UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: HEALTHEC LLC DATA BREACH LITIGATION	Case No. 2:24-cv-00026-JKS-CLW

CONSOLIDATED CLASS ACTION COMPLAINT

Beatriz Castillo Benitez, Allan Bishop, Lisa Bryson, Caroline Cappas, Kristel De Verona, Jane Doe, Jessica Fenn, Keith Fielder, Joni Fielder, Gregory Leeb, Mindy Markowitz, Abbey Robinson, J (minor son of Abbey Robinson), and Della Vallejo, ("Plaintiffs"), and on behalf of all others similarly situated ("Class Members"), bring this Consolidated Class Action Complaint against Defendants HealthEC, LLC ("HealthEC"), Community Health Care Systems, Inc. ("Community Health Care Systems"), Corewell Health d/b/a Corewell ("Corewell"), MD Valuecare, LLC ("MD Valuecare"), and Oakwood Accountable Care Organization, LLC d/b/a Beaumont ACO ("Beaumont") (together "Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendants' failure to protect the highly sensitive data of 4,656,293 Class Members.[1]

2. Defendant HealthEC is a business that sells data management and data analytics services to healthcare providers.[2] For example, HealthEC advertises its "integrated population health management (PHM) platform" which provides "comprehensive analytics and integrated, role-based tools[.]"[3]Through its PHM platform, HealthEC uses patients' personal information and data analytics to, among other things, create automated care plans, identify at risk-patients, centralize electronic patient data, and share data amongst patients' care teams.[4]

3. Defendant HealthEC partners with healthcare providers, including Defendants Beaumont, Corewell, Community Health Care Systems, and MD Valuecare ("Provider Defendants") to provide its PHM services.[5] Under these

---

[1] *Cases Currently Under Investigation*, DEPT HEALTH & HUMAN SERVS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=314987482344F3763E7B56F48A814824 (last visited April 10, 2024).
[2] *Home Page*, HEALTHEC, https://healthec.com/ (last visited April 10, 2024).
[3] *Id*.
[4] *What We Do*, HEALTHEC, https://healthec.com/what-we-do/ (last visited April 24, 2024).
[5] *Notice of the HealthEC LLC Cyber Security Event*, HEALTHEC (Dec. 22, 2023) https://healthec.com/cyber-incident/ (listing Beaumont, Corewell, Community Health Care Systems, and TennCare); *Data Breach Notifications*, MAINE ATTY

partnerships, the Provider Defendants share patients' highly sensitive personal health information and other data with HealthEC, and HealthEC provides its PHM services.

4. Together, Defendants store a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about current and former patients and employees. But Defendants failed to protect that data when cybercriminals infiltrated HealthEC's insufficiently protected computer systems in a data breach, exposing the PII/PHI of over 4.6 million patients (the "Data Breach").

5. It is unknown for precisely how long the cybercriminals had access to HealthEC's networks before the breach was discovered. In other words, HealthEC had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to current and former patients' and employees' PII/PHI.

6. On information and belief, cybercriminals were able to breach HealthEC's systems because HealthEC failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI.

GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/4680936e-e496-43ed-a35d-59ece9b523b6.shtml (last visited April 23, 2024) (listing MD Valuecare).

7. On information and belief, while industry-standard security measures were readily available to HealthEC, and HealthEC knew it had security vulnerabilities with its systems, it continued using its substandard measures due to expense. Thus, HealthEC accepted the risk of its inadequate security measures to enrich its bottom line. In other words, HealthEC prioritized its profit motive and deprioritized its obligations to protect Plaintiffs' data.

8. Provider Defendants are also responsible for the Data Breach because they have a non-delegable duty to protect their patients' PII/PHI and for failing to exercise appropriate control over HealthEC's data security, which was Provider Defendants' right and obligation as HealthEC's partners.

9. Provider Defendants knew or should have known HealthEC was unequipped to protect the Class's PII/PHI that Provider Defendants shared with HealthEC. The Provider Defendants also failed to properly evaluate and exercise appropriate discretion in selecting the vendors they chose to partner and share the Class's PII/PHI with.

10. Just as blameworthy is Defendants' delay in informing the affected patients of the Data Breach. Although the Data Breach was discovered in July 2023, Defendants waited until December 2023—five months later—to mail individual notification letters to affected patients. In short, Defendants' failures placed the

Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

11. Plaintiffs are Data Breach victims. They bring this class action on behalf of themselves, and all others harmed by Defendants' misconduct.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendants are citizens of different states. And there are over 100 putative Class Members. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

13. This Court has personal jurisdiction over Defendants because HealthEC is headquartered in New Jersey, and because Defendants regularly conduct business in New Jersey and have sufficient minimum contacts in New Jersey.

14. Venue is proper in this Court because HealthEC's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

NAMED PLAINTIFFS

15. The Plaintiffs identified below bring this action on behalf of themselves and those similarly situated. As with the rest of the 4.6 million victims of the

HealthEC data breach, Plaintiffs are individuals who had their PII/PHI compromised in the Data Breach.

16. Plaintiffs are current and/or former patients or employees of Defendants. As a condition of Plaintiffs' receipt of services, Defendants required that Plaintiffs (or their third-party agents) provide their PII/PHI and then Defendants used that PII/PHI to facilitate their provision of medical services. Similarly, Defendants conditioned employment on Plaintiffs providing PII/PHI.

17. Plaintiffs suffered a concrete and particularized injury as a result of Defendants' failures to protect their PII/PHI and the subsequent disclosure of their PII/PHI to unauthorized parties without their consent, as alleged herein.

18. Had Defendants disclosed that they disregarded their duty to safeguard and protect Plaintiffs' PII/PHI from unauthorized access, Plaintiffs would have taken that into account in making their healthcare decisions. In particular, had Plaintiffs known about Provider Defendants' failure to ensure their vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected Plaintiffs' PII/PHI, they would not have provided their PII/PHI to Provider Defendants and would have engaged a competing provider to perform medical services.

I. FLORIDA

A. Plaintiff Allan Bishop

19. Plaintiff Allan Bishop (or "Bishop") is a citizen and resident of Florida and received healthcare from MD Valuecare, LLC ("MD Valuecare") in St. Augustine, Florida, prior to December 22, 2023.

20. For purposes of receiving healthcare services, Plaintiff Bishop was required to and did provide MD Valuecare with his PII/PHI, including his address, date of birth, social security number, phone number, email address, driver's license number, payment card information, and health insurance information.

21. MD Valuecare maintained and generated Plaintiff Bishop's PII/PHI in the course of providing healthcare services to Plaintiff Bishop, including upon information and belief, patient account numbers, health insurance plan member identification numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

22. Plaintiff Bishop was presented with standard HIPAA privacy notices before disclosing his PII/PHI to MD Valuecare.

23. As an MD Valuecare patient, Plaintiff Bishop entrusted MD Valuecare with the responsibility to safeguard and protect his personal information.

24. In connection with MD Valuecare, LLC's relationship with HealthEC, MD Valuecare shared Plaintiff Bishop's PII/PHI with HealthEC.

25. Plaintiff Bishop received a Data Breach notification dated December 22, 2023, from HealthEC on behalf of MD Valuecare via U.S. mail.

26. The Data Breach notification letter informed Plaintiff Bishop that his "name, date of birth, health insurance information, subscriber member number, patient account number, and patient identification number" were compromised in the Data Breach.

27. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff Bishop could take certain actions like monitoring his financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated Plaintiff Bishop could place a "fraud alert" or "security freeze," if not both, on his credit report to detect any possible misuse of personal information.

28. As a direct and proximate result of the Data Breach, Plaintiff Bishop has spent time and effort researching the breach and reviewing his financial and medical account statements for evidence of unauthorized activity, which he will continue to do indefinitely. Plaintiff Bishop also suffered emotional distress knowing that his highly personal medical and treatment information is no longer

confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against him for the rest of his life.

29. Plaintiff Bishop also incurred mitigation expenses. As a result of the Data Breach, Plaintiff Bishop contacted United Healthcare, who offered protection through Allstate Identity Protection for a monthly fee.

30. As a direct and proximate result of the Data Breach, Plaintiff Bishop suffered actual injury and damages from having his PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of his PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or MD Valuecare, loss of value and privacy and confidentiality of his PII/PHI, the cost of indefinite monitoring and protection of his financial and medical accounts, violation of his privacy rights, loss of time, and failure to receive the benefit of his bargain.

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

B. Plaintiff Beatriz Castillo Benitez

32. Plaintiff Beatriz Castillo Benitez is a citizen and resident of Florida. Plaintiff Benitez's employer uses Advantum as a credentialing organization, which in turn stored her PII/PHI within the TennCare System maintained with HealthEC.

33. Through her employer's third-party servicers, Plaintiff Benitez entrusted Advantum and TennCare with the responsibility to safeguard and protect her personal information.

34. In connection with TennCare's relationship with HealthEC, TennCare shared Plaintiff Benitez' PII/PHI with HealthEC.

35. Plaintiff Benitez received a Data Breach notification dated December 22, 2023, from HealthEC on behalf of TennCare via U.S. mail.

36. The Data Breach notification letter informed Plaintiff Benitez that her "name, address, date of birth, social security number, Medicaid identification, and health insurance information" were compromised in the Data Breach.

37. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff Benitez could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated that Plaintiff Benitez could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

38. As a direct and proximate result of the Data Breach, Plaintiff Benitez has spent time and effort researching the breach and reviewing her financial and

medical account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff Benitez also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

39. As a direct and proximate result of the Data Breach, Plaintiff Benitez suffered actual injury and damages from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of his PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or TennCare, loss of value and privacy and confidentiality of her PII/PHI, the cost of indefinite monitoring and protection of her financial and medical accounts, violation of his privacy rights, loss of time, and failure to receive the benefit of her bargain.

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

C. Plaintiff Kristel De Verona

41. Plaintiff Kristel De Verona (or "De Verona") is a citizen and resident of Florida. Plaintiff De Verona's employer uses Advantum as a credentialing

organization, which in turn stored her PII/PHI within the TennCare System maintained with HealthEC.

42. Through her employer's third-party servicers, Plaintiff De Verona entrusted Advantum and TennCare with the responsibility to safeguard and protect her personal information.

43. In connection with TennCare's relationship with HealthEC, TennCare shared Plaintiff De Verona's PII/PHI with HealthEC.

44. Plaintiff De Verona received a Data Breach notification dated December 22, 2023, from HealthEC on behalf of TennCare via U.S. mail.

45. The Data Breach notification letter informed Plaintiff De Verona that her "name, address, date of birth, social security number, Medicaid identification, and health insurance information" were compromised in the Data Breach.

46. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff De Verona could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated that Plaintiff De Verona could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

47. Following the Data Breach, Plaintiff De Verona suffered fraud and misuse of her PII/PHI, including three fraudulent applications for credit cards at Chase Bank, Wells Fargo, and Credit First Financial. The PII/PHI disclosed to TennCare and subject to the breach can be used to open accounts in Plaintiff De Verona's name.

48. As a direct and proximate result of the Data Breach, Plaintiff De Verona has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff De Verona also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

49. As a direct and proximate result of the Data Breach, Plaintiff De Verona suffered actual injury and damages from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of his PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or TennCare, loss of value and privacy and confidentiality of her PII/PHI, the cost of indefinite monitoring and protection of her financial and medical accounts, violation of his privacy rights, loss of time, and failure to receive the benefit of her bargain.

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

II. GEORGIA

A. Plaintiff Caroline Cappas

51. Plaintiff Caroline Cappas (or "Cappas") is a citizen and resident of Georgia and received healthcare through Community Health Care Systems at Macon Medical Center Pain Management Center in Macon, Georgia, prior to December 22, 2023.

52. For purposes of receiving healthcare services, Plaintiff Cappas was required to and did provide Community Health Care Systems with her PII/PHI, including her address, date of birth, social security number, phone number, email address, driver's license number, and health insurance information.

53. Community Health Care Systems maintained and generated Plaintiff Cappas's PII/PHI in the course of providing healthcare services to Plaintiff Cappas, including her patient account numbers, health insurance plan member identification numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

54. Plaintiff Cappas was presented with standard HIPAA privacy notices before disclosing her PII/PHI to Community Health Care Systems.

55. As a Community Health Care Systems patient, Plaintiff Cappas entrusted Community Health Care Systems with the responsibility to safeguard and protect her personal information.

56. In connection with Community Health Care Systems's relationship with HealthEC, Community Health Care Systems shared Plaintiff Cappas's PII/PHI with HealthEC.

57. Plaintiff Cappas received a Data Breach notification dated December 22, 2023, from HealthEC on behalf of Community Health Care Systems via U.S. mail.

58. The Data Breach notification letter informed Plaintiff Cappas that her "name, date of birth, health insurance information, patient account number, and patient identification number" were compromised in the Data Breach.

59. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff Cappas could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated that Plaintiff Cappas could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

60. As a direct and proximate result of the Data Breach, Plaintiff Cappas has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff Cappas also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

61. As a direct and proximate result of the Data Breach, Plaintiff Cappas suffered actual injury and damages from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of her PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or Community Health Care Systems, the cost of indefinite monitoring and protection of her financial and medical accounts, loss of value and privacy and confidentiality of her PII/PHI, violation of her privacy rights, loss of time, and failure to receive the benefit of her bargain.

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

B. Plaintiff Gregory Leeb

63. Plaintiff Gregory Leeb (or "Leeb") is a citizen and resident of Georgia and received healthcare through Community Healthcare Systems in Macon, Georgia, prior to December 22, 2023.

64. For purposes of receiving healthcare services, Plaintiff Gregory Leeb was required to and did provide Community Healthcare Systems with his PII/PHI, including his address, phone number, email address, date of birth, social security number, payment card information, and health insurance information.

65. Community Healthcare Systems maintained and generated Plaintiff Leeb's PII/PHI in the course of providing healthcare services to Plaintiff Leeb, including upon information and belief, patient account numbers, health insurance plan member identification, numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

66. Plaintiff Leeb was presented with standard HIPAA privacy notices before disclosing his PII/PHI to Community Healthcare Systems.

67. As a Community Healthcare Systems patient, Plaintiff Leeb entrusted Community Healthcare Systems with the responsibility to safeguard and protect his personal information.

68. In connection with Community Healthcare Systems' relationship with HealthEC, Community Healthcare Systems shared Plaintiff Leeb's PII/PHI with HealthEC.

69. Plaintiff Gregory Leeb received a Data Breach notification dated December 22, 2023, from HealthEC on behalf of Community Healthcare Systems via U.S. mail.

70. The Data Breach notification letter informed Plaintiff Leeb that his "name, date of birth, health insurance information, patient account number, and patient identification number" were compromised in the Data Breach.

71. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff Leeb could take certain actions like monitoring his financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated that Plaintiff Leeb could place a "fraud alert" or "security freeze," if not both, on his credit report to detect any possible misuse of personal information.

72. As a direct and proximate result of the Data Breach, Plaintiff Leeb has spent time and effort researching the breach and reviewing his financial and medical account statements for evidence of unauthorized activity, which he will continue to

do indefinitely. Plaintiff Leeb also suffered emotional distress knowing that his highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against him for the rest of his life.

73. As a direct and proximate result of the Data Breach, Plaintiff Leeb suffered actual injury and damages from having his PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of his PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or Community Healthcare Systems, the cost of indefinite monitoring and protection of his financial and medical accounts, loss of value and privacy and confidentiality of his PII/PHI, violation of his privacy rights, loss of time, and failure to receive the benefit of his bargain.

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

III. MICHIGAN

A. Plaintiff Jessica Fenn

75. Plaintiff Jessica Fenn (or "Fenn") is a citizen and resident of the State of Michigan and received healthcare from Beaumont ACO through physicians at Beaumont Hospital, Gross Pointe, located in Grosse Pointe, Michigan.

76. Fenn received healthcare services from Beaumont ACO for at least several years prior to the Data Breach, including the years 2022 and 2023.

77. For purposes of receiving Healthcare, Plaintiff Fenn was required to and did provide Beaumont ACO with her PII/PHI, including her address, social security number, date of birth, email address, phone number, payment card information, and health insurance information.

78. Beaumont ACO maintained the PII/PHI it was provided by Fenn, as well as PII/PHI concerning Plaintiff Fenn generated in the course of providing healthcare services to her, including dates of service, provider names, and medical and clinical treatment information and billing and claims information.

79. Plaintiff Fenn was presented with standard HIPAA privacy notices before disclosing her PII/PHI to Beaumont ACO.

80. As a Beaumont ACO patient, Plaintiff Fenn entrusted Beaumont ACO with the responsibility to safeguard and protect her personal information.

81. In connection with Beaumont ACO's relationship with HealthEC, Beaumont ACO shared Plaintiff Fenn's PII/PHI with HealthEC.

82. Plaintiff Fenn received a Data Breach notification letter, dated December 22, 2023, from HealthEC on behalf of Beaumont ACO via U.S. mail.

83. The Data Breach notification letter informed Plaintiff Fenn that her "name, date of birth, medical information, and billing or claims information" were compromised in the Data Breach.

84. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff Fenn could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated that Plaintiff Fenn could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

85. As a direct and proximate result of the Data Breach, Plaintiff Fenn has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff Fenn also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

86. As a direct and proximate result of the Data Breach, Plaintiff Fenn suffered actual injury and damages from having her PII/PHI compromised as a result

of the Data Breach including, but not limited to: damage to and diminution in the value of her PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or Beaumont ACO, the cost of indefinite monitoring and protection of her financial and medical accounts, loss of value and privacy and confidentiality of her PII/PHI, violation of her privacy rights, loss of time, and failure to receive the benefit of her bargain.

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

B. Plaintiff Joni Fielder

88. Plaintiff Joni Fielder (or "J. Fielder") is a citizen and resident of Michigan and received healthcare from Beaumont ACO in Dearborn, Michigan, prior to December 22, 2023.

89. For purposes of receiving Healthcare, Plaintiff J. Fielder was required to and did provide Beaumont ACO with her PII/PHI, including her address, social security number, date of birth, email address, phone number, payment card information, and health insurance information.

90. Beaumont ACO maintained the PII/PHI it was provided by J. Fielder, as well as PII/PHI concerning Plaintiff J. Fielder generated in the course of providing

healthcare services to her, including dates of service, provider names, and medical and clinical treatment information and billing and claims information.

91. Plaintiff J. Fielder was presented with standard HIPAA privacy notices before disclosing her PII/PHI to Beaumont ACO.

92. As a Beaumont ACO patient, Plaintiff J. Fielder entrusted Beaumont ACO with the responsibility to safeguard and protect her personal information.

93. In connection with Beaumont ACO's relationship with HealthEC, Beaumont ACO shared Plaintiff J. Fielder's PII/PHI with HealthEC.

94. Plaintiff J. Fielder received a Data Breach notification letter, dated December 22, 2023, from HealthEC on behalf of Beaumont ACO via U.S. mail.

95. The Data Breach notification letter informed Plaintiff J. Fielder that her "name, date of birth, medical information, and billing or claims information" were compromised in the Data Breach.

96. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff J. Fielder could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated that Plaintiff J. Fielder could place a "fraud alert" or

"security freeze," if not both, on her credit report to detect any possible misuse of personal information.

97. Following the Data Breach, Plaintiff J. Fielder suffered fraud and misuse of her PII/PHI, including unauthorized charges on her PNC debit card that was associated with her payments for Beaumont ACO medical services. As a result of this fraud, Plaintiff J. Fielder spent time reversing the charges, canceling accounts, and changing passwords.

98. As a direct and proximate result of the Data Breach, Plaintiff J. Fielder has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff J. Fielder also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

99. As a direct and proximate result of the Data Breach, Plaintiff J. Fielder suffered actual injury and damages from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of her PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or Beaumont ACO, the cost of indefinite monitoring and protection of her financial and medical accounts, loss of value and privacy and confidentiality of

her PII/PHI, violation of her privacy rights, loss of time, and failure to receive the benefit of her bargain.

100. Plaintiff J. Fielder has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

C. Plaintiff Keith Fielder

101. Plaintiff Keith Fielder (or "K. Fielder") is a citizen and resident of Michigan and received healthcare from Beaumont ACO in Dearborn, Michigan, prior to December 22, 2023.

102. For purposes of receiving Healthcare, Plaintiff K. Fielder was required to and did provide Beaumont ACO with his PII/PHI, including his address, social security number, date of birth, email address, phone number, payment card information, and health insurance information.

103. Beaumont ACO maintained the PII/PHI it was provided by K. Fielder, as well as PII/PHI concerning Plaintiff K. Fielder generated in the course of providing healthcare services to him, including, dates of service, provider names, and medical and clinical treatment information and billing and claims information.

104. Plaintiff K. Fielder was presented with standard HIPAA privacy notices before disclosing his PII/PHI to Beaumont ACO.

105. As a Beaumont ACO patient, Plaintiff K. Fielder entrusted Beaumont ACO with the responsibility to safeguard and protect his personal information.

106. In connection with Beaumont ACO's relationship with HealthEC, Beaumont ACO shared Plaintiff K. Fielder's PII/PHI with HealthEC.

107. Plaintiff K. Fielder received a Data Breach notification letter, dated December 22, 2023, from HealthEC on behalf of Beaumont ACO via U.S. mail.

108. The Data Breach notification letter informed Plaintiff K. Fielder that his "name, date of birth, medical information, and billing or claims information" were compromised in the Data Breach.

109. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff K. Fielder could take certain actions like monitoring his financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated that Plaintiff K. Fielder could place a "fraud alert" or "security freeze," if not both, on his credit report to detect any possible misuse of personal information.

110. Following the Data Breach, Plaintiff K. Fielder suffered fraud and misuse of his PII/PHI, including unauthorized charges on his PNC debit card that was associated with his payments for Beaumont ACO medical services. As a result

of this fraud, Plaintiff K. Fielder spent time reversing the charges, canceling accounts, and changing passwords.

111. As a direct and proximate result of the Data Breach, Plaintiff K. Fielder has spent time and effort researching the breach and reviewing his financial and medical account statements for evidence of unauthorized activity, which he will continue to do indefinitely. Plaintiff K. Fielder also suffered emotional distress knowing that his highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against him for the rest of his life.

112. As a direct and proximate result of the Data Breach, Plaintiff K. Fielder suffered actual injury and damages from having his PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of his PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or Beaumont ACO, the cost of indefinite monitoring and protection of his financial and medical accounts, loss of value and privacy and confidentiality of his PII/PHI, violation of his privacy rights, loss of time, and failure to receive the benefit of his bargain.

D. Plaintiff Mindy Markowitz

113. Plaintiff Mindy Markowitz (or "Markowitz") is a citizen and resident of Michigan and received healthcare from Corewell Health for several years prior to the Data Breach, including the years 2022 and 2023.

114. For purposes of receiving Healthcare, Plaintiff Markowitz was required to and did provide Corewell Health with her PII/PHI, including her address, social security number, date of birth, email address, phone number, payment card information, and health insurance information.

115. Corewell Health maintained the PII/PHI it was provided by Markowitz, as well as PII/PHI concerning Plaintiff Markowitz generated in the course of providing healthcare services to her, including dates of service, provider names, and medical and clinical treatment information and billing and claims information.

116. Plaintiff Markowitz was presented with standard HIPAA privacy notices before disclosing her PII/PHI to Corewell Health.

117. As a Corewell Health patient, Plaintiff Markowitz entrusted Corewell Health with the responsibility to safeguard and protect her personal information.

118. In connection with Corewell Health's relationship with HealthEC, Corewell Health shared Plaintiff Markowitz's PII/PHI with HealthEC.

119. Plaintiff Markowitz received a Data Breach notification letter, dated December 22, 2023, from HealthEC on behalf of Corewell Health via U.S. mail.

120. The Data Breach notification letter informed Plaintiff Markowitz that her "name, date of birth, medical information, and billing or claims information" were compromised in the Data Breach.

121. In their letter, Defendants expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when they stated that Plaintiff Markowitz could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, Defendants stated that Plaintiff Markowitz could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

122. Following the Data Breach, Plaintiff Markowitz suffered fraud and misuse of her PII/PHI, including an unauthorized charge on her Kohl's credit card. As a result of this fraud, Plaintiff Markowitz spent time reversing the charge. The PII/PHI disclosed to Corewell Health and subject to the breach can be used to access Plaintiff Markowitz's financial accounts, including her Kohl's card that experienced the fraudulent charge.

123. As a direct and proximate result of the Data Breach, Plaintiff Markowitz has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity,

which she will continue to do indefinitely. Plaintiff Markowitz also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

124. As a direct and proximate result of the Data Breach, Plaintiff Markowitz suffered actual injury and damages from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of her PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or Corewell Health, the cost of indefinite monitoring and protection of her financial and medical accounts, loss of value and privacy and confidentiality of her PII/PHI, violation of her privacy rights, loss of time, and failure to receive the benefit of her bargain.

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

IV. TENNESSEE

A. Plaintiff Della Vallejo

126. Plaintiff Della Vallejo (or "Vallejo") is a citizen and resident of Tennessee and received healthcare from various healthcare providers throughout the

State of Tennessee, Division of TennCare ("TennCare"), for several years prior to the Data Breach, including the years 2022 and 2023.

127. For purposes of receiving healthcare services, Plaintiff Vallejo was required to and did provide the TennCare Healthcare Providers with her PII/PHI, including her address, phone number, email address, date of birth, social security number, driver's license number, and payment card information.

128. The TennCare Healthcare Providers maintained and generated Plaintiff Vallejo's PII/PHI in the course of providing healthcare services to Plaintiff Vallejo, including patient account numbers, health insurance plan member identification numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

129. Plaintiff Vallejo was presented with standard HIPAA privacy notices before disclosing her PII/PHI to the TennCare Healthcare Providers.

130. As a TennCare member, Plaintiff Vallejo entrusted TennCare with the responsibility to safeguard and protect her personal information.

131. In connection with TennCare's relationship with HealthEC, TennCare shared Plaintiff Vallejo's PII/PHI with HealthEC.

132. Plaintiff Vallejo received a Data Breach notification dated December 22, 2023, from HealthEC on behalf of TennCare via U.S. mail.

133. The Data Breach notification letter informed Plaintiff Vallejo that her "name, address, date of birth, social security number, taxpayer identification number, medical information, diagnosis, health insurance information, and patient identification number" were compromised in the Data Breach.

134. In its letter, HealthEC expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when it stated that Plaintiff Vallejo could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, HealthEC stated that Plaintiff Vallejo could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

135. Shortly after the Data Breach, Plaintiff Vallejo suffered fraud and misuse of her PII/PHI, including unauthorized charges on her Cash App account. As a result of this fraud, Plaintiff Vallejo spent time reversing the charges, canceling accounts, and changing passwords. The PII/PHI provided to TennCare and subject to the Data Breach can be used to access Plaintiff Vallejo's Cash App account.

136. As a direct and proximate result of the Data Breach, Plaintiff Vallejo has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will

continue to do indefinitely. Plaintiff Vallejo also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

137. As a direct and proximate result of the Data Breach, Plaintiff Vallejo suffered actual injury and damages from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of her PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or TennCare, the cost of indefinite monitoring and protection of her financial and medical accounts, loss of value and privacy and confidentiality of her PII/PHI, violation of her privacy rights, loss of time, and failure to receive the benefit of her bargain.

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

B. Plaintiff Jane Doe

139. Plaintiff Jane Doe (or "Doe") is a citizen and resident of Tennessee and has received healthcare from various healthcare providers all through the State of Tennessee, Division of TennCare ("TennCare"), for several years prior to the Breach, including the years 2022 and 2023.

140. Plaintiff Doe has been determined to be fully disabled and receives benefits and services from TennCare, including monetary benefits, health insurance benefits, and other services, as well as Social Security Disability benefits.

141. For purposes of receiving these healthcare services and benefits, Plaintiff Doe was required to and did provide TennCare with her PII/PHI, including her health and mental health records, treatment notes, dates of service, provider names, date of birth, social security number, driver's license number, and other medical information.

142. TennCare maintained and generated Plaintiff Doe's PII/PHI in the course of providing benefits and healthcare services to Plaintiff Doe, including patient account numbers, health insurance plan member identification numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

143. Plaintiff Doe was presented with standard HIPAA privacy notices before disclosing her PII/PHI to TennCare.

144. As a TennCare patient, Plaintiff Doe entrusted TennCare with the responsibility to safeguard and protect her personal information.

145. In connection with TennCare's relationship with HealthEC, TennCare shared Plaintiff Doe's PII/PHI with HealthEC.

146. Plaintiff Doe received a Data Breach notification dated December 22, 2023, from HealthEC on behalf of TennCare via U.S. mail.

147. The Data Breach notification letter informed Plaintiff Doe that her "name, address, date of birth, social security number, medical information, diagnosis, health insurance information, and patient identification number" were compromised in the Data Breach.

148. In its letter, HealthEC expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when it stated that Plaintiff Doe could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, HealthEC stated that Plaintiff Doe could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

149. As a direct and proximate result of the Data Breach, Plaintiff Doe has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff Doe also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can

be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

150. As a direct and proximate result of the Data Breach, Plaintiff Doe suffered actual injury and damages from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of her PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or TennCare, the cost of indefinite monitoring and protection of her financial and medical accounts, loss of value and privacy and confidentiality of her PII/PHI, violation of her privacy rights, loss of time, and failure to receive the benefit of her bargain.

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

C. Plaintiff Lisa Bryson

152. Plaintiff Lisa Bryson (or "Bryson") is a citizen and resident of the State of Tennessee and received healthcare from various healthcare providers throughout the State of Tennessee, Division of TennCare ("TennCare") for several years prior to the Data Breach, including the years 2022 and 2023.

153. For purposes of receiving healthcare services, Plaintiff Bryson was required to and did provide the TennCare Healthcare Providers with her PII/PHI,

including her address, phone number, email address, date of birth, social security number, TennCare insurance identification number, medical information, and emergency contact information.

154. The TennCare Healthcare Providers maintained the PII/PHI Bryson provided them with as well as PII/PHI concerning Plaintiff Bryson generated in the course of providing healthcare services to Plaintiff Bryson, including dates of service, provider names, and medical and clinical treatment information.

155. Plaintiff Bryson was presented with standard HIPAA privacy notices before disclosing her PII/PHI to the TennCare Healthcare Providers.

156. As a TennCare Healthcare Provider patient, Plaintiff Bryson entrusted TennCare with the responsibility to safeguard and protect her personal information.

157. In connection with TennCare's relationship with HealthEC, TennCare shared Plaintiff Bryson's PII/PHI with HealthEC.

158. Plaintiff Bryson received a Data Breach notification letter dated December 22, 2023, from HealthEC on behalf of the State of Tennessee, Division of TennCare via U.S. mail.

159. The Data Breach notification letter informed Plaintiff Bryson that her "name, address, date of birth, social security number, taxpayer identification number, medical information, diagnosis, health insurance information, and patient identification number" were compromised in the Data Breach.

160. In its letter, HealthEC expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when it stated that Plaintiff Bryson could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors. Furthermore, HealthEC stated that Plaintiff Bryson could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

161. Following the Data Breach, Plaintiff Bryson learned through a monitoring service she used that information concerning her, including her email address and credit card number, was found on the dark web on September 26, 2023.

162. Plaintiff Bryson also learned in about January 2024 through another monitoring service she used that information concerning her was for sale by 12 data broker websites.

163. As a direct and proximate result of the Data Breach, Plaintiff Bryson has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff Bryson also suffered emotional distress knowing that her highly personal medical and treatment information is no longer

confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

164. As a direct and proximate result of the Data Breach, Plaintiff Bryson suffered actual injury and damages from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of her PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff and/or TennCare, the cost of indefinite monitoring and protection of her financial and medical accounts, loss of value and privacy and confidentiality of her PII/PHI, violation of her privacy rights, loss of time, and failure to receive the benefit of her bargain.

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

D. Plaintiffs Abbey Robinson and J

166. Plaintiff Abbey Robinson ("Robinson") is a citizen and resident of the State of Tennessee. Plaintiff Robinson also asserts claims on behalf of her minor son, hereinafter referred to as "J." J is also a citizen and resident of the State of Tennessee.

167. Plaintiff Robinson and J received healthcare from various healthcare service providers through the State of Tennessee, Division of TennCare

("TennCare"), for several years prior to the Data Breach, including the years 2022 and 2023.

168. For purposes of receiving healthcare services, Plaintiff Robinson was required to and did provide the TennCare Healthcare Providers with her PII/PHI including her address, phone number, email address, date of birth, social security number, TennCare identification number, and certain medical information. Plaintiff was also required to and did provide the TennCare Healthcare Providers with the PII/PHI of J, including his address, date of birth, social security number, TennCare identification number, and certain medical information.

169. The TennCare Healthcare Providers maintained the PII/PHI Robinson provided them with for both herself and J, as well as the PII/PHI concerning Robinson and J generated in the course of providing healthcare services to both Robinson and J, including dates of service, healthcare provider names, and medical and clinical treatment information.

170. Plaintiff Robinson was presented with standard HIPAA privacy notices before disclosing her and J's PII/PHI to the TennCare Healthcare Providers.

171. As TennCare Healthcare Provider patients, Plaintiff Robinson, on behalf of herself as well as J, entrusted TennCare with the responsibility to safeguard and protect the personal information of both herself and J.

172. In connection with TennCare's relationship with HealthEC, TennCare shared the PII/PHI of both Robinson and J with HealthEC.

173. Plaintiff Robinson received a Data Breach notification letter dated December 22, 2023, from HealthEC on behalf of the State of Tennessee, Division of TennCare via U.S. mail. Robinson also received a Data Breach notification letter addressed to the Parent/Guardian of J dated December 22, 2023 from HealthEC on behalf of the State of Tennessee, Division of TennCare via U.S. mail.

174. The Data Breach notification letter informed Plaintiff Robinson that her "name, address, date of birth, social security number, medical information, diagnosis, health insurance information, and patient identification number" were compromised in the Data Breach. Similarly, the Data Breach notification letter Robinson received as the Parent/Guardian of J informed her that her minor child's "name, address, date of birth, social security number, medical information, diagnosis, health insurance information, and patient identification number" were compromised in the Data Breach.

175. In its letter, HealthEC expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when it stated that Plaintiff Robinson could take certain actions like monitoring her financial accounts, explanation of benefits statements, and credit reports for suspicious activity and to detect errors.

Furthermore, HealthEC stated that Plaintiff Robinson could place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

176. As a direct and proximate result of the Data Breach, Plaintiff Robinson has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff Robinson also suffered emotional distress knowing that her and J's highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against them for the rest of their lives.

177. As a direct and proximate result of the Data Breach, Plaintiff Robinson and J suffered actual injury and damages from having their PII/PHI compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of their PII/PHI, a form of intangible property that HealthEC obtained from Plaintiff Robinson and/or TennCare, the cost of indefinite monitoring and protection of his financial and medical accounts, loss of value and privacy and confidentiality of their PII/PHI, violation of their privacy rights, loss of time, and failure to receive the benefit of their bargain.

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

DEFENDANTS

179. Defendant, HealthEC, LLC, is a limited liability company formed under the laws of Delaware and with its principal place of business at 343 Thornall Street, #630, Edison, New Jersey 08837. On information and belief, each member of the LLC is a citizen and resident of New Jersey.

180. Defendant, Community Health Care Systems, Inc. is a nonprofit corporation incorporated in Georgia and with its principal place of business at 2251 W Elm Street, Wrightsville, Georgia, 31096.

181. Defendant, Corewell Health d/b/a Corewell, is a nonprofit corporation incorporated in Michigan, and with its principal place of business at 100 Michigan Street NE, Grand Rapids, Michigan 49503.

182. Defendant, MD Valuecare, LLC, is a limited liability company formed under the laws of Virginia, and with its principal place of business at 8001 Franklin Farms Drive, Suite 130, Richmond, Virginia 23229.

183. Defendant, Oakwood Accountable Care Organization, LLC d/b/a Beaumont ACO, is a limited liability company formed under the laws of Michigan

and with its principal place of business at 26901 Beaumont Boulevard, Southfield, Michigan 48033.

BACKGROUND

Defendants Collected and Stored the PII/PHI of Plaintiffs and the Class

184. Defendant HealthEC is a business that sells data management and data analytics services to healthcare providers.[6] For example, HealthEC advertises its "integrated population health management (PHM) platform" which provides "comprehensive analytics and integrated, role-based tools[.]"[7]

185. Broadly speaking, HealthEC partners with numerous healthcare systems including "Corewell Health, HonorHealth, University Medical Center of Princeton Physicians' Organization, Community Health Care Systems, State of Tennessee, Division of TennCare, Beaumont ACO, KidneyLink, Alliance for Integrated Care of New York, LLC, Compassion Health Care, Metro Community Health Centers, Advantage Care Diagnostic & Treatment Center, Inc., Long Island Select Healthcare, Mid Florida Hematology & Oncology Centers, P.A, d/b/a Mid-Florida Cancer Centers, Illinois Heath Practice Alliance, LLC, East Georgia Healthcare Center, Hudson Valley Regional Community Health Centers, Kinston

[6] *Home Page*, HEALTHEC, https://healthec.com/ (last visited April 10, 2024).
[7] *Id*.

Community Health Center Inc., Mountain Community Health Partnership, Women & Children's Health Alliance, and Upstate Family Health Center, Inc."[8]

186. HealthEC partners with Defendants Community Health Care Systems, Corewell, MD Valuecare, and Beaumont.[9]

a. Defendant Community Health Care Systems, Inc. is a healthcare provider with locations throughout Georgia.[10]

b. Defendant Corewell Health is a healthcare system with locations throughout Michigan.[11]

c. Defendant MD Valuecare, LLC is a healthcare provider based in Richmond, Virginia.[12]

[8] *Notice of the HealthEC LLC Cyber Security Event*, HEALTHEC (Dec. 22, 2023) https://healthec.com/cyber-incident/.
[9] *Id*. (listing Community Health Care Systems, Corewell, Beaumont, and TennCare); *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/4680936e-e496-43ed-a35d-59ece9b523b6.shtml (last visited April 23, 2024) (listing MD Valuecare).
[10] *About Us*, COMMUNITY HEALTH CARE SYS, https://chcsga.org/about-us/ (last visited April 23, 2024).
[11] *About*, COREWELL HEALTH, https://corewellhealth.org/about (last visited April 23, 2024).
[12] *Who We Are*, MD VALUE CARE, https://mdvaluecare.com/who-we-are/ (last visited April 23, 2024).

d. Defendant Oakwood Accountable Care Organization, LLC d/b/a Beaumont ACO is a healthcare system with locations throughout Michigan.[13]

187. Defendants receive and maintain the PII/PHI of millions of current and former patients and employees. Specifically, Plaintiffs and Class Members are the current and former patients and employees of healthcare systems that use (or used) HeathEC's services. As such, HealthEC required that Provider Defendants obtain the PII/PHI of Plaintiffs and Class Members.

188. In collecting and maintaining the PII/PHI, Defendants agreed to safeguard the data in accordance with internal policies, state law, and federal law. Plaintiffs and Class Members themselves took reasonable steps to secure their PII/PHI.

189. Under state and federal law, businesses like Defendants have common law and statutory duties to protect current and former patients' and employees' PII/PHI and to notify them about breaches.

190. Defendants recognize these duties. For example, in its "Privacy Policy," HealthEC declares that:

[13] *About Us*, BEAUMONT ACO, https://www.beaumont-aco.org/about-us (last visited April 23, 2024).

a. "At HealthEC, LLC . . . we take your privacy seriously and are committed to protecting your personal information."[14]

b. "We are committed to ensuring that your information is secure."[15]

c. "In order to prevent unauthorized access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online."[16]

d. "We further protect your information from potential security breaches by implementing certain technological security measures including encryption, firewalls and secure socket layer technology."[17]

191. And on its "Data Security & Privacy" webpage, HealthEC advertises, among other things, that:

a. "HealthEC is going above and beyond to protect our data and our clients with privacy and security measures that exceed industry standards."[18]

[14] *Privacy Policy*, HEALTHEC (March 19, 2021) https://healthec.com/privacy-policy/.
[15] *Id*.
[16] *Id*.
[17] *Id*.
[18] *Data Security & Privacy*, HEALTHEC, https://healthec.com/about/data-security-and-privacy/ (last visited April 10, 2024).

b. "First and foremost, all our security and privacy practices are HIPAA compliant."[19]

c. "HealthEC is also Certified by the Electronic Healthcare Network Accreditation Commission (EHNAC) and our SOC2 certification is in progress."[20]

d. "Security at HealthEC begins with our people. We make sure that they are all carefully trained in regards to HIPAA and our security protocols."[21]

e. "HealthEC has in place a comprehensive information security program that follows international and national data protection conventions."[22]

f. "HealthEC employs a variety of technology solutions and resources focused on data protection and privacy."[23]

g. "We use enterprise-wide multi-factor authentication (MFA)."[24]

h. "All access to data is protected by comprehensive identity and access management security (IAM)."[25]

---

[19] *Id*.
[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] *Id*.
[24] *Id*.
[25] *Id*.

i. "All data is encrypted in rest and transit."[26]

192. Defendant Beaumont advertises in its "Code of Conduct" that:

a. "We are committed to maintaining the confidentiality and security of personal information obtained throughout the course of the patient's treatment."[27]

b. "All patient information is confidential and only obtained, used or disclosed as necessary to perform job duties including reporting as required."[28]

c. "We do not tolerate breaches in confidential information and proactively safeguard patient information in keeping with The Health Insurance Portability and Accountability Act (HIPAA) requirements."[29]

d. "Beaumont ACO employees must never use or disclose confidential patient information that violates the privacy rights of our patients."[30]

---

[26] *Id*.
[27] *Code of Conduct*, BEAUMONT ACO, https://www.beaumont-aco.org/docs/default-source/about_us/2024-baco-code-of-conduct.pdf?sfvrsn=2dac1357_1 (last visited April 10, 2024).
[28] *Id*.
[29] *Id*.
[30] *Id*.

e. "Protected health information collected to provide care for a patient is confidential."[31]

f. "We enforce policies and procedures that protect confidential information from unauthorized use and disclosure."[32]

g. "In order to maintain the confidentiality and integrity of protected health information and confidential information, we enforce security policies and standards when information is transmitted electronically outside of the corporation; stored on portable devices, such as laptop computers and portable digital assistance devices (PDAs); or transferred to CD or USB drive."[33]

h. "Beaumont ACO's electronic communication systems are intended for business purposes and are designed to maintain the confidentiality, integrity, and availability of its information resources." [34]

i. "Beaumont . . . will monitor and/or control any access considered to be harmful to or inconsistent with Beaumont ACO business and will conduct routine audits of user access."[35]

---

[31] *Id*.
[32] *Id*.
[33] *Id*.
[34] *Id*.
[35] *Id*.

193. Defendant Community Health Care Systems, Inc. includes a "Notice of Privacy Practices" with its "New Patient Forms."[36] And via its "Notice of Privacy Practices," Community Health Care Systems promises that:

a. "The law requires us to: make sure that medical information that identifies you is kept private[.]"[37]

b. "Other uses and disclosures of medical information not covered by this notice or the laws that apply to use will be made only with your written authorization."[38]

c. "WHO WILL FOLLOW THIS NOTICE. This notice describes our practice's policies and procedures and that of any health care professional authorized to enter information into your medical chart, any member of a volunteer group which we allow to help you, as well as all employees, staff and other practice personnel."[39]

d. "You have the RIGHT to . . . [c]onfidential treatment of all communications and records pertaining to health status and care."[40]

[36] *New Patient Forms*, COMMUNITY HEALTH CARE SYS, https://chcsga.org/wp-content/uploads/2020/11/CHCSNewPatientForms.pdf (last visited April 23, 2024).
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*

194. Defendant MD Valuecare, LLC, advertises on its "For Patients" web page that:

a. "Your privacy is very important to us."[41]

b. "The privacy and security of your medical information is protected by federal law."[42]

The Data Breach

195. From July 14, 2023, until July 23, 2023, cybercriminals infiltrated Defendants' systems and had nine full days to peruse and exfiltrate data.[43]

196. According to Defendants, during this period, "certain systems were accessed by an unknown actor" and that "files were ***copied***."[44] In its breach notice, TennCare confirmed that the stolen data was "held for ransom."[45] Through the Data Breach, at least the following types of PII/PHI were compromised:

a. names;

b. addresses;

c. dates of birth;

---

[41] *For Patients*, MD VALUE CARE, https://mdvaluecare.com/for-patients/ (last visited April 23, 2024).
[42] *Id*.
[43] *Notice of the HealthEC LLC Cyber Security Event*, HEALTHEC (Dec. 22, 2023) https://healthec.com/cyber-incident/.
[44] *Id*. (emphasis added).
[45] *HealthEC Data Breach Information (February 2024)*, TENNCARE, https://www.tn.gov/content/dam/tn/tenncare/documents/TennCareHealthECFAQs.pdf (last visited Apr. 29, 2024).

d. Social Security numbers;

e. taxpayer identification numbers;

f. medical record numbers;

g. medical information;

h. diagnoses;

i. diagnosis codes;

j. mental/physical conditions;

k. prescription information;

l. provider's names and locations;

m. health insurance information;

n. beneficiary numbers;

o. subscriber numbers;

p. Medicaid/Medicare identifications;

q. billing and claims information;

r. patient account numbers;

s. patient identification numbers;

t. and treatment cost information.[46]

[46] *Id*.

197. In total, Defendants injured at least 4,656,293 persons—via the exposure of their PII/PHI—in the Data Breach.[47] Upon information and belief, these 4,656,293 persons include Provider Defendants' current and former patients and employees.

198. Thus far, the entities which contracted with HealthEC —and thus were impacted by the Data Breach—include "Corewell Health, HonorHealth, University Medical Center of Princeton Physicians' Organization, Community Health Care Systems, State of Tennessee, Division of TennCare, Beaumont ACO, KidneyLink, Alliance for Integrated Care of New York, LLC, Compassion Health Care, Metro Community Health Centers, Advantage Care Diagnostic & Treatment Center, Inc., Long Island Select Healthcare, Mid Florida Hematology & Oncology Centers, P.A, d/b/a Mid-Florida Cancer Centers, Illinois Heath Practice Alliance, LLC, East Georgia Healthcare Center, Hudson Valley Regional Community Health Centers, Kinston Community Health Center Inc., Mountain Community Health Partnership, Women & Children's Health Alliance, and Upstate Family Health Center, Inc."[48]

[47] *Cases Currently Under Investigation*, DEPT HEALTH & HUMAN SERVS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=314987482344F3763E7B56F48A814824 (last visited April 10, 2024).
[48] *Notice of the HealthEC LLC Cyber Security Event*, HEALTHEC (Dec. 22, 2023) https://healthec.com/cyber-incident/.

199. Although Defendants were aware of the breach in July 2023, they waited until December 22, 2023, until they began notifying the class.[49] Such notification was unreasonably delayed given that the notification was sent:

a. a full 161 days after the Data Breach began; and

b. a full 59 days after Defendant claimed it "completed" its Data Breach analysis on "October 24, 2023."[50]

200. Thus, Defendants kept the Class in the dark for an unreasonably long period, thereby depriving Plaintiffs and the Class of the opportunity to mitigate their injuries in a timely manner.

201. And when Defendants did notify Plaintiffs and the Class of the Data Breach, Defendants acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class to:

a. "remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors[;]" and

[49] *Id.*
[50] *Id.*

b. "educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General."[51]

202. Defendants failed their duties to protect Plaintiffs' and the Class's PII/PHI because their inadequate security practices caused the Data Breach. In other words, Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the Class's PII/PHI. And thus, Defendants caused widespread injury and monetary damages.

203. Since the breach, Defendants have promised to "review[] our existing policies and procedures."[52] But this is too little too late. Simply put, these measures—which Defendants now recognize as necessary—should have been implemented *before* the Data Breach.

204. On information and belief, Defendants failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures. Furthermore, Provider Defendants failed to exercise appropriate discretion in partnering with vendors and business associates that maintain adequate security measures. And Provider Defendants failed to exercise appropriate

[51] *Id.*
[52] *Id.*

supervision over HealthEC to ensure that it had adequate security measures that would safeguard the PII/PHI that they shared with HealthEC.

205. What's more, the Notice of Data Breach demonstrates that Defendants cannot—or will not—determine the full scope of the Data Breach, as Defendants have been unable to determine precisely what information was stolen and when.

206. Defendants have done little to remedy the Data Breach. Defendants have offered some victims limited credit monitoring and identity related services. But such services are wholly insufficient to compensate Plaintiffs and Class Members for the injuries that Defendants inflicted upon them.

207. Because of Defendants' Data Breach, the sensitive PII/PHI of Plaintiffs and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class Members.

208. The cybercriminals who compromised Defendants' systems are intent on engaging in criminal conduct. After all, the cybercriminals: (1) defeated Defendants' data security systems, (2) gained actual access to sensitive data, and (3) successfully "copied" files.[53]

209. As the Harvard Business Review succinctly put it, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit

[53] *Id*.

activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[54]

210. Thus, it is probable that Plaintiffs' and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiffs and Class Members Face Imminent and Continued Risk of Identity Theft and Other Fraud.

211. Because of Defendants' failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, among other things, monetary losses, lost time, nominal damages, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

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

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

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

e. the cost of indefinite monitoring of financial and medical accounts;

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

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

g. delay in receipt of tax refund monies;

h. unauthorized use of their stolen PII/PHI;

i. continued risk to their PII/PHI—which remains in Defendants' possession—and is thus at risk for future breaches so long as Defendants fail to take appropriate measures to protect the PII/PHI; and

j. nominal damages.

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

213. The value of Plaintiffs' and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years after a data breach. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

214. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both accurate and comprehensive. Criminals create them by cross-referencing and

combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

215. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

216. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/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 among the imminent and continuing risks to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members's stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

217. Defendants disclosed the PII/PHI of Plaintiffs and Class Members for criminals to use for criminal activity. Specifically, Defendants exposed the PII/PHI of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

218. Defendants' failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members's injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

The Data Breach was Preventable

219. Following the Data Breach, HealthEC stated that it "take[s] this event, your privacy, and the security of information in [its] care very seriously" and among other things, it is "reviewing [its] existing policies and procedures."

220. Upon information and belief, these "existing policies and procedures" were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true for at least two reasons: (1) because HealthEC was already on the path to standardizing its cybersecurity practices before the project was abandoned due to costs; and (2) because the healthcare industry is frequently one of the most targeted sectors for cyberattacks and attacks using stolen credentials have increased precipitously over the last several years.

221. On information and belief, HealthEC uses a vulnerable data center vendor. There is no access control, no security protocols, no audits, no performance metrics, or any reasonable cyber security protocols in place for HealthEC's data

center. Recognizing the potential risk, HealthEC proposed moving the data center to Azure, a secure-cloud computing platform operated by Microsoft. However, before HealthEC could implement the more secure system, HealthEC's senior management abandoned the data security project because it was too expensive. Had HealthEC followed through with the planned migration to a safer environment, this Data Breach most likely would not have occurred.

222. Furthermore, healthcare providers and their affiliates, like Defendants, are prime targets for data thieves because the information they collect and store—including patients' financial information, login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—are extremely valuable to fraudsters in underground markets.

223. Defendants were well aware that they were targets of cybercriminals, often through phishing efforts or other techniques for stealing login credentials. For example, the Department of Health and Human Services (HHS) recently disclosed that in 2023 alone more than 88 million individuals have been subjected to healthcare-related data breaches, a staggering 60% increase from the prior year.[55]

[55] *HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation*, HHS (Oct. 31, 2023), https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html.

224. It is well known that use of stolen credentials has long been a popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

225. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[56] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[57]

226. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[58] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human

[56] *Internet Crime Report 2020*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Apr. 17, 2024).
[57] 2021 DBIR Master's Guide, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited Apr. 17, 2024).
[58] https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited Jan. 17, 2024).

Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[59]

227. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making employees and other users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. For example, a common phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. The request may come from an e-mail address that appears official but contains only one different number or letter. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or to download an attachment containing malware.

228. User education provides the easiest method to properly identify fraudulent "spoofing" e-mails and prevent unauthorized access of sensitive internal information. According to a September 2020 guidance from CISA, organizations housing sensitive data should "[i]mplement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious

[59] *Id.*

activity" and conduct "organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails."[60]

229. From a technical perspective, companies can also greatly reduce the flow of fraudulent e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[61]

230. Additionally, because the goal of these schemes is to gain an employee's login credentials in order to access a company's network, there are industry-standard measures that companies can implement to greatly reduce

[60] *Ransomware Guide September 2020*, CISA, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf (last visited Apr. 17, 2024).
[61] *Id.*

unauthorized access, even if an individual's login credentials are disclosed. For example, multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login. This could include entering a code from the user's smartphone, answering a security question, or providing a biometric indicator such as a fingerprint or facial recognition—in addition to entering a username and password. Thus, even if hackers obtain an employee's username and password, access to the company's system is thwarted because they do not have access to the additional authentication methods.

231. Similarly, companies housing sensitive data must implement adequate "network segmentation," which is the practice of dividing a larger network into several smaller subnetworks that are each isolated from one another to provide enhanced security. For example, hackers who gain access to an unsegmented network (commonly through phishing) can move laterally across the network to access databases containing valuable assets such as sensitive personal information or financial records. Malicious lateral movement can be difficult to detect because it oftentimes appears as normal network traffic. By implementing adequate network segmentation, companies can prevent even those hackers who already gained a foothold in their network from moving across databases to access their most sensitive data.

232. Network segmentation is commonly used in conjunction with the principle of least privilege (POLP), which is a security practice that limits employees' privileges to the minimum necessary to perform the job or task. In an IT environment, adhering to POLP reduces the risk of hackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.[62] In an example given by security software provider Digital Guardian:

> [A]n employee whose job is to enter info into a database only needs the ability to add records to that database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root access privileges, however, the infection can spread system-wide.[63]

233. This is precisely why approximately 67% of targeted malware and stolen credential schemes are directed at individual contributors and lower-level management personnel.[64]

234. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;

---

[62] Nate Lord, *What is the Principle of Least Privilege (POLP)?* (May 6, 2023), https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance.

[63] *Id.*

[64] Jessica Davis, *Pharmaceutical Companies Most Targeted Industry by Cybercriminals* (Nov. 30, 2018), https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals.

- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;

- Ensuring devices are properly configured and that security features are enabled;

- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and

- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[65]

235. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[66]

236. Despite holding and sharing the PII/PHI of millions of patients, HealthEC failed to adhere to these recommended practices. And Provider Defendants failed to confirm that HealthEC adhered to these recommended best practices. Indeed, had Defendants taken necessary steps to inspect, inquire, and

[65] CISA Guide at 4.
[66] *Id.* at 5.

require documentation from HealthEC that it implemented and maintained adequate security measures in order to protect the Class's PII/PHI, then hackers never could have accessed millions of patient files, and the breach would have been prevented or much smaller in scope.

Defendants Failed to Follow FTC Guidelines

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

238. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for data security principles and practices businesses must use.[67] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

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

240. Furthermore, the FTC explains that companies must:

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

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

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

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

242. In short, HealthEC's failure to use reasonable and appropriate measures (and Provider Defendants' failure to ensure HealthEC implemented appropriate measures) to protect against unauthorized access to its current and former patients' and employees' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

243. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendants. These industry standards include: educating all employees, strong passwords, multi-layer security including firewalls, anti-virus, and anti-malware software, encryption (making data unreadable without a key), multi-factor authentication, backup data, and limiting which employees can access sensitive data.

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

245. HealthEC failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without

limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness. And Provider Defendants failed to ensure that HealthEC met these minimum standards before providing the Class's PII/PHI to HealthEC.

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

Defendants Violated HIPAA

247. 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.[68]

[68] 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.

248. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI is properly maintained.[69]

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

a. failing to ensure the confidentiality and integrity of electronic PII/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 PII/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 PII/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 Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

[69] *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).

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PII/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 PII/PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PII/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 PII/PHI, in compliance with 45 C.F.R. § 164.530(c).

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

CLASS ACTION ALLEGATIONS

I. NATIONWIDE CLASS

251. Pursuant to Fed. R. Civ. P. 23, Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All individuals whose personal information was compromised in the Data Breach announced by HealthEC in December 2023 (the "Class").

252. The Nationwide Class asserts claims against each Defendant for negligence (Count 1), negligence *per se* (Count 2), and invasion of privacy (Count 3). The Nationwide Class also asserts a claim for declaratory judgment (Count 19).

II. STATEWIDE SUBCLASSES

253. Pursuant to Fed. R. Civ. P. 23, Plaintiffs seek certification of state-by-state-claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 4 through 18; 20 through 23), on behalf of separate statewide subclasses for each State (the "Statewide Subclasses"), defined as follows:

> All individuals residing in [name of state] whose personal information was compromised in the Data Breach announced by HealthEC in December 2023 ("Statewide Subclass").
>
> All individuals whose personal information that was provided to [name of Provider Defendant] was compromised in the Data Breach announced by HealthEC in December 2023 ("Provider Subclass").

254. Excluded from the Nationwide Class and each Statewide Subclass are Defendants, any entity in which either Defendant has a controlling interest, and either Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Statewide Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

255. Class Identity: The members of the Class are readily identifiable and ascertainable. Defendants and/or their affiliates, among others, possess the information to identify and contact Class Members.

256. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. Defendants' disclosures reveal that the Class contains more than 4.6 million individuals whose PII/PHI was compromised in the Data Breach.

257. Typicality: Plaintiffs' claims are typical of the claims of the members of the Class because all Class Members had their PII/PHI compromised in the Data Breach and were harmed as a result.

258. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and their interests are aligned with Class Members's interests. Plaintiffs were subject to the same Data Breach as Class Members, suffered similar harms, and face similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including data breach cases involving multiple classes and data breach claims.

259. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class Members. The common questions of law and fact include, without limitation:

a. Whether HealthEC owed Plaintiffs and Class Members a duty to implement and maintain reasonable security procedures and practices to protect the Class's PII/PHI;

b. Whether Provider Defendants owed Plaintiffs and Class Members a duty to exercise due care in partnering with and conducting oversight over HealthEC to ensure it maintained adequate data security to protect Plaintiffs' and Class Members's PII/PHI;

c. Whether Defendants received a benefit without proper restitution making it unjust for Defendants to retain the benefit without commensurate compensation;

d. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class Members's PII/PHI;

e. Whether Provider Defendants violated their duty to exercise due care in partnering with and conducting oversight over HealthEC to ensure it maintained adequate data security to protect Plaintiffs' and Class Members's PII/PHI;

f. Whether HealthEC's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class Members;

g. Whether Provider Defendants' breach of their duty to exercise due care and conduct oversight over HealthEC's data security practices directly and/or proximately caused damages to Plaintiffs and Class Members;

h. Whether Defendants adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

i. Whether Plaintiffs and Class Members are entitled to damages to pay for future protective measures like credit monitoring;

j. Whether Defendants provided timely notice of the Data Breach to Plaintiffs and Class members; and

k. Whether Class Members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

260. Defendants have engaged in a common course of conduct and Plaintiffs and Class Members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect patients' PII/PHI, as well as Defendant's failure to timely alert affected customers to the Data Breach.

261. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal

litigation. Absent a class action, most, if not all, Class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class Members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

COUNT I
NEGLIGENCE
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

262. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

263. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members's PII/PHI within their control from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Further, Defendants owed a duty of care to Plaintiffs and Class Members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the PII/PHI.

264. Defendants knew or should have known the risks of collecting and storing Plaintiffs' and all other Class Members's PII/PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that targeted healthcare providers—and their vendors/business associates—that collect and store PII/PHI in recent years.

265. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems or their third-party vendor's systems and prevented the Data Breach from occurring.

266. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members's PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class Members's PII/PHI.

267. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members's PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data

security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members's PII/PHI to unauthorized individuals.

268. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their PII/PHI would not have been compromised.

269. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, 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 PII/PHI; (iii) out-of-pocket expenses associated with the monitoring, prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) overpayment for the services that were received without adequate data security; and (viii) nominal damages.

COUNT II
NEGLIGENCE PER SE
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

270. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

271. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

272. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as BACO, of failing to employ reasonable measures to protect and secure PII/PHI.

273. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to, or contracting with companies that failed to, use reasonable measures to protect Plaintiffs' and other Class Members's PII/PHI, by failing to provide timely notice, and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the

nature and amount of PII/PHI they obtain and store, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

274. Defendants' violation of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

275. Plaintiffs and Class Members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

276. The harm occurring as a result of the Data Breach is the type of harm that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class Members as a result of the Data Brach.

277. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members's PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and

hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' PII/PHI to unauthorized individuals.

278. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendants' violations of the HIPAA Privacy and Security Rules and Section 5 of the FTCA. 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 PII/PHI; (iii) out-of-pocket expenses associated with the monitoring, prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) overpayment for the services that were received without adequate data security; and (viii) nominal damages.

COUNT III
INVASION OF PRIVACY
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

279. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

280. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII/PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

281. Plaintiffs and Class Members took reasonable efforts to ensure their PII/PHI would remain unknown and undisclosed to the general public prior to the Data Breach.

282. Plaintiffs' and Class Members's PII/PHI is not of legitimate concern to the general public.

283. Defendants owed a duty to Plaintiffs and Class Members to keep their PII/PHI confidential.

284. Defendants invaded Plaintiffs' and Class Members's right to privacy by failing to adequately protect and maintain the confidentiality of Plaintiffs' and Class Members's PII/PHI and exposing their PII/PHI to unauthorized persons without Plaintiffs' and Class Members's consent.

285. The unauthorized release to, custody of, and examination of Plaintiffs' and Class Members's PII/PHI by unauthorized third parties is highly

offensive to Plaintiffs, Class Members, and to a reasonable person of ordinary sensibilities.

286. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs' and Class Members' PII/PHI was disclosed to Defendants in connection with receiving medical care and treatment or other benefits. Plaintiffs and Class Members disclosed their PII/PHI to Defendants privately and with the intention that their PII/PHI would be kept confidential and would be protected from unauthorized access and disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

287. Defendants failed to protect Plaintiffs' and Class Members's PII/PHI and exposed this highly-sensitive information to unauthorized persons in the Data Breach.

288. The Data Breach constitutes an intentional or reckless interference by Defendants with Plaintiffs' and Class Members's interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, or private quarters, of a kind that would be highly offensive to a reasonable person.

289. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they had actual knowledge that their data security practices were inadequate and insufficient.

290. Defendants acted with reckless disregard for Plaintiffs' and Class Members's privacy when they allowed unauthorized persons to access their systems containing Plaintiffs' and Class Members's PII/PHI.

291. Defendants were aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies and practices to prevent the unauthorized release of Plaintiffs' and Class Members's PII/PHI.

292. Because Defendants acted with this knowing state of mind, they had notice and knew their inadequate and insufficient data security practices would cause injury and harm to Plaintiffs and Class Members.

293. As a direct and proximate result of Defendant's above acts, Plaintiffs' and Class Members's PII/PHI was viewed, distributed, and used by persons without prior authorization and Plaintiffs and Class Members suffered damages as described herein

294. As a direct and proximate result of the Defendants' invasion of privacy—intrusion into seclusion, Plaintiffs and Class Members have suffered and imminently will suffer actual, tangible, injury-in-fact and damages, including, without limitation: loss of the opportunity to control how their PII/PHI is used; diminution in value of their PII/PHI; the compromise and continuing publication of their PII/PHI; out-of-pocket expenses associated with

the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to monitor, prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen PII/PHI; the continued risk to their PII/PHI, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII/PHI in its possession; and increased risk of fraud and identity theft.

COUNT IV
BREACH OF CONTRACT
Against Beaumont ACO On Behalf of Beaumont ACO Subclass

295. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

296. Beaumont ACO disseminated a "Notice of Privacy Practices" and "Code of Conduct" to its patients which constitutes an agreement between Beaumont ACO and persons who provided their PII/PHI to Beaumont ACO, including Beaumont ACO Subclass.

297. Beaumont ACO Subclass formed a contract with Beaumont ACO and complied with all obligations under such contract when they provided PII/PHI to Beaumont ACO subject to the Notice of Privacy Practices and Code of Conduct.

298. Beaumont ACO promised in the Notice of Privacy Practices and Code of Conduct that "Protected health information collected to provide care for a patient is confidential" and that "We enforce policies and procedures that protect confidential information from unauthorized use and disclosure."

299. Beaumont ACO breached its agreements with Beaumont ACO Subclass when Beaumont ACO allowed for the disclosure of Beaumont ACO Subclasses' PII/PHI without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in the Notice of Privacy Practices and Code of Conduct, as well as when it failed to maintain the confidentiality of Plaintiffs' and Class Members's medical and treatment information.

300. As a direct and proximate result of these breaches, Plaintiffs and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT V
BREACH OF IMPLIED CONTRACT
Against Beaumont ACO On Behalf of Beaumont ACO Subclass

301. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs and assert this claim in the alternative to their breach of contract claim to the extent necessary.

302. Beaumont ACO Subclass was required to provide their PII/PHI to Beaumont ACO in order to receive healthcare services and treatment.

303. As part of these transactions, Beaumont ACO agreed to safeguard and protect the PII/PHI of the Beaumont ACO Subclass. Implicit in these transactions between Beaumont ACO and Class Members was the obligation that Defendants would use the PII/PHI for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

304. Additionally, Beaumont ACO implicitly promised to retain this PII/PHI only under conditions that kept such information secure and confidential and, therefore, had a duty to reasonably safeguard and protect the PII/PHI of Beaumont ACO Subclass from unauthorized disclosure or access.

305. Beaumont ACO Subclass entered into implied contracts with the reasonable expectation that Beaumont ACO data security practices and policies were

reasonable and consistent with industry standards, including ensuring its vendors maintained adequate security measures. Beaumont ACO Subclass believed that Beaumont ACO would use part of the monies paid to it under the implied contracts to fund adequate and reasonable data security practices to protect their PII/PHI.

306. Beaumont ACO Subclass would not have provided and entrusted their PII/PHI to Beaumont ACO or would have paid less for Beaumont ACO's services in the absence of the implied contract between them and Beaumont ACO. The safeguarding of Beaumont ACO Subclasses's PII/PHI was critical to realizing the intent of the parties.

307. The nature of Beaumont ACO's implied promise itself—the subject matter of the contractual provision at issue—was to protect Beaumont ACO Subclasses's PII/PHI in order to prevent harm and prevent present and continuing increased risk.

308. Beaumont ACO breached its implied contract with Beaumont ACO Subclass by failing to reasonably safeguard and protect Beaumont ACO Subclasses's PII/PHI and failing to supervise and ensure HealthEC maintained adequate data security for the protection of Beaumont ACO Subclasses's PII/PHI consistent with industry standards, which was compromised as a result of the Data Breach.

309. As a direct and proximate result of Beaumont ACO's breaches, Beaumont ACO Subclass sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT VI
BREACH OF FIDUCIARY DUTY
Against Beaumont ACO On Behalf of Beaumont ACO Subclass

310. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

311. Beaumont ACO Subclass gave Beaumont ACO their PII/PHI in trust and confidence, believing that Beaumont ACO would protect that information. Beaumont ACO Subclass would not have provided Beaumont ACO with this information had they known it would not be adequately protected. Beaumont ACO's acceptance and storage of Beaumont ACO Subclasses's PII/PHI created a fiduciary relationship between Beaumont ACO and Beaumont ACO Subclass. In light of this relationship, Beaumont ACO must act primarily for the benefit of its patients, which includes safeguarding and protecting Beaumont ACO Subclasses's PII/PHI.

312. Due to the nature of the relationship between Beaumont ACO and Beaumont ACO Subclass, Beaumont ACO Subclass were entirely reliant upon Beaumont ACO to ensure that their PII/PHI was adequately protected. Beaumont ACO Subclass had no way of verifying or influencing the nature and extent of

Beaumont ACO's or its vendors' data security policies and practices, and Beaumont ACO was in an exclusive position to guard against the Data Breach.

313. Beaumont ACO has a fiduciary duty to act for the benefit of Beaumont ACO Subclass upon matters within the scope of their relationship. Beaumont ACO breached that duty by contracting with companies that failed to properly protect the integrity of the system containing Beaumont ACO Subclasses's PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Beaumont ACO Subclasses's PII/PHI that they collected.

314. As a direct and proximate result of Beaumont ACO Subclasses's breaches of its fiduciary duties, Beaumont ACO Subclass 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 PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Beaumont ACO's possession; (vi) future costs in terms of time, effort, and money that will be required to monitor, prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) overpayment for the services that were received without adequate data security; and (viii) nominal damages.

COUNT VII
UNJUST ENRICHMENT
Against Beaumont ACO On Behalf of Beaumont ACO Subclass

315. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

317. Beaumont ACO Subclass conferred a monetary benefit upon Beaumont ACO in the form of monies paid to their Beaumont ACO for healthcare services, which the Beaumont ACO used in turn for commercial gain.

318. Beaumont ACO accepted or had knowledge of the benefits conferred upon them by Beaumont ACO Subclass.

319. As a result of Beaumont ACO's conduct, Beaumont ACO Subclasssuffered actual damages in an amount equal to the difference in value between their payments made for services with reasonable data privacy and security practices and procedures that Beaumont ACO Subclass paid for and those services without reasonable data privacy and security practices and procedures that they received.

320. Beaumont ACO should not be permitted to retain the money belonging to Beaumont ACO Subclass because Beaumont ACO failed to adequately implement the data privacy and security procedures for themselves that Beaumont ACO

Subclass paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

321. Beaumont ACO Subclass have no adequate remedy at law.

322. Beaumont ACO should be compelled to provide for the benefit of Beaumont ACO Subclass all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT VIII
BREACH OF CONTRACT
Against Community Health Care Systems On Behalf of Community Health Care Systems Subclass

323. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

324. Community Health Care Systems disseminated a "Notice of Privacy Practices" to its patients which constitutes an agreement between Community Health Care Systems and persons who provided their PII/PHI to Community Health Care Systems, including Community Health Care Systems Subclass.

325. Community Health Care Systems Subclass formed a contract with Community Health Care Systems and complied with all obligations under such contract when they provided PII/PHI to Community Health Care Systems subject to the Notice of Privacy Practices.

326. Community Health Care Systems promised in the Notice of Privacy Practices that "[t]he law requires us to: make sure that medical information that

identifies you is kept private" and "[o]ther uses and disclosures of medical information not covered by this notice or the laws that apply to use will be made only with your written authorization."

327. Community Health Care Systems breached its agreements with Community Health Care Systems Subclass when Community Health Care Systems allowed for the disclosure of Community Health Care Systems Subclasses's PII/PHI without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in the Notice of Privacy Practices, as well as when it failed to maintain the confidentiality of Community Health Care Systems Subclasses's medical and treatment information.

328. As a direct and proximate result of these breaches, Community Health Care Systems Subclass sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Community Health Care Systems Subclass alternatively seek an award of nominal damages.

COUNT IX
BREACH OF IMPLIED CONTRACT
Against Community Health Care Systems On Behalf of Community Health Care Systems Subclass

329. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs and assert this claim in the alternative to their breach of contract claim to the extent necessary.

330. Community Health Care Systems Subclass was required to provide their PII/PHI to Community Health Care Systems in order to receive healthcare services and treatment.

331. As part of these transactions, Community Health Care Systems agreed to safeguard and protect the PII/PHI of Community Health Care Systems Subclass. Implicit in these transactions between Community Health Care Systems and Class Members was the obligation that Community Health Care Systems would use the PII/PHI for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

332. Additionally, Community Health Care Systems implicitly promised to retain this PII/PHI only under conditions that kept such information secure and confidential and, therefore, had a duty to reasonably safeguard and protect the PII/PHI of Community Health Care Systems Subclass from unauthorized disclosure or access.

333. Community Health Care Systems entered into implied contracts with the reasonable expectation that Community Health Care Systems data security practices and policies were reasonable and consistent with industry standards, including ensuring its vendors maintained adequate security measures. Community Health Care Systems Subclass believed that Community Health Care Systems would

use part of the monies paid to it under the implied contracts to fund adequate and reasonable data security practices to protect their PII/PHI.

334. Community Health Care Systems Subclass would not have provided and entrusted their PII/PHI to Community Health Care Systems or would have paid less for Community Health Care Systems's services in the absence of the implied contract between them and Community Health Care Systems. The safeguarding of Community Health Care Systems Subclasses's PII/PHI was critical to realizing the intent of the parties.

335. The nature of Community Health Care Systems's implied promise itself—the subject matter of the contractual provision at issue—was to protect Community Health Care Systems Subclasses's PII/PHI in order to prevent harm and prevent present and continuing increased risk.

336. Community Health Care Systems breached its implied contract with Community Health Care Systems Subclass by failing to reasonably safeguard and protect Community Health Care Systems's PII/PHI and failing to supervise and ensure HealthEC maintained adequate data security for the protection of Community Health Care Systems Subclasses's PII/PHI consistent with industry standards, which was compromised as a result of the Data Breach.

337. As a direct and proximate result of Community Health Care Systems's breaches, Community Health Care Systems Subclass sustained actual losses and

damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT X
BREACH OF FIDUCIARY DUTY
Against Community Health Care Systems On Behalf of Community Health Care Systems Subclass

338. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

339. Community Health Care Systems Subclass gave Community Health Care Systems their PII/PHI in trust and confidence, believing that Community Health Care Systems would protect that information. Community Health Care Systems Subclass would not have provided Community Health Care Systems with this information had they known it would not be adequately protected. Community Health Care Systems' acceptance and storage of Community Health Care Systems Subclasses's PII/PHI created a fiduciary relationship between Community Health Care Systems and Community Health Care Systems Subclass. In light of this relationship, Community Health Care Systems must act primarily for the benefit of its patients, which includes safeguarding and protecting Community Health Care Systems Subclasses's PII/PHI.

340. Due to the nature of the relationship between Community Health Care Systems and Community Health Care Systems Subclass, Community Health Care

Systems Subclass were entirely reliant upon Community Health Care Systems to ensure that their PII/PHI was adequately protected. Community Health Care Systems Subclass had no way of verifying or influencing the nature and extent of Community Health Care Systems's or its vendors' data security policies and practices, and Community Health Care Systems was in an exclusive position to guard against the Data Breach.

341. Community Health Care Systems has a fiduciary duty to act for the benefit of Community Health Care Systems Subclass upon matters within the scope of their relationship. Community Health Care Systems breached that duty by contracting with companies that failed to properly protect the integrity of the system containing Community Health Care Systems Subclasses's PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Community Health Care Systems Subclasses's PII/PHI that they collected.

342. As a direct and proximate result of Community Health Care Systems's breaches of its fiduciary duties, Community Health Care Systems Subclass 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 PII/PHI; (iii) out-of-pocket expenses associated with the monitoring, prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity

costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Community Health Care Systems'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 PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT XI
UNJUST ENRICHMENT
Against Community Health Care Systems On Behalf of Community Health Care Systems Subclass

343. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

345. Community Health Care Systems Subclass conferred a monetary benefit upon Community Health Care Systems in the form of monies paid to their Community Health Care Systems for healthcare services, which Community Health Care Systems used in turn for commercial gain.

346. Community Health Care Systems accepted or had knowledge of the benefits conferred upon them by Community Health Care Systems Subclass.

347. As a result of Community Health Care Systems' conduct, Community Health Care Systems Subclass suffered actual damages in an amount equal to the

difference in value between their payments made for services with reasonable data privacy and security practices and procedures that Community Health Care Systems Subclass paid for and those services without reasonable data privacy and security practices and procedures that they received.

348. Community Health Care Systems should not be permitted to retain the money belonging to Community Health Care Systems Subclass because Community Health Care Systems failed to adequately implement the data privacy and security procedures for themselves that Community Health Care Systems Subclass paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

349. Community Health Care Systems Subclass have no adequate remedy at law.

350. Community Health Care Systems should be compelled to provide for the benefit of Community Health Care Systems Subclass all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT XII
BREACH OF CONTRACT
Against Corewell Health On Behalf of Corewell Health Subclass

351. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

352. Corewell Health disseminated a "Notice of Privacy Practices" to its patients which constitutes an agreement between Corewell Health and persons who provided their PII/PHI to Corewell Health, including Corewell Health Subclass.

353. Corewell Health Subclass formed a contract with Corewell Health and complied with all obligations under such contract when they provided PII/PHI to Corewell Health subject to the Notice of Privacy Practices.

354. Corewell Health promised in the Notice of Privacy Practices that it would only disclose patients' PII/PHI under certain circumstances and "[o]ther uses and disclosures of health information not covered by this notice or the laws that apply to Corewell Health will only be made with your written permission."

355. Corewell Health breached its agreements with Corewell Health Subclass when Corewell Health allowed for the disclosure of Corewell Health Subclasses's PII/PHI without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in the Notice of Privacy Practices, as well as when it failed to maintain the confidentiality of Plaintiffs' and Class Members's medical and treatment information.

356. As a direct and proximate result of these breaches, Plaintiffs and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT XIII
BREACH OF IMPLIED CONTRACT
Against Corewell Health On Behalf of Corewell Health Subclass

357. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs and assert this claim in the alternative to their breach of contract claim to the extent necessary.

358. Corewell Health Subclass was required to provide their PII/PHI to Corewell Health in order to receive healthcare services and treatment.

359. As part of these transactions, Corewell Health agreed to safeguard and protect the PII/PHI of Corewell Health Subclass. Implicit in these transactions between Corewell Health and Class Members was the obligation that Corewell Health would use the PII/PHI for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

360. Additionally, Corewell Health implicitly promised to retain this PII/PHI only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII/PHI of Corewell Health Subclass from unauthorized disclosure or access.

361. Corewell Health Subclass entered into implied contracts with the reasonable expectation that Corewell Health's data security practices and policies were reasonable and consistent with industry standards, including ensuring its

vendors maintained adequate security measures. Corewell Health Subclass believed that Corewell Health would use part of the monies paid to it under the implied contracts to fund adequate and reasonable data security practices to protect their PII/PHI.

362. Corewell Health Subclass would not have provided and entrusted their PII/PHI to Corewell Health or would have paid less for Corewell Health's services in the absence of the implied contract between them and Corewell Health. The safeguarding of Corewell Health Subclasses's PII/PHI was critical to realizing the intent of the parties.

363. The nature of Corewell Health's implied promise itself—the subject matter of the contractual provision at issue—was to protect Corewell Health Subclasses's PII/PHI in order to prevent harm and prevent present and continuing increased risk.

364. Corewell Health breached its implied contract with Corewell Health Subclass by failing to reasonably safeguard and protect Corewell Health Subclasses's PII/PHI and failing to supervise and ensure HealthEC maintained adequate data security for the protection of Corewell Health Subclasses's PII/PHI consistent with industry standards, which was compromised as a result of the Data Breach.

365. As a direct and proximate result of Corewell Health's breaches, Corewell Health Subclass sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT XIV
BREACH OF FIDUCIARY DUTY
Against Corewell Health On Behalf of Corewell Health Subclass

366. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

367. Corewell Health Subclass gave Corewell Health their PII/PHI in trust and confidence, believing that Corewell Health would protect that information. Corewell Health Subclass would not have provided Corewell Health with this information had they known it would not be adequately protected. Corewell Health's acceptance and storage of Corewell Health Subclasses's PII/PHI created a fiduciary relationship between Corewell Health and Corewell Health Subclass. In light of this relationship, Corewell Health must act primarily for the benefit of its patients, which includes safeguarding and protecting Corewell Health Subclasses's PII/PHI.

368. Due to the nature of the relationship between Corewell Health and Corewell Health Subclass, Corewell Health Subclass were entirely reliant upon Corewell Health to ensure that their PII/PHI was adequately protected. Corewell Health Subclass had no way of verifying or influencing the nature and extent of

Corewell Health's or its vendors' data security policies and practices, and Corewell Health was in an exclusive position to guard against the Data Breach.

369. Corewell Health has a fiduciary duty to act for the benefit of Corewell Health Subclass upon matters within the scope of their relationship. Corewell Health breached that duty by contracting with companies that failed to properly protect the integrity of the system containing Corewell Health Subclasses's PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Corewell Health Subclasses's PII/PHI that they collected.

370. As a direct and proximate result of Corewell Health's breaches of its fiduciary duties, Corewell Health Subclass 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 PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Corewell Health's possession; (vi) future costs in terms of time, effort, and money that will be required to monitor, prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) overpayment for the services that were received without adequate data security; and (viii) nominal damages.

COUNT XV
UNJUST ENRICHMENT
Against Corewell Health On Behalf of Corewell Health Subclass

371. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

373. Corewell Health Subclass conferred a monetary benefit upon Corewell Health in the form of monies paid to Corewell Health for healthcare services, which Corewell Health used in turn for commercial gain.

374. Corewell Health accepted or had knowledge of the benefits conferred upon them by Corewell Health Subclass.

375. As a result of Corewell Health's conduct, Corewell Health Subclasses's suffered actual damages in an amount equal to the difference in value between their payments made for services with reasonable data privacy and security practices and procedures that Corewell Health Subclass paid for and those services without reasonable data privacy and security practices and procedures that they received.

376. Corewell Health should not be permitted to retain the money belonging to Corewell Health Subclass because Corewell Health failed to adequately implement the data privacy and security procedures for themselves that Corewell

Health Subclass paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

377. Corewell Health Subclass have no adequate remedy at law.

378. Corewell Health should be compelled to provide for the benefit of Corewell Health Subclass all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT XVI
BREACH OF IMPLIED CONTRACT
Against MD Valuecare On Behalf of MD Valuecare Subclass

379. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs and assert this claim in the alternative to their breach of contract claim to the extent necessary.

380. MD Valuecare Subclass was required to provide their PII/PHI to MD Valuecare in order to receive healthcare services and treatment.

381. As part of these transactions, MD Valuecare agreed to safeguard and protect the PII/PHI of MD Valuecare Subclass. Implicit in these transactions between MD Valuecare and Class Members was the obligation that MD Valuecare would use the PII/PHI for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

382. Additionally, MD Valuecare implicitly promised to retain this PII/PHI only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII/PHI of MD Valuecare Subclass from unauthorized disclosure or access.

383. MD Valuecare Subclass entered into implied contracts with the reasonable expectation that MD Valuecare data security practices and policies were reasonable and consistent with industry standards, including ensuring its vendors maintained adequate security measures. MD Valuecare Subclass believed that MD Valuecare would use part of the monies paid to it under the implied contracts to fund adequate and reasonable data security practices to protect their PII/PHI.

384. MD Valuecare Subclass would not have provided and entrusted their PII/PHI to MD Valuecare or would have paid less for MD Valuecare's services in the absence of the implied contract between them and MD Valuecare. The safeguarding of MD Valuecare Subclasses' PII/PHI was critical to realizing the intent of the parties.

385. The nature of MD Valuecare's implied promise itself—the subject matter of the contractual provision at issue—was to protect MD Valuecare Subclasses's PII/PHI in order to prevent harm and prevent present and continuing increased risk.

386. MD Valuecare breached its implied contract with MD Valuecare Subclass by failing to reasonably safeguard and protect MD Valuecare Subclasses'sPII/PHI and failing to supervise and ensure HealthEC maintained adequate data security for the protection of MD Valuecare Subclasses's PII/PHI consistent with industry standards, which was compromised as a result of the Data Breach.

387. As a direct and proximate result of MD Valuecare's breaches, MD Valuecare Subclass sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT XVII
BREACH OF FIDUCIARY DUTY
Against MD Valuecare On Behalf of MD Valuecare Subclass

388. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

389. MD Valuecare Subclass MD Valuecare their PII/PHI in trust and confidence, believing that MD Valuecare would protect that information. MD Valuecare Subclass would not have provided MD Valuecare with this information had they known it would not be adequately protected. MD Valuecare's acceptance and storage of MD Valuecare Subclasses's PII/PHI created a fiduciary relationship between MD Valuecare and MD Valuecare Subclass. In light of this relationship,

MD Valuecare must act primarily for the benefit of its patients, which includes safeguarding and protecting MD Valuecare Subclasses's PII/PHI.

390. Due to the nature of the relationship between MD Valuecare and MD Valuecare Subclass, MD Valuecare Subclass were entirely reliant upon MD Valuecare to ensure that their PII/PHI was adequately protected. MD Valuecare Subclass had no way of verifying or influencing the nature and extent of MD Valuecare's or its vendors' data security policies and practices, and MD Valuecare was in an exclusive position to guard against the Data Breach.

391. MD Valuecare has a fiduciary duty to act for the benefit of MD Valuecare Subclass upon matters within the scope of their relationship. MD Valuecare breached that duty by contracting with companies that failed to properly protect the integrity of the system containing MD Valuecare Subclasses's PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard MD Valuecare Subclasses's PII/PHI that they collected.

392. As a direct and proximate result of MD Valuecare's breaches of its fiduciary duties, MD Valuecare Subclass 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 PII/PHI; (iii) out-of-pocket expenses associated with the monitoring, prevention, detection, and recovery from

unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in MD Valuecare'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 PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT XVIII
UNJUST ENRICHMENT
Against MD Valuecare On Behalf of MD Valuecare Subclass

393. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

395. MD Valuecare Subclass conferred a monetary benefit upon MD Valuecare in the form of monies paid to their MD Valuecare for healthcare services, which the MD Valuecare used in turn for commercial gain.

396. MD Valuecare accepted or had knowledge of the benefits conferred upon them by MD Valuecare Subclass.

397. As a result of MD Valuecare's conduct, MD Valuecare Subclasses's suffered actual damages in an amount equal to the difference in value between their

payments made for services with reasonable data privacy and security practices and procedures that MD Valuecare Subclass paid for and those services without reasonable data privacy and security practices and procedures that they received.

398. MD Valuecare should not be permitted to retain the money belonging to MD Valuecare Subclass because MD Valuecare failed to adequately implement the data privacy and security procedures for themselves that MD Valuecare Subclass paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

399. MD Valuecare Subclass have no adequate remedy at law.

400. MD Valuecare should be compelled to provide for the benefit of MD Valuecare Subclass all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT XIX
DECLARATORY JUDGMENT
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

401. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

402. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority

to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

403. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard PII/PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further cyberattacks and data breaches that could compromise their PII/PHI.

404. Defendants still possess PII/PHI pertaining to Plaintiffs and Class Members, which means their PII/PHI remains at risk of further breaches because Defendants' data security measures remain inadequate. Plaintiffs and Class Members continue to suffer injuries as a result of the compromise of their PII/PHI and remain at an imminent risk that additional compromises of their PII/PHI will occur in the future.

405. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that:

a. Defendants' existing data security measures do not comply with their obligations and duties of care;

b. in order to comply with their obligations and duties of care, Defendants must have policies and procedures in place to ensure the parties with whom they share sensitive personal information maintain reasonable,

industry-standard security measures, including, but not limited to, those listed below and must comply with those policies and procedures;

c. Defendants must: (1) purge, delete, or destroy in a reasonably secure manner Plaintiffs' and Class Members's PII/PHI if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (2) implement and maintain reasonable, industry-standard security measures, including:

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

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

iii. Auditing, testing, and training their security personnel regarding any new or modified procedures;

iv. Encrypting PII/PHI and segmenting PII/PHI by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of its systems;

v. Purging, deleting, and destroying in a reasonable and secure manner PII/PHI not necessary to perform essential business functions;

vi. Conducting regular database scanning and security checks;

vii. Conducting regular employee education regarding best security practices;

viii. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

ix. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

COUNT XX
VIOLATIONS OF THE MICHIGAN CONSUMER PROTECTION ACT, Mich. Comp. Laws § 445.901, *et seq*.
On Behalf of the Michigan Subclass

406. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

407. Michigan Subclass and Defendants are each a "person" as defined in the Michigan Consumer Protection Act ("MCPA"). Mich. Comp. Laws § 445.902(d).

408. Defendants are each engaged in "trade or commerce" as defined in the MCPA in that they advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws § 445.902(g).

409. Defendants intentionally represented that their services included adequate data security practices and procedures that would ensure the safety of Michigan Subclasses's PII/PHI. However, Defendants' services did not include the promised adequate data security practices and procedures.

410. Defendants advertised their services as including adequate data security practices and procedures, when in fact the services did not include adequate data security practices and procedures, and Defendants did not intend to supply Plaintiffs and Class Members with services that included adequate data security practices and procedures, as advertised.

411. Defendants' conduct constitutes violations of the MCPA.

412. Defendants also engaged in unlawful and unfair practices in violation of the MCPA by failing to, or contracting with companies that failed to, implement and maintain reasonable security measures to protect and secure Michigan Subclasses's PII/PHI in a manner that complied with applicable laws, regulations, and industry standards.

413. Defendants had exclusive knowledge of material information regarding their deficient security policies and practices, as well as the security of Michigan Subclasses's PII/PHI. This exclusive knowledge includes, but is not limited to, information that Defendants received through internal and other non-public audits and reviews that concluded that Defendants' security policies were substandard and deficient, and that Michigan Subclasses's PII/PHI and other data was vulnerable.

414. Due to the Data Breach, Plaintiffs and Class Members have lost property in the form of their PII/PHI. Further, Defendants' failure to adopt, or

contracting with companies that failed to adopt, reasonable practices in protecting and safeguarding their patients' PII/PHI will force Michigan Subclass to spend time or money to protect against identity theft. Michigan Subclass are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

415. As a result of Defendants' violations of the MCPA, Michigan Subclass 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 PII/PHI; (iii) out-of-pocket expenses associated with the monitoring, prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to monitor, prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT XXI
VIOLATIONS OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. § 501.201, *et seq.*
On Behalf of the Florida Subclass

416. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

417. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). Fla. Stat. § 501.201, *et seq.* The express purpose of the FDUPTA is to "protect the consuming public . . . from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

418. Florida Subclass are "consumers" as defined in FDUTPA, Fla. Stat. § 501.203(7).

419. At all relevant times, Defendants were each engaged in "trade or commerce" as defined in FDUTPA by advertising, soliciting, providing, offering, or distributing services, goods, or other things of value. *See* Fla. Stat. § 501.203(8).

420. It is unlawful to engage in "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce" under FDUTPA. Fla. Stat. § 501.204(1).

421. As set forth above, Defendants engaged in unfair and deceptive acts or practices, including but not limited to:

a. Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Florida Subclasses's PII/PHI;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Florida Subclasses's PII/PHI, including duties imposed by the HIPAA Privacy Rule, Section 5 of the FTCA, and Florida's data security statute, Fla. Stat.§ 501.171;

c. Failing to properly protect the integrity of the systems containing Florida Subclasses's PII/PHI;

d. Failing to prevent the unauthorized access or disclosure of Florida Subclasses's PII/PHI;

e. Failing to timely disclose the Data Breach to Florida Subclass;

f. Misrepresenting that they would protect the privacy and confidentiality of Florida Subclasses's PII/PHI, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Florida Subclasses's PII/PHI, including duties imposed by the HIPAA Privacy Rule, Section 5 of the FTCA, and Florida's data security statute, Fla. Stat.§ 501.171;

h. Omitting, suppressing, and concealing the material fact that they did not properly secure Florida Subclasses's PII/PHI;

i. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Florida

Subclasses's PII/PHI, including duties imposed by the HIPAA Privacy Rule, Section 5 of the FTCA, and Florida's data security statute, Fla. Stat.§ 501.171; and

j. Overcharging for services provided without adequate data security measures in place.

422. Defendants engaged in these or other unfair and deceptive acts or practices in the course of trade or commerce.

423. Defendants' unfair and deceptive acts or practices, as described herein, were the direct and proximate cause of the Data Breach.

424. As a direct and proximate result of Defendants' unfair acts or practices, Florida Subclass Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT XXII
VIOLATIONS OF THE GEORGIA FAIR BUSINESS PRACTICES ACT, O.C.G.A. § 10-1-390, *et seq.*
On Behalf of the Georgia Subclass

425. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

426. Georgia Subclass and Defendants are all "persons" as defined in the Georgia Fair Business Practices Act ("GFBPA"). O.C.G.A. § 10-1-392(a)(24). Georgia Subclass are each a "consumer" under the GFBPA. O.C.G.A. § 10-1-392(a)(6).

427. At all relevant times, Defendants were each engaged in "trade" or "commerce" as defined in the GFBPA by advertising or selling goods or services. *See* O.C.G.A. § 10-1-392(a)(28).

428. The GFBPA states "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce are declared unlawful." O.C.G.A. § 10-1-193(a).

429. As set forth herein, Defendants engaged in unfair and deceptive acts or practices, including but not limited to:

a. Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Georgia Subclasses's PII/PHI;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Georgia Subclasses's PII/PHI, including duties imposed by the HIPAA Privacy Rule and Section 5 of the FTCA;

c. Failing to properly protect the integrity of the systems containing Georgia Subclasses's PII/PHI;

d. Failing to prevent the unauthorized access or disclosure of Georgia Subclasses's PII/PHI;

e. Failing to timely disclose the Data Breach to Georgia Subclass ;

f. Misrepresenting that they would protect the privacy and confidentiality of Georgia Subclasses's PII/PHI, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Georgia Subclasses's PII/PHI, including duties imposed by the HIPAA Privacy Rule and Section 5 of the FTCA;

h. Omitting, suppressing, and concealing the material fact that they did not properly secure Georgia Subclasses's PII/PHI;

i. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Georgia Subclasses's PII/PHI, including duties imposed by the HIPAA Privacy Rule and Section 5 of the FTCA; and

j. Overcharging for services provided without adequate data security measures in place.

430. Defendants engaged in these or other unfair and deceptive acts or practices in the course of trade or commerce.

431. Defendants' unfair and deceptive acts or practices, as described herein, were the direct and proximate cause of the Data Breach.

432. As a direct and proximate result of Defendants' unfair acts or practices, Georgia Subclass have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT XXIII
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-1, *et seq.*
On Behalf of Plaintiffs and the Nationwide Class

433. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

434. Plaintiffs, Class Members, and Defendants are each a "person" within the meaning of the New Jersey Consumer Fraud Act ("NJCFA"). N.J.S.A. § 56:8-1(d).

435. At all relevant times, Defendants were engaged in the advertising and sale of merchandise and services, as those terms are defined in the NJCFA. N.J.S.A. *See* § 56:8-1.

436. Under the CFA, the "act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice." N.J.S.A. § 56:8-2.

437. The NJCFA further forbids the "advertisement of merchandise as part of a plan or scheme not to sell the item or service so advertised." N.J.S.A. § 56:8-2.2.

438. As set forth herein, Defendants engaged in unfair and deceptive acts or practices, including but not limited to:

a. Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members's PII/PHI;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members's PII/PHI, including duties imposed by the HIPAA Privacy Rule and Section 5 of the FTCA;

c. Failing to properly protect the integrity of the systems containing Plaintiffs' and Class Members's PII/PHI;

d. Failing to prevent the unauthorized access or disclosure of Plaintiffs' and Class Members's PII/PHI;

e. Failing to timely disclose the Data Breach to Plaintiffs and Class Members;

f. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs 'and Class Members's PII/PHI, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members's PII/PHI, including duties imposed by the HIPAA Privacy Rule and Section 5 of the FTCA;

h. Omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiffs' and Class Members's PII/PHI;

i. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII/PHI, including duties imposed by the HIPAA Privacy Rule and Section 5 of the FTCA; and

j. Overcharging for services provided without adequate data security measures in place.

439. Defendants knowingly represented they would protect Plaintiffs' and Class Members's PII/PHI despite not having adequate protections in place to induce Plaintiffs and Class Members to purchase their merchandise or services.

440. Defendants' concealments, omissions, and false promises induced Plaintiffs and Class Members to purchase Defendants' merchandise or services. But for these unlawful acts by Defendants, Plaintiffs and Class Members would not have entrusted Defendants with their PII/PHI.

441. Defendants engaged in unfair or deceptive acts in violation of the NJCFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class Members' PII/PHI in a manner that complied with applicable laws, regulations, and industry standards, as they represented they would.

442. As a direct and proximate result of Defendants' unfair acts or practices, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the monitoring, prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv)

lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to monitor, prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

REQUESTS FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

1. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiffs as class representatives and Plaintiffs' counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

4. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

5. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

6. That Plaintiffs be granted the declaratory and injunctive relief sought herein;

7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

8. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: April 30, 2024

Respectfully,

/s/James E. Cecchi
James Cecchi
CARELLA, BRYNE, CECCHI, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
Telephone: (973) 994-1700
jcecchi@carellabyrne.com

Plaintiffs' Liaison Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com

Executive Committee Chair

Sabita J. Soneji
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808
ssoneji@tzlegal.com

James J. Pizzirusso
HAUSFELD LLP
888 16th Street, N.W., Suite 300
Washington, D.C. 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeld.com

Jean S. Martin
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street,
Tampa, FL 33602
Telephone: (813) 223-5505
jeanmartin@forthepeople.com

Christopher L. Ayers
SEEGER WEISS LLP
55 Challenger Rd., 6th Floor
Ridgefield Park, NJ 07660
Telephone: (973) 639-9100
cayers@seegerweiss.com

Vicki Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
100 Garden City Plaza, Suite 500
Garden City, NY 11530
Tel.: (866) 252-0878
vmaniatis@milberg.com

Plaintiffs' Executive Committee