. In these and other ways, Defendant violated its duty of good faith and fair dealing.

146. Plaintiffs and members of the Class have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

FIFTH CAUSE OF ACTION
VIOLATION OF INDIANA DECEPTIVE CONSUMER SALES ACT,
Ind. Code §§ 24-5-0.5-1, *et seq.*

147. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

148. Defendant is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

149. Defendant is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

150. Defendant engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

151. Defendant's representations and omissions include both implicit and explicit representations through:

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

b. Failing to identify and remediate foreseeable security and privacy risks and adequately maintain security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Class's PHI, including duties imposed by the HIPAA, 45 C.F.R. § 160.102 and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class's sensitive information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class's PHI, including duties imposed by the HIPAA, 45 C.F.R. § 160.102;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class's sensitive information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class's PHI, including duties imposed by HIPAA, 45 C.F.R. §160.102 or the FTC Act, 15 U.S.C. § 45.

152. Defendant's acts and practices were "unfair" because they caused or were likely to cause substantial injury to patients which was not reasonably avoidable by patients themselves and not outweighed by countervailing benefits to patients or to competition.

153. The injury to patients from Defendant's conduct was and is substantial because it was nontrivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their PHI.

154. Plaintiffs and the Class could not have reasonably avoided injury because Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of patient healthcare decision-making. By withholding important information from patients about the inadequacy of its data security, Defendant created an asymmetry of

information between it and patients that precluded patients from taking action to avoid or mitigate injury.

155. Defendant also engaged in "deceptive" acts and practices in violation of Ind. Code §24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have; and

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not.

156. Had Defendant disclosed to Plaintiffs and the Class that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant was trusted with sensitive and valuable PHI regarding hundreds of thousands of patients, including Plaintiffs and the Class. Defendant accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the Class acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

157. Defendant had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PHI in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Defendant and Plaintiffs and the Class as described herein.

158. As a direct and proximate result of Defendant's unfair, abusive, and deceptive acts or practices, Plaintiffs and the Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PHI; overpayment for Defendant's services; and the value of identity protection services made necessary by the Data Breach.

159. Plaintiffs and the Class seek all relief allowed by law, including the greater of actual damages or $500 for each violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

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

160. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

161. Plaintiffs and the Class had a legitimate expectation of privacy to their PHI, which contained intimate details about the physical characteristics and lives of Plaintiffs and the Class and were entitled to the protection of this information against disclosure and/or publication to unauthorized third parties.

162. Defendant owed a duty to its current and former patients and/or employees, including Plaintiffs and the Class, to keep their PHI contained as a part thereof, confidential.

163. Defendant failed to protect and released to unknown and unauthorized third parties the PHI of Plaintiffs and the Class.

164. Defendant allowed unauthorized and unknown third parties access to and examination of the PHI of Plaintiffs and the Class, by way of Defendant's failure to protect the PHI.

165. The unauthorized release to, custody of, and examination by unauthorized third parties of the PHI of Plaintiffs and the Class is highly offensive to a reasonable person, especially considering the sensitive nature of the personal and medical information at issue.

166. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their PHI to Defendant as part of Plaintiffs and the Class's relationships with Defendant, but privately with an intention that the PHI would be kept confidential and would be 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.

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

168. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

169. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

170. As a proximate result of the above acts and omissions of Defendant, the PHI of Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

171. 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 in that the PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

SEVENTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

172. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

173. Plaintiffs and Class members gave Defendant their PHI in confidence, believing that Defendant would protect that information. Plaintiffs and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class members' PHI created a fiduciary relationship between Defendant and Plaintiffs and Class members. In light of this relationship, Defendant must act primarily for the benefit of its patients, former patients, and employees, which includes safeguarding and protecting Plaintiffs' and Class Members' PHI.

174. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' PHI that it collected.

175. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i)

a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recove1y from unauthorized use of their PHI; (iv) lost opportunity costs associated with attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PHI compromised as a result of the Data Breach; and {vii) overpayment for the services that were received without adequate data security.

EIGHTH CAUSE OF ACTION
BAILMENT
(on behalf of Plaintiffs and the Class)

176. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

177. Plaintiffs and the Class provided, or authorized disclosure of, their PHI to Defendant.

178. In allowing their PHI to be made available to Defendant, Plaintiffs and the Class intended and understood that Defendant would adequately safeguard their PHI.

179. For its own benefit, Defendant accepted possession of Plaintiffs' and the Class's PHI.

180. By accepting possession of Plaintiffs' and the Class's PHI, Defendant understood that Plaintiffs and the Class expected Defendant to adequately safeguard their PHI. Accordingly, bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their personal information.

181. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs and' the Class's personal information, resulting in the unlawful and unauthorized access to and misuse of their PHI.

182. As a direct and proximate result of Defendant's breach of its duty, Plaintiffs and Class Members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth above.

183. As a direct and proximate result of Defendant's breach of its duties, the personal information of Plaintiffs and the Class entrusted, directly or indirectly, to Defendant during the bailment (or deposit) was damaged and its value diminished.

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

184. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

185. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

186. Plaintiffs and members of the Class that are current or former patients of Defendant conferred a monetary benefit upon Defendant in the form of monies paid for treatment services.

187. Current and former employees of Defendant that are members of the Class conferred a benefit upon Defendant in the form of services through employment.

188. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class. Defendant also benefited from the receipt of Plaintiffs' and members of the Class's PHI, as this was used to facilitate patient payment and treatment services, and to facilitate their employment.

189. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that Plaintiffs and members of the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

190. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

TENTH CAUSE OF ACTION
Declaratory Judgment
(on behalf of Plaintiffs and the Class)

191. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

192. Pursuant to Ind. Code § 34-14-1-2 Courts of record within their respective jurisdiction have the power to declare rights, status, and other legal relations, whether or not further relief is or could be claimed. Further, this Court has the power to declare either affirmative or negative decrees in form and effect, such as restraining acts that violate the laws described in this Complaint.

193. Whether Defendant's actions caused the Data Breach and its subsequent harm to Plaintiffs and the Class, and whether Defendant is presently maintaining adequate data security measure to safeguard Plaintiffs and the Class from further data breaches is an actual controversy.

194. Plaintiffs and the Class are at a substantial and imminent risk of further compromise of their PHI. This is true irrespective of whether Plaintiffs and the Class are current patients of Defendant because Defendant still maintains as swath of Plaintiffs' and the Class's PHI.

195. Pursuant to its authority under the Ind. Code Ann. § 34-14-1-1, this Court should enter a judgment declaring the following:

a. Defendant owed a legal duty, at the time of the Data Breach, to Plaintiffs and members of the proposed Class to reasonably protect and secure their PHI under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

b. Defendant owed a legal duty to Plaintiffs and members of the proposed Class to provide timely notice of the Data Breach under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

c. Defendant continues to owe a legal duty to Plaintiffs and members of the proposed Class to protect and secure their sensitive information under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

d. Defendant continues to owe a legal duty to Plaintiffs and members of the proposed Class to provide timely notice of data breaches under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b).

196. Defendant continues to breach its legal duties by failing to employ reasonable measures to protect and secure Plaintiffs' and the putative Class members' PHI, including that of new patients who are without notice of the Data Breach.

ELEVENTH CAUSE OF ACTION
Injunctive Relief
(on behalf of Plaintiffs and the Class)

197. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

198. Pursuant to Ind. Code Title 34 § 34-24-26, the court may grant restraining orders and injunctions when a complaint alleges Defendant's actions or omissions will continue to produce great injury to the Plaintiffs and members of the Class.

199. Without the injunctive relief requested herein, Plaintiffs and the Class will suffer irreparable harm, and lack an adequate remedy at law, if Defendant is breached again. The risk of additional data breaches in the future is not hypothetical, but instead, it is real, immediate, and substantial. If Defendant is breached again, Plaintiffs and the Class will lack an adequate legal remedy because the resulting injuries may not be readily quantifiable. Additionally, Plaintiffs and the Class will have to bring additional, future lawsuits to rectify the same conduct alleged herein.

200. The Court should enter an order enjoining Defendant from engaging in the wrongful and unlawful acts described herein and require:

a. Defendant to protect all PHI collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

b. Defendant to protect all data collected through the course of its business in accordance with HIPAA;

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

d. Defendant to run security monitoring, and conduct regular database scanning and securing checks;

e. Defendant to train and assess its personnel on new or modified security procedures through education programs, policies, and tests;

f. Defendant to fully disclose the extent and nature of the security breach and theft; and

g. Defendant to pay for, not less than three years, identity theft and credit monitoring services for Plaintiffs and the Class.

201. Defendant is required by law to employ reasonable safety measures for storing PHI. The cost of complying with this legal obligation, and the injunctive relief requested herein, is marginal when compared to the hardship Plaintiffs and the Class will likely suffer if another breach occurs, including but not limited to, fraud and identity theft.

202. The requested injunctive relief will serve the public interest by mitigating the risk of future data breaches, thereby decreasing or eliminating the possibility of future harm to Plaintiffs, the Class, and new patients of Defendant.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, on behalf of themselves and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives and the undersigned as Class counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the PHI of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PHI to unauthorized persons;

D. A mandatory injunction enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PHI;

E. An award of damages, in an amount to be determined;

F. An award of attorneys' fees and costs;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: May 1, 2023

Respectfully submitted,

/s/Katherine A. Franke
Katherine A. Franke (Atty No. 26280-03)
BROADWING LEGAL
429 E. Vermont Street, Suite 013
Indianapolis, IN 46202
T: (317)854-3388
F: (317) 854-3308
kate@broadwinglegal.com

J. Gerard Stranch, IV (Atty No. 7611-95-TA)
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC[28]
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel.: (615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

Interim Lead Class Counsel

Samuel J. Strauss*
Raina C. Borrelli (Atty No. 8588-95-TA)
Alex Phillips *
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
T: (608) 237-1775
F: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com
alexp@turkestrauss.com

Jean Martin
Francesca Kester
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor

[28] Formerly Branstetter, Stranch & Jennings, PLLC

Tampa, Florida 33602
Phone: (813) 559-4908
jeanmartin@forthepeople.com
fkester@forthepeople.com

Scott L. Starr, I.D. #1601-09
Andrew B. Miller, I.D. #18795-45
STARR AUSTEN & MILLER, LLP
201 South Third Street
Logansport, IN 46947
Telephone: (574) 722-6676
Facsimile: (574) 753-3299
starr@starrausten.com
miller@starrausten.com

Brian C. Gudmundson*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
rachel.tack@zimmreed.com

Brandon E. Tate, Atty. No. 31531-49
Katherine A. Piscione, Atty. No. 37166-49
WALDRON TATE BOWEN SPANDAU LLC
156 E Market St, 5th Floor
Indianapolis, IN 46204
317.296.5294
F: 317.423.0772
brandon@wtbs-law.com
katie@wtbs-law.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Kathleen A. DeLaney (#18604-49)
Matthew R. Gutwein (#16414-49)
DELANEY & DELANEY LLC
3646 North Washington Blvd.
Indianapolis, Indiana 46205
Telephone: (317) 920-0400
kathleen@delaneylaw.net
mgutwein@delaneylaw.net

Jeffrey S. Goldenberg
Todd B. Naylor
Robert B. Sherwood
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com
rsherwood@gs-legal.com

Charles E. Schaffer
LEVIN, SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com

Joseph M. Lyon*
THE LYON FIRM, LLC
2754 Erie Ave.
Cincinnati, OH 45208
Tel: 513.381.2333
jlyon@thelyonfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Tel: 513.651-3700.5442
TCoates@msdlegal.com

Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

* to seek admission *pro hac vice*

Counsel for the Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I certify that the foregoing has been served upon the following counsel of record by email using the Indiana E-Filing System (IEFS), on May 1, 2023:

Philip r. Zimmerly
Bose McKinney & Evans LLP
111 Monument Circle, Suite 2700
Indianapolis, IN 46204
pzimmerly@boselaw.com

Paul G. Karlsgodt
Michelle R. Gomez
Baker Hostetler LLP
1801 California Street, Suite 4400
Denver, CO 80202
pkarlsgodt@bakerlaw.com
mgomez@bakerlaw.com

J. Gerard Stranch, IV
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel.: (615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss*
Raina C. Borrelli
Alex Phillips *
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
T: (608) 237-1775
F: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com
alexp@turkestrauss.com

Jean Martin
Francesca Kester
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, Florida 33602

Phone: (813) 559-4908
jeanmartin@forthepeople.com
fkester@forthepeople.com

Scott L. Starr, I.D. #1601-09
Andrew B. Miller, I.D. #18795-45
STARR AUSTEN & MILLER, LLP
201 South Third Street
Logansport, IN 46947
Telephone: (574) 722-6676
Facsimile: (574) 753-3299
starr@starrausten.com
miller@starrausten.com

Brian C. Gudmundson*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
rachel.tack@zimmreed.com

Brandon E. Tate, Atty. No. 31531-49
Katherine A. Piscione, Atty. No. 37166-49
WALDRON TATE BOWEN SPANDAU LLC
156 E Market St, 5th Floor
Indianapolis, IN 46204
317.296.5294
F: 317.423.0772
brandon@wtbs-law.com
katie@wtbs-law.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Kathleen A. DeLaney (#18604-49)

Matthew R. Gutwein (#16414-49)
DELANEY & DELANEY LLC
3646 North Washington Blvd.
Indianapolis, Indiana 46205
Telephone: (317) 920-0400
kathleen@delaneylaw.net
mgutwein@delaneylaw.net

Jeffrey S. Goldenberg
Todd B. Naylor
Robert B. Sherwood
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com
rsherwood@gs-legal.com

Charles E. Schaffer
LEVIN, SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com

Joseph M. Lyon*
THE LYON FIRM, LLC
2754 Erie Ave.
Cincinnati, OH 45208
Tel: 513.381.2333
jlyon@thelyonfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Tel: 513.651-3700.5442
TCoates@msdlegal.com

Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100

Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

/s/Katherine A. Franke
Katherine A. Franke