UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

IN RE: FORTRA FILE TRANSFER SOFTWARE DATA SECURITY BREACH LITIGATION **This Document Relates to: Track Four**	Case No. 24-md-03090-RAR MDL No. 3090

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Sandra Kuffrey, Angela Martin, Lola Tatum, Glenda G. Corn, Wilhelmina Gill, Brandy McGowen, Kelly Kern, and Timothy Ferguson (collectively, the "Community Plaintiffs"), on behalf of themselves and those similarly situated, bring their claims against Defendants Community Health Systems, Inc. ("CHS"), and CHSPSC, LLC ("CHSPSC") (collectively, the "Community Defendants");

Plaintiffs Terrance Rosa, Ryan Watson, Donisha Jackson, Kyle Castro, on behalf of himself and his minor children, E.N.C., C.J.C., and E.J.C., Itaunya Milner, on behalf of herself and her minor child, B.G., and Anthony Ndifor (collectively, the "Brightline Plaintiffs"), on behalf of themselves and those similarly situated, bring their claims against Defendant Brightline, Inc. ("Brightline");

Plaintiffs Anthony Collins and Dawn McGee (collectively, the "Imagine360 Plaintiffs"), on behalf of themselves and those similarly situated, bring their claims against Defendant Imagine360, LLC ("Imagine360"); and

Plaintiffs Lauren Perrone, Victoria Evans, Thomas Kelly, Jose Cabrales, Nicholas Timmons, Kristi McDavitt, Robert Terwilliger, and Edwin Rodriguez (collectively, the "Intellihartx Plaintiffs"), on behalf of themselves and those similarly situated, bring their claims

against Defendant Intellihartx, LLC ("ITx" or "Intellihartx"), and allege as follows based upon personal knowledge as to Plaintiffs themselves, and information and belief as to all other matters.[1]

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard their personally identifying information ("PII") and personal health information ("PHI"), including names, dates of birth, addresses, medical billing and insurance information, medical diagnoses, prescription information, member identification numbers, stat and end dates of health plan coverage, employer names, and Social Security numbers (collectively, "PII/PHI").

2. On February 2, 2023, Defendants were notified that one of the vendors with which they had contracted—Fortra, LLC ("Fortra"), the provider of file transfer software, GoAnywhere MFT, used by Defendants—experienced a data breach between January 28, 2023 and January 30, 2023. Unauthorized individual(s) breached Fortra's network systems and accessed and acquired files containing the PII and PHI of Defendants' and their affiliates' patients and employees, including Plaintiffs and Class members (the "Data Breach" or "Breach").

3. Each of the Defendants named in this Complaint owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. They breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their patients' and employees' PII/PHI from unauthorized access and disclosure.

[1] Unless otherwise specified, the Community Defendants, Brightline, Imagine360, and Intellihartx will be collectively referred to herein as Defendants. The named Plaintiffs in each of the foregoing cases will be collectively referred to herein as Plaintiffs.

4. As a result of Defendants' negligence, including inadequate vendor screening, and inadequate security measures including their failures to ensure Fortra maintained adequate data security, and breach of their legal duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII/PHI was exposed because of the Data Breach.

5. Plaintiffs, on behalf of themselves and all other Class members seek to represent Plaintiffs and Class members who assert claims herein against their respective named Defendants concerning the Data Breach for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, breach of contracts to which Plaintiffs and Class Members are intended third party beneficiaries, violations of state statutes, including several state consumer fraud statutes, and unjust enrichment. Plaintiffs seek declaratory, injunctive, and equitable relief including monetary, statutory, and punitive damages, and all other relief authorized by law.

PARTIES

Community Plaintiff Sandra Kuffrey

6. Plaintiff Sandra Kuffrey is a citizen of Tennessee.

7. Plaintiff Kuffrey was employed by Tennova Healthcare – Cleveland, an affiliate of Community Defendants, and obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants. As a condition of her employment and receiving these services, Community Defendants required her to provide Defendants with her PII/PHI.

8. Based on representations made by Defendants, Plaintiff Kuffrey believed that the Community Defendants had implemented and maintained reasonable security practices to protect her PII/PHI. With this belief in mind, Plaintiff Kuffrey provided her PII/PHI to the Community

Defendants as a condition of her employment, and in connection with and in exchange for receiving healthcare or related services from the Community Defendants.

9. In connection with her employment and services provided to Plaintiff Kuffrey, the Community Defendants stored and maintained Plaintiff Kuffrey's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

10. Plaintiff Kuffrey takes great care to protect her PII/PHI. Had Plaintiff Kuffrey known that the Community Defendants do not adequately protect her PII/PHI in their possession, she would not have obtained or used services from the Community Defendants or agreed to provide the Community Defendants with her PII/PHI.

11. In a letter addressed to Plaintiff Kuffrey, Defendant CHSPSC, LLC disclosed to Plaintiff Kuffrey that her PII and/or PHI was accessible as a result of the Data Breach.

12. As a direct result of the Data Breach, Plaintiff Kuffrey has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Community Plaintiff Angela Martin

13. Plaintiff Angela Martin is a citizen of Alabama.

14. Plaintiff Martin obtained healthcare or related services from hospitals or clinics serviced by or affiliated with the Community Defendants. As a condition of receiving these services, the Community Defendants required her to provide them with her PII/PHI.

15. Based on representations made by the Community Defendants, Plaintiff Martin believed that the Community Defendants had implemented and maintained reasonable security

practices to protect her PII/PHI. With this belief in mind, Plaintiff Martin provided her PII/PHI to the Community Defendants in connection with and in exchange for receiving healthcare or related services from the Community Defendants.

16. In connection with services provided to Plaintiff Martin, the Community Defendants stored and maintained Plaintiff Martin's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

17. Plaintiff Martin takes great care to protect her PII/PHI. Had Plaintiff Martin known that the Community Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained or used services from the Community Defendants or agreed to provide them with her PII/PHI.

18. In a letter addressed to Plaintiff Martin, defendant CHSPSC, LLC disclosed to Plaintiff Martin that her PII and/or PHI was accessible as a result of the Data Breach.

19. Plaintiff Martin has experienced fraud since cybercriminals obtained her PII/PHI in the Data Breach. An unauthorized person or persons attempted to open a Zelle account in her name. Plaintiff Martin has also received alerts that people are applying for other bank accounts. Also, in late January or early February of 2023, Plaintiff Martin had two attempted unauthorized transactions made on her bank account. She has also been advised by Experian that her personal information is now on the dark web. Plaintiff Martin estimates that she has spent approximately 40 hours dealing with these issues.

20. As a direct result of the Data Breach, Plaintiff Martin has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI;

deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Community Plaintiff Lola Tatum

21. Plaintiff Lola Tatum is a citizen of Mississippi.

22. Plaintiff Tatum obtained healthcare or related services from hospitals or clinics serviced by or affiliated with the Community Defendants.

23. Plaintiff Tatum was previously employed by an affiliate of the Community Defendants.

24. As a condition of receiving healthcare or related services, and in connection with her employment, the Community Defendants required Plaintiff Tatum to provide them with her PII/PHI.

25. Based on representations made by the Community Defendants, Plaintiff Tatum believed that they had implemented and maintained reasonable security practices to protect her PII/PHI. With this belief in mind, Plaintiff Tatum provided her PII/PHI to the Community Defendants in connection with her employment and in exchange for receiving healthcare or related services from the Community Defendants.

26. In connection with employment and services provided to Plaintiff Tatum, the Community Defendants stored and maintained Plaintiff Tatum's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

27. Plaintiff Tatum takes great care to protect her PII/PHI, including her Medicare information. Had Plaintiff Tatum known that the Community Defendants do not adequately protect her PII/PHI in their possession, she would not have obtained or used services or employment from the Community Defendants or their affiliates or agreed to provide them with her PII/PHI.

28. In a letter addressed to Plaintiff Tatum, Defendant CHSPSC, LLC disclosed to Plaintiff Tatum that her PII and/or PHI was accessible as a result of the Data Breach.

29. As a direct result of the Data Breach, Plaintiff Tatum has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Community Plaintiff Glenda G. Corn

30. Plaintiff Glenda G. Corn is a citizen of Florida.

31. Plaintiff Corn obtained healthcare or related services from hospitals or clinics serviced by or affiliated with the Community Defendants. As a condition of receiving these services, the Community Defendants required Plaintiff Corn to provide them with her PII/PHI.

32. Based on representations made by the Community Defendants, Plaintiff Corn believed that they had implemented and maintained reasonable security practices to protect her PII/PHI. With this belief in mind, Plaintiff Corn provided her PII/PHI to the Community Defendants in connection with and in exchange for receiving healthcare or related services from the Community Defendants.

33. In connection with services provided to Plaintiff Corn, the Community Defendants stored and maintained Plaintiff Corn's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

34. Plaintiff Corn takes great care to protect her PII/PHI. Had Plaintiff Corn known that the Community Defendants do not adequately protect her PII/PHI in their possession, she would

not have obtained or used services from the Community Defendants or their affiliates or agreed to provide them with her PII/PHI.

35. In a letter addressed to Plaintiff Corn, Defendant CHSPSC, LLC disclosed to Plaintiff Corn that her PII and/or PHI was accessible as a result of the Data Breach.

36. As a direct result of the Data Breach, Plaintiff Corn has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Community Plaintiff Wilhelmina Gill

37. Plaintiff Wilhelmina Gill is a citizen of Tennessee.

38. Plaintiff Gill obtained healthcare or related services from hospitals or clinics serviced by or affiliated with the Community Defendants. As a condition of receiving these services, the Community Defendants required Plaintiff Gill to provide Defendants with her PII/PHI.

39. Based on representations made by the Community Defendants, Plaintiff Gill believed that they had implemented and maintained reasonable security practices to protect her PII/PHI. With this belief in mind, Plaintiff Gill provided her PII/PHI to the Community Defendants in connection with and in exchange for receiving healthcare or related services from the Community Defendants.

40. In connection with services provided to Plaintiff Gill, the Community Defendants stored and maintained Plaintiff Gill PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

41. Plaintiff Gill takes great care to protect her PII/PHI. Had Plaintiff Gill known that the Community Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained or used services from the Community Defendants or their affiliates or agreed to provide the Community Defendants with her PII/PHI.

42. In a letter addressed to Plaintiff Gill, Defendant CHSPSC, LLC disclosed to Plaintiff Gill that her PII and/or PHI was accessible as a result of the Data Breach

43. As a direct result of the Data Breach, Plaintiff Gill has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Community Plaintiff Kelly Kern

44. Plaintiff Kelly Kern is a citizen of Pennsylvania.

45. Plaintiff Kern obtained healthcare or related services from hospitals or clinics serviced by or affiliated with the Community Defendants. As a condition of receiving these services, the Community Defendants required Plaintiff Kern to provide them with her PII/PHI.

46. Based on representations made by the Community Defendants, Plaintiff Kern believed that the Community Defendants had implemented and maintained reasonable security practices to protect her PII/PHI. With this belief in mind, Plaintiff Kern provided her PII/PHI to the Community Defendants in connection with and in exchange for receiving healthcare or related services from the Community Defendants.

47. In connection with services provided to Plaintiff Kern, the Community Defendants stored and maintained Plaintiff Kern's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

48. Plaintiff Kern takes great care to protect her PII/PHI. Had Plaintiff Kern known that the Community Defendants do not adequately protect her PII/PHI in their possession, she would not have obtained or used services from the Community Defendants or agreed to provide them with her PII/PHI.

49. In a letter addressed to Plaintiff Kern, Defendant CHSPSC, LLC disclosed to Plaintiff Kern that her PII and/or PHI was accessible as a result of the Data Breach.

50. Plaintiff Kern has experienced suspicious activity subsequent to the Data Breach. On April 13, 2023, she received a text message from Fidelity Bank asking to confirm an $85 purchase that was made in another state. This was the first time Plaintiff Kern had ever experienced an issue like this.

51. As a direct result of the Data Breach, Plaintiff Kern has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Community Plaintiff Brandy McGowen

52. Plaintiff Brandy McGowen is a citizen of Mississippi.

53. Plaintiff McGowen obtained healthcare or related services from hospitals or clinics serviced by or affiliated with the Community Defendants. As a condition of receiving these services, the Community Defendants required Plaintiff McGowen to provide Defendants with her PII/PHI.

54. Based on representations made by the Community Defendants, Plaintiff McGowen believed that they had implemented and maintained reasonable security practices to protect her PII/PHI. With this belief in mind, Plaintiff McGowen provided her PII/PHI to the Community

Defendants in connection with and in exchange for receiving healthcare or related services from the Community Defendants.

55. In connection with services provided to Plaintiff McGowen, the Community Defendants stored and maintained Plaintiff McGowen's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

56. Plaintiff McGowen takes great care to protect her PII/PHI. Had Plaintiff McGowen known that the Community Defendants do not adequately protect her PII/PHI in its possession, she would not have obtained or used services from the Community Defendants or agreed to provide them with her PII/PHI.

57. In a letter addressed to Plaintiff McGowen, Defendant CHSPSC, LLC disclosed to Plaintiff McGowen that her PII and/or PHI was accessible as a result of the Data Breach.

58. As a direct result of the Data Breach, Plaintiff McGowen has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Community Plaintiff Timothy Ferguson

59. Plaintiff Timothy Ferguson is a citizen of Tennessee.

60. Plaintiff Ferguson obtained healthcare or related services from hospitals or clinics serviced by or affiliated with the Community Defendants. As a condition of receiving these services, the Community Defendants required Plaintiff Ferguson to provide them with his PII/PHI.

61. Based on representations made by the Community Defendants, Plaintiff Ferguson believed that they had implemented and maintained reasonable security practices to protect his

PII/PHI. With this belief in mind, Plaintiff Ferguson provided his PII/PHI to the Community Defendants in connection with and in exchange for receiving healthcare or related services from the Community Defendants.

62. In connection with services provided to Plaintiff Ferguson, the Community Defendants stored and maintained Plaintiff Ferguson's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

63. Plaintiff Ferguson takes great care to protect his PII/PHI. Had Plaintiff Ferguson known that the Community Defendants do not adequately protect his PII/PHI in their possession, he would not have obtained or used services from the Community Defendants or agreed to provide them with his PII/PHI.

64. In a letter addressed to Plaintiff Ferguson, Defendant CHSPSC, LLC disclosed to Plaintiff Ferguson that his PII and/or PHI was accessible as a result of the Data Breach.

65. As a direct result of the Data Breach, Plaintiff Ferguson has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

Brightline Plaintiff Terrance Rosa

66. Plaintiff Terrance Rosa is a citizen of Pennsylvania.

67. Plaintiff Rosa first learned of the Data Breach when he received a notice email (substantially similar to the Notice) from his employer.

68. Upon information and belief, Brightline obtained Plaintiff Rosa's PII and PHI from his employer, which used Brightline to deliver health services.

69. Soon after and as a result of the Data Breach, Plaintiff Rosa experienced a significant increase in spam and suspicious phone calls, texts, and emails. He was also alerted through his credit monitoring service that his Private Information is now on the dark web.

70. As a result of the Data Breach and at the recommendation of Brightline and its Notice, Plaintiff Rosa made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information.

71. Plaintiff Rosa has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

72. Plaintiff Rosa suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI and/or financial information.

73. Plaintiff Rosa is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII and PHI, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

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

Brightline Plaintiff Ryan Watson

75. Plaintiff Ryan Watson is a citizen of Virginia.

76. Plaintiff Watson first found out about the Breach when he reviewed a notice email (substantially similar to the Notice) that he received from his employer.

77. Upon information and belief, Brightline obtained Plaintiff Watson's PII and PHI from his employer, which used the company to deliver health services.

78. Shortly after and as a result of the Data Breach, Plaintiff Watson received a fraudulent call where the caller attempted to elicit banking information from him. This caller pretended to be an Amazon representative who needed to verify his banking information for a pending delivery. In actuality, there was no pending delivery as Plaintiff Watson had made no such purchase. This was just one of the many spam and suspicious phone calls, texts, and emails Plaintiff Watson received as a result of the Data Breach.

79. Plaintiff Watson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information.

80. Plaintiff Watson has spent significant time responding to the Data Breach and will continue to spend valuable time dealing with the effects of the Data Breach, time that he otherwise would have spent on other activities.

81. Plaintiff Watson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI for fraudulent purposes.

82. Plaintiff Watson is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII and PHI, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

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

Brightline Plaintiff Donisha Jackson

84. Plaintiff Donisha Jackson is a citizen of Illinois.

85. Plaintiff Jackson received the data breach notice letter from Brightline on or about May 5, 2023.

86. Plaintiff Jackson has been damaged by the compromise of her Private Information in the Data Breach.

87. Plaintiff Jackson entrusted her Private Information to Defendant in order to receive Defendant's services.

88. Plaintiff Jackson's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices, procedures, and protocols, as discussed herein.

89. As a direct and proximate result of Defendant's actions and omissions, Plaintiff Jackson has been harmed and is at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in her name, loans opened in her name, tax returns filed in her name, utility bills opened in her name, credit card accounts opened in her name, and other forms of identity theft.

90. Further, as a direct and proximate result of the Data Breach, Plaintiff Jackson has been forced to spend time dealing with and attempting to mitigate the negative effects thereof.

91. Plaintiff Jackson also faces a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of her Private Information, since

potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff Jackson as they already have other Class Members.

92. The Private Information maintained by and stolen from Defendant's system, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff Jackson, which can also be used to carry out targeted medical fraud and/or identity theft against her.

93. Additionally, Plaintiff Jackson has spent and will continue to spend significant amounts of time monitoring her accounts and records, including medical records and explanations of benefits, for misuse.

94. Plaintiff Jackson has suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of her time reasonably incurred to remedy or mitigate the effects of the Data Breach.

95. Moreover, Plaintiff Jackson has an interest in ensuring that her Private Information, which is believed to still be in the possession of Defendant, is protected from future breaches by the implementation of appropriate data security measures and safeguards.

96. As a direct and proximate result of Defendant's actions and inactions, Plaintiff Jackson has suffered a loss of privacy and cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

Brightline Plaintiff Kyle Castro

97. Plaintiff Kyle Castro is a citizen of Tennessee.

98. Plaintiff Castro received the data breach notice letter from Brightline on or about May 5, 2023.

99. Plaintiff Castro has been damaged by the compromise of his Private Information in the Data Breach.

100. Plaintiff Castro entrusted his Private Information, along with that of his minor children, to Defendant in order to receive Defendant's services.

101. Plaintiff Castro's and his children's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices, procedures, and protocols, as discussed herein.

102. As a direct and proximate result of Defendant's actions and omissions, Plaintiff Castro and his children have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

103. Further, as a direct and proximate result of the Data Breach, Plaintiff Castro has been forced to spend time dealing with and attempting to mitigate the negative effects thereof. For example, in an effort to mitigate the heightened risk of identity theft and fraud that he and his children now face, Plaintiff Castro has subscribed to a paid online credit monitoring service through IDshield. While this credit monitoring service allows Plaintiff Castro to monitor his and his children's credit reports to determine whether suspicious activity has occurred, it is powerless to stop identity theft in advance and does not indemnify them from, or insure them against, the harm caused by the Data Breach.

104. Plaintiff Castro also expended considerable time and effort attempting to contact Brightline after learning of the Data Breach, while also monitoring his and his children's identity and credit reports periodically.

105. Plaintiff Castro has also been targeted in recent spam and phishing attempts and is at a risk of experiencing similar future risks that also include data intrusion and other illegal schemes through the misuse of his Private Information, since potential fraudsters have used and will likely continue to use such Private Information to carry out such targeted schemes against Plaintiff Castro.

106. The Private Information maintained by and stolen from Defendant's system, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff Castro, which can also be used to carry out targeted medical fraud and/or identity theft against him.

107. Additionally, Plaintiff Castro has spent and will continue to spend significant amounts of time monitoring his accounts and records, including medical records and explanations of benefits, for misuse.

108. Plaintiff Castro has suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of his time reasonably incurred to remedy or mitigate the effects of the Data Breach.

109. Moreover, Plaintiff Castro has an interest in ensuring that his Private Information and that of his children, which is believed to still be in the possession of Defendant, is protected from future breaches by the implementation of appropriate data security measures and safeguards.

110. As a direct and proximate result of Defendant's actions and inactions, Plaintiff Castro has suffered a loss of privacy and cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

Brightline Plaintiff Itaunya Milner

111. Plaintiff Itaunya Milner is a citizen of New Jersey.

112. Plaintiff Milner received the data breach notice letter from Brightline on or about May 5, 2023.

113. Plaintiff Milner has been damaged by the compromise of her Private Information in the Data Breach.

114. Plaintiff Milner entrusted her Private Information, along with that of her minor child, to Defendant in order to receive Defendant's services.

115. Plaintiff Milner's and her minor child's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which resulted from Defendant's inadequate data security practices, procedures, and protocols, as discussed herein.

116. As a direct and proximate result of Defendant's actions and omissions, Plaintiff Milner and her child have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

117. Further, as a direct and proximate result of the Data Breach, Plaintiff Milner has been forced to spend time dealing with and attempting to mitigate the negative effects thereof.

118. Plaintiff Milner also faces a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of her Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff Milner as they already have other Class Members.

119. The Private Information maintained by and stolen from Defendant's system, combined with publicly available information, allows nefarious actors to assemble a detailed

mosaic of Plaintiff Milner, which can also be used to carry out targeted medical fraud and/or identity theft against her.

120. Additionally, Plaintiff Milner has spent and will continue to spend significant amounts of time monitoring her accounts and records, including medical records and explanations of benefits, for misuse.

121. Plaintiff Milner has suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of her time reasonably incurred to remedy or mitigate the effects of the Data Breach.

122. Moreover, Plaintiff Milner has an interest in ensuring that her Private Information and that of her child, which is believed to still be in the possession of Defendant, is protected from future breaches by the implementation of appropriate data security measures and safeguards.

123. As a direct and proximate result of Defendant's actions and inactions, Plaintiff Milner has suffered a loss of privacy and cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

Brightline Plaintiff Anthony Ndifor

124. Plaintiff Anthony Ndifor is a citizen of California.

125. Plaintiff Ndifor first learned about the Data Breach from a notice email (substantially similar to the Notice) sent by his employer.

126. Upon information and belief, Brightline obtained Plaintiff Ndifor's PII and PHI from his employer, which used the website to deliver health services.

127. Like the other Plaintiffs, following the Data Breach, Plaintiff Ndifor experienced an increase in spam and suspicious phone calls, texts, and emails. Like Plaintiff Rosa, Plaintiff Ndifor's credit monitoring service alerted him that his Private Information is now on the dark web.

128. As a result of the Data Breach, Plaintiff Ndifor made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information.

129. Plaintiff Ndifor has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

130. Plaintiff Ndifor suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI and/or financial information.

131. Plaintiff Ndifor is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from their PII and PHI, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

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

Imagine360 Plaintiff Anthony Collins

133. Plaintiff Anthony Collins is a citizen of Illinois.

134. Plaintiff Collins obtained health insurance or related services from Imagine360 through his employer. As a condition of receiving these services, Imagine360 required Plaintiff Collins' employer to provide it with his PII/PHI.

135. Based on representations made by Imagine360, Plaintiff Collins believed that it had implemented and maintained reasonable security practices to protect his PII/PHI. With this belief in mind, Plaintiff Collins allowed his PII/PHI to be provided to Imagine360 in connection with and in exchange for receiving health insurance or related services from Imagine360.

136. In connection with services provided to Plaintiff Collins, Imagine360 stored and maintained Plaintiff Collins' PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

137. Plaintiff Collins takes great care to protect his PII/PHI. Had Plaintiff Collins known that Imagine360 does not adequately protect his PII/PHI in its possession, he would not have obtained or used services from Imagine360 or agreed to provide them with his PII/PHI.

138. In a letter addressed to Plaintiff Collins, Imagine360 disclosed to Plaintiff Collins that his PII and/or PHI was accessed as a result of the Data Breach.

139. As a direct result of the Data Breach, Plaintiff Collins has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

Imagine360 Plaintiff Dawn McGee

140. Plaintiff Dawn McGee is a citizen of Pennsylvania.

141. Plaintiff McGee obtained health insurance or related services from Imagine360 through her employer. As a condition of receiving these services, Imagine360 required Plaintiff McGee's employer to provide it with her PII/PHI.

142. Based on representations made by Imagine360, Plaintiff McGee believed that it had implemented and maintained reasonable security practices to protect her PII/PHI. With this belief in mind, Plaintiff McGee allowed her PII/PHI to be provided to Imagine360 in connection with and in exchange for receiving health insurance or related services from Imagine360.

143. In connection with services provided to Plaintiff McGee, Imagine360 stored and maintained Plaintiff McGee's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

144. Plaintiff McGee takes great care to protect her PII/PHI. Had Plaintiff McGee known that Imagine360 does not adequately protect her PII/PHI in its possession, she would not have obtained or used services from Imagine360 or agreed to provide them with her PII/PHI.

145. In a letter addressed to Plaintiff McGee, Imagine360 disclosed to Plaintiff McGee that her PII and/or PHI was accessed as a result of the Data Breach.

146. As a direct result of the Data Breach, Plaintiff McGee has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

ITx Plaintiff Lauren Perrone

147. Plaintiff Lauren Perrone is a citizen of New Jersey.

148. Plaintiff Perrone obtained healthcare or related services from ITx's client, AtlantiCare Regional Medical Center. As a condition of receiving these services, Plaintiff Perrone was required to provide ITx with her PII/PHI in connection with and in exchange for the receipt of healthcare services from AtlantiCare Regional Medical Center.

149. In connection with the medical services provided to Plaintiff Perrone, ITx stored and maintained Plaintiff Perrone's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

150. Plaintiff Perrone takes great care to protect her PII/PHI. Had Plaintiff Perrone known that ITx did not adequately protect the PII/PHI in its possession, she would not have permitted ITx to maintain her PII/PHI.

151. In a letter addressed to Plaintiff Perrone, ITx disclosed to Plaintiff Perrone that her PII and/or PHI was accessible as a result of the Data Breach.

152. As a direct result of the Data Breach, Plaintiff Perrone has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

ITx Plaintiff Victoria Evans

153. Plaintiff Victoria Evans is a citizen of Missouri.

154. Plaintiff Evans obtained healthcare or related services from hospitals or clinics serviced by or affiliated with ITx. As a condition of receiving these services, Plaintiff Evans was required to provide ITx with her PII/PHI in connection with and in exchange for the receipt of healthcare or related services.

155. In connection with the medical services provided to Plaintiff Evans, ITx stored and maintained Plaintiff Evan's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

156. Plaintiff Evans takes great care to protect her PII/PHI. Had Plaintiff Evans known that ITx did not adequately protect the PII/PHI in its possession, she would not have permitted ITx to maintain her PII/PHI.

157. In a letter addressed to Plaintiff Evans, ITx disclosed to Plaintiff Evans that her PII and/or PHI was accessible as a result of the Data Breach.

158. As a direct result of the Data Breach, Plaintiff Evans has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

159. Further, as a result of the Data Breach, Plaintiff Evans has suffered actual misuse of her PII/PHI. Specifically, after the Data Breach occurred in January of 2023, Plaintiff Evans received a notification that her PII was found on the dark web, including her email address.

ITx Plaintiff Thomas Kelly

160. Plaintiff Thomas Kelly is a citizen of Ohio.

161. Plaintiff Kelly obtained medical services at Fulton County Medical Center, which contracted with ITx in approximately 2020. As a condition of receiving these services, Plaintiff Kelly was required to provide ITx with his PII/PHI in connection with and in exchange for the receipt of healthcare services from Fulton County Medical Center.

162. In connection with the medical services provided to Plaintiff Kelly, ITx stored and maintained Plaintiff Kelly's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

163. Plaintiff Kelly takes great care to protect his PII/PHI. Had Plaintiff Kelly known that ITx did not adequately protect the PII/PHI in its possession, he would not have permitted ITx to maintain his PII/PHI.

164. In a letter addressed to Plaintiff Kelly, ITx disclosed to Plaintiff Kelly that his PII and/or PHI was accessible because of the Data Breach.

165. As a direct result of the Data Breach, Plaintiff Kelly has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

166. Further, because of the Data Breach, Plaintiff Kelly has experienced actual misuse of his PII/PHI, including, but not limited to: (i) fraudulent charges to his Fifth Third Bank account in or about March 2023; (ii) his PII being disseminated on the dark web according to Experian; and (iii) a significant increase in spam calls, texts, and/or emails.

ITx Plaintiff Jose Cabrales

167. Plaintiff Jose Cabrales is a citizen of Arizona.

168. Plaintiff Cabrales obtained healthcare or related services from hospitals or clinics serviced by or affiliated with ITx. As a condition of receiving these services, Plaintiff Cabrales was required to provide ITx with his PII/PHI in connection with and in exchange for the receipt of healthcare or related services.

169. In connection with the medical services provided to Plaintiff Cabrales, ITx stored and maintained Plaintiff Cabrales's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

170. Plaintiff Cabrales takes great care to protect his PII/PHI. Had Plaintiff Cabrales known that ITx did not adequately protect the PII/PHI in its possession, he would not have permitted ITx to maintain his PII/PHI.

171. In a letter addressed to Plaintiff Cabrales, ITx disclosed to Plaintiff Cabrales that his PII and/or PHI was accessible because of the Data Breach.

172. As a direct result of the Data Breach, Plaintiff Cabrales has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

ITx Plaintiff Nicholas Timmons

173. Plaintiff Nicholas Timmons is a citizen of Missouri.

174. Plaintiff Timmons obtained healthcare or related services from SoutheastHealth—a client of ITx. As a condition of receiving these services, Plaintiff Timmons was required to provide ITx with his PII/PHI in connection with and in exchange for the receipt of healthcare or related services from SoutheastHealth.

175. In connection with the medical services provided to Plaintiff Timmons by its affiliate, SoutheastHealth, ITx stored and maintained Plaintiff Timmons's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

176. Plaintiff Timmons takes great care to protect his PII/PHI. Had Plaintiff Timmons known that ITx did not adequately protect the PII/PHI in its possession, he would not have permitted ITx to maintain his PII/PHI.

177. In a letter addressed to Plaintiff Timmons, ITx disclosed to Plaintiff Timmons that his PII and/or PHI was accessible as a result of the Data Breach.

178. As a direct result of the Data Breach, Plaintiff Timmons has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security. Plaintiff Timmons also receives consistent scammer telephone calls and suffered actual injury in the form of lost time spent dealing with a wave of fraudulent loan and credit pre-approval mail received in his name since the Data Breach.

179. Further, because of the Data Breach, Plaintiff Timmons also suffered actual misuse of his PII/PHI in the form of fraudulent transactions to his Regions Bank debit card account. Specifically, after the Data Breach occurred, Plaintiff Timmons suffered fraudulent transactions to his Regions Bank debit card. As a result, Plaintiff Timmons has been forced to obtain a new debit card at least three different times since the Data Breach.

ITx Plaintiff Kristi McDavitt

180. Plaintiff Kristi McDavitt is a citizen of Ohio.

181. Plaintiff McDavitt obtained healthcare or related services from her healthcare provider—a client of ITx. As a condition of receiving these services, Plaintiff McDavitt was required to provide ITx with her PII/PHI in connection with medical services she received from her healthcare provider.

182. In connection with the medical services provided to Plaintiff McDavitt, ITx stored and maintained Plaintiff McDavitt's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

183. Plaintiff McDavitt takes great care to protect her PII/PHI. Had Plaintiff McDavitt known that ITx did not adequately protect the PII/PHI in its possession, she would not have permitted ITx to maintain her PII/PHI.

184. In a letter addressed to Plaintiff McDavitt, ITx disclosed to Plaintiff McDavitt that her PII and/or PHI was accessible because of the Data Breach.

185. As a direct result of the Data Breach, Plaintiff McDavitt has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

ITx Plaintiff Robert Terwilliger

186. Plaintiff Robert Terwilliger is a citizen of Missouri.

187. Plaintiff Terwilliger obtained healthcare or related services from CoxHealth—a client of ITx. As a condition of receiving these services from, Plaintiff Terwilliger was required to provide ITx with his PII/PHI in connection with and in exchange for the receipt of healthcare or related services from CoxHealth.

188. In connection with the medical services provided to Plaintiff Terwilliger, ITx stored and maintained Plaintiff Terwilliger's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

189. Plaintiff Terwilliger takes great care to protect his PII/PHI. Had Plaintiff Terwilliger known that ITx did not adequately protect the PII/PHI in its possession, he would not have permitted ITx to maintain his PII/PHI.

190. In a letter addressed to Plaintiff Terwilliger, ITx disclosed to Plaintiff Terwilliger that his PII and/or PHI was accessible because of the Data Breach.

191. As a direct result of the Data Breach, Plaintiff Terwilliger has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

192. Further, Plaintiff Terwilliger has experienced actual misuse of his PII/PHI in the form of multiple hard inquiries made in his name since the Data Breach. Specifically, since the Data Breach occurred in January of 2023, Plaintiff Terwilliger has received a total of seventeen (17) hard inquiries into his credit that he did not initiate, which has caused his credit score to drop a total of 209 points. This sudden decrease in Plaintiff Terwilliger's credit could not have come at a worse time. On January 22, 2024, Plaintiff Terwilliger was informed by his bank that, because of the sudden decrease in his credit score, Plaintiff Terwilliger did not qualify for financing to purchase a home for him and his family.

193. Finally, because of the Data Breach Plaintiff Terwilliger purchased credit monitoring services through Credit Karma, Equifax, and Experian, which costs Plaintiff Terwilliger approximately $1,442.00 per year.

ITx Plaintiff Edwin Rodriguez

194. Plaintiff Edwin Rodriquez is a citizen of Massachusetts.

195. Plaintiff Rodriquez obtained healthcare or related services from ITx's client, Life Laboratories. As a condition to receiving these services, ITx required Plaintiff Rodriquez to

provide ITx with his PII/PHI in connection with and in exchange for the receipt of medical services from Life Laboratories.

196. In connection with the medical services provided to Plaintiff Rodriquez, ITx stored and maintained Plaintiff Rodriquez's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

197. Plaintiff Rodriquez takes great care to protect his PII/PHI. Had Plaintiff Rodriquez known that ITx did not adequately protect the PII/PHI in its possession, he would not have permitted ITx to maintain his PII/PHI.

198. In a letter addressed to Plaintiff Rodriquez, ITx disclosed to Plaintiff Rodriquez that his PII and/or PHI was accessible because of the Data Breach.

199. As a direct result of the Data Breach, Plaintiff Rodriquez has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

200. Further, as a result of the Data Breach, Plaintiff Rodriquez has experienced actual misuse of his PII/PHI due to hard inquiries appearing on his credit report. Specifically, on July 21, 2023, months after the Data Breach occurred, a hard inquiry was made into Plaintiff Rodriquez's credit from "Cred-Co Cardinal Financing". Plaintiff Rodriquez has no affiliation with "Cred-Co Cardinal Financing", and this hard inquiry was not initiated by Plaintiff Rodriquez.

201. Finally, since the Data Breach, Plaintiff Rodriquez consistently receives notifications via email that "someone has attempted to log-in" to his Google email account. Plaintiff Rodriquez does not know who is trying to log in to his email account.

The Community Defendants

202. Defendant CHSPSC, LLC is a Delaware corporation with its principal place of business in Franklin, Tennessee. CHSPSC's headquarters are located at 4000 Meridian Blvd., Franklin, Tennessee 37067.

203. Defendant Community Health Systems, Inc. is a Delaware corporation, with its principal place of business in Franklin, Tennessee. CHS is one of the largest publicly traded hospital companies in the United States.[2] Defendant CHSPSC is a related entity that provides "management services" for entities affiliated with CHS.[3] Specifically, CHSPSC identifies and enters into contracts with vendors to provide services for CHS and its affiliates. CHS's website states that "we . . . hold CHSPSC and CHS affiliated entities' vendors and their representatives to specific standards of conduct when committing financial resources for the purchase of goods, services, and equipment."[4]

Defendant Brightline, Inc.

204. Defendant Brightline, Inc. is a Delaware corporation, with its principal place of business in San Mateo, California.

Defendant Imagine360, LLC

205. Defendant Imagine360, LLC is headquartered and maintains its principal place of business at 1550 Liberty Ridge Dr. #330, Wayne, Pennsylvania in Delaware County.

---

[2] *Company Overview*, CMTY. HEALTH SYS., https://www.chs.net/company-overview/ (last visited Apr. 3, 2024).

[3] *Vendor Information*, CMTY. HEALTH SYS., https://www.chs.net/company-overview/vendor-information/ (last visited Apr. 3, 2024).

[4] *Id.*

206. Upon information and belief, Imagine360 has two limited liability members– Stephen Kelly and Charles Walters, III.

207. Imagine360 member, Stephen Kelly, is an adult who, at all relevant times, is a resident and citizen of the Commonwealth of Pennsylvania.

208. Imagine360 member, Charles Walters, III, is an adult who, at all relevant times, is a resident and citizen of the State of Georgia.

209. Imagine360 is a citizen of each of the states in which one of its members is a citizen. Imagine360, thus, is a citizen of the Commonwealth of Pennsylvania and the State of Georgia.

Defendant Intellihartx, LLC

210. Defendant Intellihartx, LLC is headquartered and maintains its principal place of business at 129 E. Crawford St., Suite 360, Findlay, Ohio 45840 in Hancock County. Further, Intellihartx, LLL's sole limited liability member, Phillip R. Grower, at all relevant times, is and has been an adult and is a resident and citizen of the state of Ohio.

JURISDICTION AND VENUE

211. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

212. This Court has jurisdiction over every Defendant in this multi-district litigation because every Defendant was transferred to this forum from a transferor court which had personal jurisdiction over that MDL Defendant.

213. Under 28 U.S.C. § 1407, venue is proper pursuant to the valid transfer and Fed. R. Civ. P. 42 pre-trial consolidation of these cases in this District by the Judicial Panel on Multidistrict Litigation.

FACTUAL ALLEGATIONS

Overview of the Community Defendants

214. "CHSPSC is a professional services company that provides services to hospitals and clinics affiliated with Community Health Systems, Inc."[5] Upon information and belief, CHSPSC is a subsidiary of CHS.

215. CHS is a publicly traded company whose stock (CYH) has been listed on the New York Stock Exchange since 2000. In its Form 10-K filed with the Securities and Exchange Commission for the year ended 2022, CHS reported $12.2 billion in revenue, with $1.4 billion in earnings before interest, taxes, depreciation, and amortization.

216. CHS describes itself as "one of the nation's leading healthcare providers."[6] It operates in 15 states: Alabama, Alaska, Arizona, Arkansas, Florida, Georgia, Indiana, Mississippi, Missouri, New Mexico, North Carolina, Oklahoma, Pennsylvania, Tennessee and Texas.[7] It maintains 78 acute-care hospitals and more than 1,000 other sites of care, including physician

[5] *Notice of Third-Party Security Incident Impacting CHSPSC Affiliate Data* ("Website Notice"), CMTY. HEALTH SYS., https://web.archive.org/web/20230717075117/https://www.chs.net/notice-of-third-party-security-incident-impacting-chspsc-affiliate-data/ (last visited Apr. 15, 2024).

[6] https://www.chs.net/ (last visited Apr. 15, 2024).

[7] *Locations*, CMTY. HEALTH SYS., https://www.chs.net/serving-communities/locations/#USMap (last visited Apr. 3, 2024). Steve Alder, Community Health Systems Pays $5 Million to Settle Multi-State Breach Investigation, HIPAA J. (Oct. 9, 2020), https://www.hipaajournal.com/community-health-systems-pays-5-million-to-settle-multi-state-breach-investigation/ (last visited Apr. 3, 2024).

practices, urgent care centers, freestanding emergency departments, occupational medicine clinics, imaging centers, cancer centers, and ambulatory surgery centers.[8]

217. Due to the nature of the services that they provide, CHSPSC and CHS acquire and electronically store patient PII and PHI: "When a patient enters a CHS affiliated facility, a large amount of personal, medical, and insurance data is collected."[9] The Community Defendants' Code of Conduct states "[p]atient information may only be discussed or released as permitted or required under the Health Insurance Portability and Accountability Act ('HIPAA') or other privacy laws and in accordance with our HIPAA policies . . . which may require either a patient-directed request, a request from a patient's personal representative, or the express written authorization of the patient."[10]

218. The Community Defendants' Code of Conduct also states that they are "dedicated to compliance with all applicable federal, state, and local laws, rules, and regulations ('Applicable Law'), including privacy and security of patient health information."[11] And the Community Defendants acknowledge that "[p]atient information is highly confidential."[12] The Community Defendants also state that patient rights include "[p]ersonal privacy" and "privacy of health information."[13]

---

[8] *Id.*

[9] Community Health Systems, *Community Health Systems Code of Conduct* 9 (2023), https://www.chs.net/wp-content/uploads/Code-of-Conduct-January-2023-FINAL.pdf (last visited Apr. 15, 2023). The Code of Conduct applies to, and has been independently adopted by, each subsidiary of Community Health Systems, including CHSPSC. *See id.*

[10] *Id.* at 10.

[11] *Id.* at 3.

[12] *Id.* at 9.

[13] *Id.* at 11.

The 2014 Data Breach at Community

219. The Community Defendants were previously targets of a data breach that compromised the sensitive personal information of over six million people. The hackers gained access to the Community Defendants' internal computer systems between April and June 2014. The data that was exfiltrated included patient names, Social Security numbers, addresses, dates of birth, and phone numbers.

220. Shortly after this breach was announced, the Iowa Attorney General filed a complaint against the Community Defendants which alleged, *inter alia*, that they:

a. failed to implement and maintain reasonable security practices to protect consumers' personal information they collect and maintain;

b. failed to store personal information in a way that maximized its security and confidentiality; and

c. permitted the disclosure of Protected Health Information in a manner inconsistent with the requirements of HIPAA and its rules.[14]

221. Several other Attorneys General also prosecuted similar claims against the Community Defendants. These matters were resolved in 2020 for $5 million. Iowa Attorney General Tom Miller issued a statement at that time that said "CHS failed to implement and maintain reasonable security practices."[15]

[14] https://www.iowaattorneygeneral.gov/media/cms/CHS_Petition_011932DDEE45E.pdf (last visited Apr. 3, 2024).

[15] Heather Landi, *CHS to pay $5M to 28 states to settle 2014 data breach*, FIERCE HEALTHCARE (Oct. 9, 2020 1:04 PM), https://www.fiercehealthcare.com/tech/chs-to-pay-5m-to-28-states-to-settle-2014-data-breach.

222. CHSPSC agreed to pay another $2.3 million to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) in connection with the 2014 breach.[16] A statement issued by that agency announcing the settlement stated that its

> investigation found longstanding, systemic noncompliance with the HIPAA Security Rule including failure to conduct a risk analysis, and failures to implement information system activity review, security incident procedures, and access controls. "The health care industry is a known target for hackers and cyberthieves. The failure to implement the security protections required by the HIPAA Rules, especially after being notified by the FBI of a potential breach, is inexcusable," said OCR Director Roger Severino.[17]

223. The Community Defendants additionally agreed to settle a class action lawsuit filed in connection with the 2014 data breach for $3.1 million.[18]

224. The Data Breach was reasonably foreseeable to Defendants. In fact, CHS was the subject of a massive breach in 2014 that impacted 6.1 million patients. On September 22, 2020, both CHSPSC and CHS entered into a consent decree with the Iowa Attorney General and 27 other participating states whereby they agreed to pay $5 million to resolve allegations that they lacked sufficient security measures in relation to the 2014 breach.[19] CHSPSC and CHS also agreed to

---

[16] *HIPAA Business Associate Pays $2.3 Million to Settle Breach Affecting Protected Health Information of Over 6 million Individuals*, HHS (Sept. 23, 2020), https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2020/09/23/hipaa-business-associate-pays-2.3-million-settle-breach.html.

[17] *Id.*

[18] *Community Health Systems agrees to pay nearly $3.1 million as a part of settlement for 2014 data breach*, CYWARE (Feb. 6, 2019), https://cyware.com/news/community-health-systems-agrees-to-pay-nearly-31-million-as-a-part-of-settlement-for-2014-data-breach-73d4c448 (last visited Apr. 3, 2024).

[19] https://www.iowaattorneygeneral.gov/media/cms/CHS_Consent_Decree_4FD176209906F.PDF (last visited Apr. 3, 2024).

settle a similar investigation with the HHS' Office for Civil Rights for $2.3 million, as well as a class action lawsuit for $3.1 million.[20]

Overview of Brightline

225. Founded in 2019, Brightline provides mental and behavioral health services, including virtual counseling for children, teenagers and their families, and is based in San Mateo, California.

226. Upon information and belief, Brightline employs more than 140 people and generates approximately $20 million in annual revenue, but reportedly has received over $200 million in venture capital funding.

227. As a condition for receiving pediatric behavioral health and/or benefit eligibility, Brightline required the Brightline Plaintiffs to confide and make available to it, its agents, and its employees, sensitive and confidential PII and PHI.

228. In its Notice of HIPAA Privacy Practices (referred to herein as the "Privacy Policy"), Brightline makes it clear that "[t]he protection of [its patients'] health information is very important" to it, and that it will only release this protected information "with your permission, or under circumstances," none of which listed circumstances are applicable here.[21]

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

---

[20] Steve Alder, *Community Health Systems Pays $5 Million to Settle Multi-State Breach Investigation*, HIPAA J. (Oct. 9, 2020), https://www.hipaajournal.com/community-health-systems-pays-5-million-to-settle-multi-state-breach-investigation/ (last visited Apr. 3, 2024).

[21] *See* https://www.hellobrightline.com/privacy-practices (last visited on April 17, 2024).

230. The Brightline Plaintiffs and similarly situated individuals relied on Brightline to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Brightline ultimately failed to do.

Overview of Imagine360

231. Imagine360 provides self-funded health insurance plan services to employers within a number of different industries, including auto dealing, convenience stores, construction, manufacturing, nonprofits, marine services, restaurants, senior living, trucking and transportation, technology, and professional services. [22]

232. According to its own website, Imagine360 was founded on the "powerful idea" that "[h]ealth plans can do better[,]" and "[e]mployees should get the high-quality care they need at a fair price."[23]

233. As a condition of receiving these services, Imagine360 requires that its employer clients, including Imagine360 Plaintiffs' employers, turn over highly sensitive employee personal and health information.

234. By obtaining, collecting, using, and deriving a benefit from Imagine360 Plaintiffs' and Class Members' Private Information, Imagine360 assumed legal and equitable duties owed to them and knew or should have known that it was responsible for protecting Imagine360 Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

235. Imagine360 Plaintiffs and Class Members relied on Imagine360 to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Imagine306 ultimately failed to do.

---

[22] *See* https://www.imagine360.com/industries/ (last visited April 16, 2024).

[23] *See* https://www.imagine360.com/about/ (last visited July 6, 2023).

Overview of Intellihartx

236. ITx was founded in 2012 as a healthcare revenue cycle company focused exclusively on healthcare clients including hospitals and physicians' groups. Revenue cycle management is the process of using billing software to track patient care episodes through each stage of interaction between the healthcare service provider and the patient—from registration and appointment scheduling to the final payment of a balance.

237. According to its own website, "ITx is a leading company in healthcare revenue cycle focused exclusively on healthcare clients[.]"[24] ITx also expressly states that it "serve[s] patients, not debtors."[25]

238. ITx claims to increase revenue for its clients by providing debt-payment services, including self-pay concierge services and patient open balances services. ITx further explains who it works to serve on its website, stating, "We serve Patients, not Debtors."[26]

239. As a condition to receiving revenue cycle services, ITx requires that its healthcare clients' patients turn over highly sensitive personal and health information.

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

241. ITx Plaintiffs and Class Members relied on ITx to keep their PII/PHI confidential and securely maintained and to only make authorized disclosures of this information, which ITx

[24] *See* https://www.itxcompanies.com/what-we-do (last visited April 16, 2024).

[25] *Id*.

[26] *Id*.

ultimately failed to do. ITx owed a duty to ITx Plaintiffs and Class Members to secure their PII/PHI as such, and ultimately breached that duty.

Defendants Partnered with Fortra for File Transfer Services and Data Storage.

242. Each of the Defendants contracted with Fortra, a company that sells information technology management software and services, for the use of file transfer software called the "GoAnywhere MFT."[27] Defendants upload, store, transfer, or access their or their affiliates' patients' and employees' PII/PHI using GoAnywhere MFT.

243. GoAnywhere MFT "is a managed file transfer solution that automates and secures file transfers using a centralized enterprise-level approach" It acts as a "central point of administration" between an organization's internal organization, external partners and clients, appliances, and cloud environments. It allegedly includes "extensive security controls" and "automatic encryption" that may be customized for each organization. Fortra purposed that GoAnywhere MFT "will provide a safe, audited method for automatically transferring information in and outside of your enterprise."[28]

244. On information and belief, the default settings for GoAnywhere MTF are not compliant with reasonable security standards. The GoAnywhere MFT installation guide provides instructions for how to make the product more secure.

245. For example, the default configuration of GoAnywhere MFT allows anyone with access to the internet to view the landing page, or "administrative console" for a client's

[27] *See* Website Notice, *supra*, n.6.

[28] *Start Using GoAnywhere MFT*, FORTRA, https://www.goanywhere.com/offers/start-using-mft (last visited April 18, 2024).

GoAnywhere MFT, where users can sign in to, access, operate, and modify the program.[29] Fortra's instructions provide several simple steps that limit public access to this console, such as limiting access to specific ports, meaning that only certain users can access an organization's administrative console. Without these changes, GoAnywhere MFT is vulnerable to attack and exploitation, and is not compliant with reasonable security standards and HIPAA requirements.[30]

246. Fortra has also disclosed security vulnerabilities in GoAnywhere MFT in the past, which rendered the software vulnerable to exploitation, which Defendants knew or should have known.[31] Indeed, since 2014 the National Vulnerability Database has documented approximately 136 vulnerabilities impacting managed file transfer products or similar software. Of those documented vulnerabilities, 51 were classified as high risk, 72 as medium risk, and 13 as low risk.[32]

247. Upon information and belief, Defendants were able to control the security and configurations of the MFT servers that stored Class Members' PII and PHI for transfer, and were responsible for protecting, maintaining, and monitoring those servers for threat activity.

248. Upon information and belief, Defendants did not change the default settings on their installation of GoAnywhere MFT, including the administrative console exposed to anyone

---

[29] *GoAnywhere MFT Install Guide*, FORTRA, https://static.goanywhere.com/guides/ga_installation_guide.pdf (last visited April 18, 2024).

[30] Dave Shackleford, *Web-Based Admin Consoles: The Critical, Overlooked Security Exposure you must Address*, BEYONDTRUST (Aug. 10, 2021), https://www.beyondtrust.com/blog/entry/web-basedadmin-consoles-the-critical-overlooked-security-exposure-you-must-address.

[31] Fortra, *GoAnywhere MFT Security Advisory*, https://www.goanywhere.com/support/advisory/68x (last visited April 18, 2024).

[32] https://intel471.com/blog/managed-file-transfer-software-assessing-the-risks

with internet access, failing to comply with reasonable security standards and HIPAA requirements.

The 2023 Fortra Data Breach

249. Between January 28, 2023 and January 30, 2023, the Russia-linked ransomware group, Clop, "used a previously unknown vulnerability to gain access to Fortra's systems, specifically Fortra's GoAnywhere file transfer service platform, compromising sets of files throughout Fortra's platform"[33] that included the highly sensitive PII/PHI of Plaintiffs and Class Members.

Community Defendants' Notification of Fortra's 2023 Data Breach

250. Fortra first notified the Community Defendants of the Data Breach on February 2, 2023.[34] The Community Defendants then undertook their own investigation, which revealed that the personal information of patients, employees, and other individuals "may have been disclosed to the unauthorized party as a result of the Fortra incident."[35] Specifically, the compromised data may have included full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number.[36]

251. CHS has, for example, acknowledged in its SEC filings that the compromised information included "Protected Health Information" as defined by HIPAA.[37]

---

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] Community Health Systems, *Form 8-K* 2 (Feb. 13, 2023), https://chsnet.gcs-web.com/static-files/706bf25d-a064-4a04-90b6-bf4e5357defa (last visited Apr. 15, 2024).

252. The Data Breach impacted the PII/PHI of certain persons who received services from the Community Defendants or their affiliates, family members or guarantors of patients of the Community Defendants or their affiliates, and current or former employees of the Community Defendants or their affiliates.[38]

253. CHSPSC began notifying affected persons on or around March 20, 2023.[39] CHSPSC's Website Notice states that it has "implemented additional security measures, including immediate steps to implement measures to harden the security of CHSPSC's use of the GoAnywhere platform."[40]

254. The CHS and CHSPSC patient data compromised in the Data Breach was reportedly intentionally targeted by a criminal ransomware group linked to Russia and known as Clop.[41] It has not been reported whether Defendants were solicited to pay or actually paid a ransom demand.

255. In a May 16, 2023 press release discussing the various organizations that were targeted in the Data Breach, Michigan Attorney General Dana Nessel said "[c]ompanies that handle our personal data have a responsibility to implement safety measures that can withstand cyber-attacks. . . A breach like this one threatens to expose some of our most personal information

[38] *Id.*

[39] *See CHSPSC, LLC Data Breach Notification*, ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/e71fd844-b34a-449c-aba9-e4f63265f422.shtml (last visited Apr. 3, 2024).

[40] *Id.*

[41] Carly Page, *Ransomware gang uses new zero-day to steal data on 1 million patients*, TECHCRUNCH (Feb. 15, 2023), https://techcrunch.com/2023/02/15/clop-ransomware-community-health-systems/ (last visited Apr. 15, 2024).

– our health information."[42]

ITx's Notification of Fortra's 2023 Data Breach

256. According to ITx's Notice of Security Incident ("ITx Notice"), Defendant ITx waited until June 6, 2023, and June 9, 2023, to report to affected individuals that it was one of the entities impacted by the Data Breach, despite learning of the Data Breach on February 2, 2023.[43]

257. The individuals notified of the Data Breach by ITx were certain patients of its clients, including healthcare providers such as CoxHealth and Life Laboratories.[44]

258. Specifically, the unauthorized cybercriminals accessed a cache of highly sensitive PII/PHI, including names, addresses, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as dates of birth and Social Security numbers.[45]

259. According to the ITx Notice, it conducted multiple different investigations to fully understand the scope of the Data Breach and to whom the compromised information related.[46]

260. As a result of ITx's delayed notification, ITx Plaintiffs were completely unaware their PII/PHI was exposed as a result of the Data Breach.

Imagine360's Notification of Fortra's 2023 Data Breach

261. Despite identifying the Data Breach on January 30, 2023, Imagine360 waited

---

[42] *Fortra Data Breach Targets 130 Companies, Many in Healthcare Sector*, MICH. ATT'Y GEN. (May 16, 2023), https://www.michigan.gov/ag/news/press-releases/2023/05/16/fortra-data-breach-targets-130-companies-many-in-healthcare-sector.

[43] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/cd6cca3b-8ef7-40fd-8814-d0688c72716a.shtml (last visited Apr. 16, 2024).

[44] *Id*.

[45] *Id*.

[46] *Id*.

months, until or about June 30, 2023, to issue a notice of data security incident ("Imagine360 Notice").

262. The Imagine360 Notice indicated that the information impacted included: names, medical information, health insurance information, and Social Security Numbers. The Data Breach impacted the information of over 130,000 individuals who have had healthcare claims processed by Imagine360.

263. According to the Imagine360 Notice, it conducted a diligent investigation to confirm the full nature and scope of the Data Breach.

264. As a result of Imagine360's delayed notification, Imagine360 Plaintiffs were completely unaware their PII/PHI was exposed because of the Data Breach.

Brightline's Notification of Fortra's 2023 Data Breach

265. On or about May 5, 2023, three months after learning of the Data Breach, Brightline publicly announced through its website[47] that it was one of the entities impacted by the Fortra Data Breach, and that the PII and PHI of certain of its patients and employees of its clients, including that of children, were exposed.

266. Brightline delivered its notice to the Brightline Plaintiffs and Class Members between mid-April and mid-May 2023 – over three months after learning of the Data Breach – alerting them that their highly sensitive Private Information had been exposed. The initial notices sent in April 2023 were only sent to approximately 28,000 impacted individuals. The over 900,000 other victims were not notified until May 2023.

267. Brightline's announcement of the Data Breach received widespread coverage in the media. One of the outlets that covered it was the website "BleepingComputers.com," a website

[47] *See* https://www.hellobrightline.com/fortra-data-notice (last visited on April 17, 2024).

known for its reporting on data breaches. The website stated that at the time of the article, the Data Breach was thought to have impact 783,606 Brightline patients, "[h]owever, this figure may increase as internal investigations progress."[48] In addition to reporting on Brightline's notice, BleepingComputer.com also reported that Brightline was "listed on Clop's extortion portal on March 16th, 2023, indicating that the health startup was among the firms the ransomware actors breached in their large-scale attack."[49] The outlet then noted that "Brightline's extensive partnerships with healthcare institutes and companies in the U.S. has resulted in a security incident impacting many entities. This includes well-known organizations like Diageo, Nintendo of America Inc., Harvard University, Stanford University, and Boston Children's Hospital."[50] Brightline maintains a list of the 64 impacted entities on its website.[51]

268. After BleepingComputer.com posted its news story on May 3, 2023, the Clop ransomware gang emailed the website on May 5, 2023 to state that it removed Brightline's information from its data leak website. The gang told BleepingComputer.com that:

> We delete the data and we did not know what this company is doing, because not all companies are analyzing. And we ask for forgiveness for this incident.[52]

269. BleepingComputer.com was unable to confirm whether Clop had fully deleted the information in its possession, but the website did confirm that Brightline was no longer listed on the gang's data leak website. However, BleepingComputer.com was unable to provide information

---

[48] *See* https://www.bleepingcomputer.com/news/security/brightline-data-breach-impacts-783k-pediatric-mental-health-patients/#:~:text=Update%205%2F3%2F23%3A,not%20all%20companies%20are%20analyzing (last visited on April 17, 2024).

[49] *Id*.

[50] *Id*.

[51] *See* https://www.hellobrightline.com/list-of-impacted-covered-entities (last visited on April 17, 2024).

[52] *Id.*

regarding who downloaded the Brightline files from Clop's data link website in the *fifty days* it was available for download (from March 16th to May 5th).

The Healthcare Sector is Particularly Susceptible to Data Breaches.

270. Defendants were on notice that companies in the healthcare industry, including Defendants' vendors, are susceptible targets for data breaches.

271. Defendants were also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a previous cyberattack on Defendant CHS, the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[53]

272. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting confidential medical information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[54]

273. The healthcare sector reported the second largest number of data breaches among

[53] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on Apr. 17, 2024).

[54] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on Apr. 17, 2024).

all measured sectors in 2018, with the highest rate of exposure per breach.[55] In 2022, the largest growth in data compromises occurred in the healthcare sector.[56]

274. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[57]

275. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[58]

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

---

[55] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on Apr. 17, 2024).

[56] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on Apr. 17, 2024).

[57] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on Apr. 17, 2024).

[58] *Id*.

organization, including credit bureaus, have so much monetizable information stored in their data centers."[59]

277. Defendants knew, or should have known, the importance of safeguarding its clients', patients', and/or employees' PII/PHI, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a Data Breach. Defendants failed, however, to ensure its vendor, Fortra, took adequate cybersecurity measures to prevent the Data Breaches from occurring.

Defendants Failed to Comply with HIPAA.

278. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301 et seq. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendants failed to secure. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

279. The Data Breaches resulted from a combination of insufficiencies that indicate Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from the Data Breach that Defendants failed to ensure Fortra implemented information security policies or procedures sufficient to protect Plaintiffs' and Class Members' PHI.

280. Plaintiffs' and Class Members' PII/PHI compromised in the 2023 Fortra Data Breach included "protected health information" as defined by CFR § 160.103.

[59] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on Apr. 17, 2024).

281. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

282. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

283. Plaintiffs' and Class Members' PII/PHI included "unsecured protected health information" as defined by 45 CFR § 164.402.

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

285. Based upon Defendants' Notices to Plaintiffs and Class Members, Defendants reasonably believe that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

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

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

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

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

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

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

291. Defendants' security failures also include, but are not limited to:

a. Failing to adequately screen its vendors and ensure Fortra was capable of maintaining the confidentiality, integrity, and availability of all electronic protected health information it creates, receives, maintains, or transmits", and guarantee Fortra was able to "protect against any reasonably anticipated threats or hazards to the security or integrity of such information," in violation of 45 C.F.R. § 164.306 (emphasis added);

b. Failing to ensure Fortra implemented policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR § 164.308(a)(1);

c. Failing to ensure Fortra was capable of mitigating, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR § 164.308(a)(6)(ii);

d. Failing to guarantee Fortra was equipped with adequate data security to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR § 164.306(a)(2);

e. Failing to guarantee Fortra was equipped with adequate data security to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR § 164.306(a)(3); and

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

292. Because Defendants failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Defendants' approach to vendor screening, information security, especially as such approach relates to the supervision of its business associates, vendors, and/or suppliers, is adequate and appropriate going forward. Defendants still maintain the PHI and other highly sensitive PII of its clients' current and former patients and/or employees. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' PII/PHI remains at risk of subsequent data breaches.

Defendants Failed to Comply with FTC Guidelines.

293. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

294. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should ensure the protection of the personal customer information that they collect, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

296. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

297. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Specifically, Defendants failed to ensure that its vendor, Fortra, maintained adequate data security in providing file transfer and data management services. Defendants' failure to conduct adequate vendor screening guaranteeing the protection of Plaintiffs' and Class Members' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

298. At all times, Defendants were fully aware of its obligations to conduct adequate vendor screening to protect the PII/PHI of its clients' patients and/or employees yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendants Breached Their Duty to Safeguard Plaintiffs' and Class Members' PII/PHI.

299. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to adequately screen their vendors, including Fortra, to ensure it provided reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII/PHI of Plaintiffs and Class Members.

300. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because it failed to adequately screen Fortra to ensure it was capable of properly maintaining and safeguarding its computer systems containing Plaintiffs' and Class Members' data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to ensure Fortra was capable of adequately protecting Plaintiffs' and Class Members' PII/PHI;

b. Failing to sufficiently monitor Fortra regarding the proper handling of its clients' patients' and/or employees' PII/PHI;

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

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

e. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' PII/PHI.

301. Had Defendants remedied the deficiencies in their vendor screening, security practices, procedures, and protocols, followed industry guidelines, and ensured Fortra adopted data security monitoring, supervision, and other measures recommended by experts in the field, they could have prevented the theft of Plaintiffs' and Class Members' confidential PII/PHI.

302. Accordingly, Plaintiffs' and Class Members' lives have been severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, medical fraud and identity theft.

Defendants Knew or Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft.

303. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[60] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

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

305. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

[60] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited Apr. 17, 2024).

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

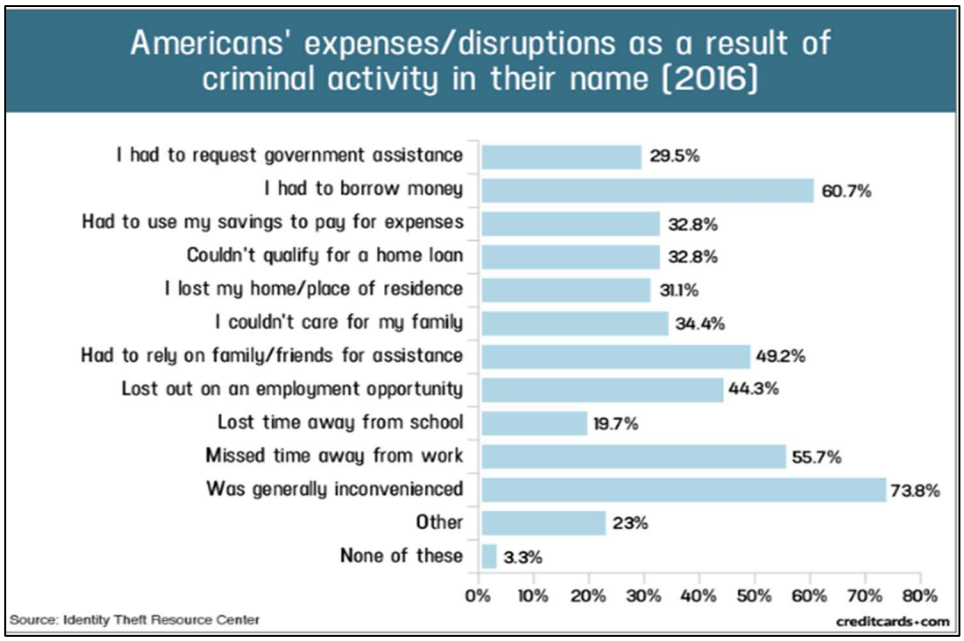
306. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

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

308. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[61] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[61] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Apr. 17, 2024).

309. In fact, a study by the Identity Theft Resource Center[62] shows the multitude of harms caused by fraudulent use of PII:



310. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[63]

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

[62] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Apr. 17, 2024).

[63] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Apr. 17, 2024).

312. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[64]

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

314. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[65]

315. The ramifications of Defendants' failures to conduct adequate vendor screening necessary to keep its clients' patients' and/or employees' PII/PHI secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

316. Here, not only was sensitive medical information compromised, but Social Security numbers have been compromised too. The value of both PII and PHI is axiomatic. The value of

[64] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Apr. 17, 2024).

[65] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Apr. 17, 2024).

"big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the PII/PHI compromised here has considerable market value.

317. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[66]

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

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

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

The Foreseeability of a Data Breach

320. It is well known among companies that store sensitive PII that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in a

[66] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Apr. 17, 2024).

data breach—is valuable and frequently targeted by criminals. A recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[67]

321. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were 1,161 medical data breaches in 2023 with over 171 million patient records exposed.[68] This is an increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[69]

322. PII/PHI is a valuable property right.[70] The value of PII/PHI as a commodity is measurable.[71] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[72] American companies are estimated to have spent over $19 billion on acquiring

---

[67] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[68] *See* Protenus, *2024 Breach Barometer* 2 (2024), https://www.protenus.com/breach-barometer-report (last visited Apr. 3, 2024).

[69] *See id*.

[70] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), available at https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[70] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[71] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[72] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

personal data of consumers in 2018.[73] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

323. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

324. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[74] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[75]

325. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[76] According to a report released by the Federal Bureau of Investigation's

---

[73] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[74] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[75] *Id.*

[76] *See* Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market..

("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[77]

326. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[78] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[79]

327. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[80]

328. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[77] *See* FBI Cyber Division, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, PUB. INTEL. (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf .

[78] Steager, *supra* note 43.

[79] *Id.*

[80] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims.

329. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[81]

330. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[82] Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[83]

331. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the

[81] *See What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Apr. 3, 2024).

[82] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[83] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

victim's information. Identity thieves may even give the victim's personal information to police during an arrest.[84]

332. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[85]

333. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new Social Security number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

334. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[86]

335. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records

---

[84] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Apr. 3, 2024).

[85] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Apr. 3, 2024).

[86] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

that can plague victims' medical and financial lives for years."[87] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[88] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [89] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[90]

336. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

---

[87] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[88] *See* FBI Cyber Division, *Health Care Systems and Medical Devices at Risk*…, *supra* note 46.

[89] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Apr. 3, 2024).

[90] *Id*.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[91]

337. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[92]

338. It is within this context that Plaintiffs and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiffs and the Other Class Members

339. 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 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

[91] *See* Dixon & Emerson, *supra* n.56.

[92] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

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) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

340. This action is brought and may be properly maintained as a class action pursuant to Rules 23(a), 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of the various putative classes in the Track 4 actions.

Class Definitions – Community Defendants

341. The Community Plaintiffs bring this action on behalf of themselves and all members of the following Community Nationwide Class of similarly situated persons:

> All persons in the United States and its territories whose personally identifiable information or personal health information was compromised in the Community Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

342. In the alternative to the Community Nationwide Class, the Community Plaintiffs seek to represent each of the following Community State Classes (the Community Nationwide Class and Community State Classes are collectively referred to as the "Community Class"):

> **Alabama Class:** All persons in Alabama whose personally identifiable information or personal health information was compromised in the Community Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **Florida Class:** All persons in Florida whose personally identifiable information or personal health information was compromised in the Community Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **Mississippi Class:** All persons in Mississippi whose personally identifiable information or personal health information was compromised in the Community Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

Pennsylvania Class: All persons in Pennsylvania whose personally identifiable information or personal health information was compromised in the Community Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

Tennessee Class: All persons in Tennessee whose personally identifiable information or personal health information was compromised in the Community Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

343. Excluded from the Community Class are Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

Class Definitions – Brightline

344. The Brightline Plaintiffs bring this action on behalf of themselves and all members of the following Brightline Nationwide Class of similarly situated persons:

All persons in the United States and its territories whose personally identifiable information or personal health information was compromised in the Brightline Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

345. In the alternative to the Brightline Nationwide Class, the Brightline Plaintiffs seek to represent each of the following Brightline State Classes (the Brightline Nationwide Class and Brightline State Classes are collectively referred to as the "Brightline Class"):

California Class: All persons in California whose personally identifiable information or personal health information was compromised in the Brightline Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

Illinois Class: All persons in Illinois whose personally identifiable information or personal health information was compromised in the Brightline Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

New Jersey Class: All persons in New Jersey whose personally identifiable information or personal health information was compromised in the Brightline Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach

> **Pennsylvania Class:** All persons in Pennsylvania whose personally identifiable information or personal health information was compromised in the Brightline Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **Tennessee Class:** All persons in Tennessee whose personally identifiable information or personal health information was compromised in the Brightline Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **Virginia Class:** All persons in Virginia whose personally identifiable information or personal health information was compromised in the Brightline Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

346. Excluded from the Brightline Class are Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

Class Definitions – Imagine360

347. The Imagine360 Plaintiffs bring this action on behalf of themselves and all members of the following Imagine360 Nationwide Class of similarly situated persons:

> All persons in the United States and its territories whose personally identifiable information or personal health information was compromised in the Imagine360 Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

348. In the alternative to the Imagine360 Nationwide Class, the Imagine360 Plaintiffs seek to represent each of the following Imagine360 state subclasses (the Imagine360 Nationwide Class and Imagine360 State Classes are collectively referred to as the "Imagine360 Class"):

> **Illinois Class**: All persons in Illinois whose personally identifiable information or personal health information was compromised in the Imagine360 Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **Pennsylvania Class**: All persons in Pennsylvania whose personally identifiable information or personal health information was compromised in the Community Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

349. Excluded from the Imagine360 Class are Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

Class Definitions – Intellihartx

350. The ITx Plaintiffs bring this action on behalf of themselves and all members of the following ITx Nationwide Class of similarly situated persons:

> All persons in the United States and its territories whose personally identifiable information or personal health information was compromised in the ITx Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

351. In the alternative to the ITx Nationwide Class, the ITx Plaintiffs seek to represent each of the following ITx state subclasses (the ITx Nationwide Class and ITx state subclasses are collectively referred to as the "ITx Class"):

> **Arizona Class:** All persons in Arizona whose personally identifiable information or personal health information was compromised in the ITx Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **Massachusetts Class:** All persons in Massachusetts whose personally identifiable information or personal health information was compromised in the ITx Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **Missouri Class**: All persons in Missouri whose personally identifiable information or personal health information was compromised in the ITx Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **New Jersey Class:** All persons in New Jersey whose personally identifiable information or personal health information was compromised in the ITx Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.
>
> **Ohio Class:** All persons in Ohio whose personally identifiable information or personal health information was compromised in the ITx Data Breach by

unauthorized persons, including all persons who were sent a notice of the Data Breach.

352. Excluded from the ITx Class are Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

Common Class Action Allegations as to all Track 4 Defendants

353. The Community Class, the Brightline Class, the Imagine360 Class, and the ITx Class are collectively referred to herein as the "Class."

354. Certification of Plaintiffs' claims for class wide treatment is appropriate because Plaintiffs in each of the Track 4 cases can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

355. The members of the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable.

356. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendants had duties not to disclose the PII/PHI of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII/PHI;

d. Whether Defendants knew or should have known that Fortra's network and systems were susceptible to a data breach;

e. Whether Defendants knew or should have known that their data security procedures and monitoring processes were deficient;

f. Whether Defendants were negligent in failing to adequately monitor and audit the data security systems of Fortra;

g. Whether Defendants' efforts (or lack thereof) to ensure the security of Plaintiffs' and Class members' Private Information provided to Fortra were reasonable in light of known legal requirements;

h. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

i. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiffs and Class members;

j. Whether Defendants breached their duties to protect Plaintiffs' and Class members' PII/PHI; and

k. Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

357. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

358. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

359. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

360. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class, or alternatively, Plaintiffs and the State Classes)

361. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

362. All Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding, securing, and protecting the PII/PHI in their possession, custody, or control. This duty extended to any vendor selected by Defendants to be entrusted with the sensitive data of Plaintiffs and Class Members.

363. Defendants knew or should have known the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining and using secure systems. Defendants knew or should have known of the many data breaches that have targeted companies that stored PII/PHI in recent years.

364. 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 and foreseen that the third parties with whom they contract could have vulnerabilities in their systems and prevented the dissemination of Plaintiffs' and Class members' PII/PHI.

365. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to ensure that the third parties that they share PII/PHI with 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 them—including Plaintiffs' and Class members' PII/PHI.

366. Plaintiffs and Class members had no ability to protect their PII/PHI that was, or remains, in Defendants' possession.

367. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to ensure that the third parties that they share PII/PHI with 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' PII/PHI to unauthorized individuals.

368. 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. The PII/PHI of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, ensuring that third parties they contract with and share PII/PHI with adopt, implement, and maintain appropriate security measures.

369. 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 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) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class, or alternatively, Plaintiffs and the State Classes)

370. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

371. 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").

372. 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 businesses of failing to employ reasonable measures to protect and secure PII/PHI.

373. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to ensure that third parties they contract with and shares PII/PHI with use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and comply 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.

374. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

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

376. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

377. It was, or should have been, reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to ensure that the third-parties that they contract with and shares PII/PHI with 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.

378. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA.

379. 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 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; (vii) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class, or alternatively, Plaintiffs and the State Classes)

380. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

381. As a condition of obtaining services or employment from Defendants, Plaintiffs and Class members gave Defendants their PII/PHI in confidence, believing that they would protect that information. Plaintiffs and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between Defendants and Plaintiffs and Class members. In light of this relationship, Defendants must act primarily for the benefit of their and their affiliates' patients and employees, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

382. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. It breached that duty by failing to ensure that the third-parties they contract with and share PII/PHI with properly protect the integrity of the system containing Plaintiffs' and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that they collected.

383. As a direct and proximate result of Defendants' breach of their fiduciary duties, 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 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; (vii) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class, or alternatively, Plaintiffs and the State Classes)

384. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

385. In connection with receiving health care services or employment, Plaintiffs and all other Class members entered into implied contracts with Defendants.

386. Pursuant to these implied contracts, Plaintiffs and Class members benefited Defendants, directly or through an affiliate, through their labor or by paying monies to Defendants, and provided Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and Plaintiffs understood that Defendants would: (1) provide products, services, or employment, to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; (3) protect Plaintiffs' and Class

members' PII/PHI in compliance with federal and state laws and regulations and industry standards; and (4) ensure third parties they contract with and provide PII/PHI to implement and maintain reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI.

387. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Defendants, on the other hand. Indeed, as set forth *supra*, Defendants recognized the importance of data security and the privacy of their and their affiliates' patients' and employees' PII/PHI. Had Plaintiffs and Class members known that Defendants would not adequately protect their PII/PHI, they would not have paid for products or services or obtained employment from Defendants.

388. Plaintiffs and Class members performed their obligations under the implied contract when they provided Defendants with their PII/PHI and paid for products and services from Defendants or their affiliates, or completed work for Defendants or their affiliates, expecting that their PII/PHI would be protected.

389. Defendants breached their obligations under their implied contracts with Plaintiffs and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to ensure that third parties they contract with and share PII/PHI with implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

390. Defendants' breach of their obligations of the implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiffs and Class members.

391. Plaintiffs and all other Class members were damaged by Defendants' breach of implied contracts because: (i) they paid monies (directly or through their insurers or Defendants' affiliates) or provided labor in exchange for data security protection they did not receive; (ii) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

COUNT V
BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD-PARTY BENEFICIARIES
(On Behalf of Plaintiffs and the Class, or alternatively, Plaintiffs and the State Classes)

392. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

393. This claim is pleaded in the alternative to the breach of implied contract claim and unjust enrichment claim.

394. Plaintiffs bring this claim individually and on behalf of the Class.

395. Defendants had valid contracts with each of the hospitals and clinics at which Plaintiffs and Class members received services or employment. A principal purpose of those contracts was to securely store, transmit, and safeguard the PII/PHI of Plaintiffs and Class members.

396. Upon information and belief, Defendants and each of the contracting hospitals and clinics expressed an intention that Plaintiffs and Class members were intended third-party beneficiaries of these agreements.

397. Plaintiffs and Class members are also intended third-party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that Defendants intended to give the beneficiaries the benefit of the promised performance.

398. Defendants breached their agreements with the contracting hospitals and clinics by allowing the Data Breach to occur, and as otherwise set forth herein.

399. Defendants' breach caused foreseeable and material damages to Plaintiffs and Class members.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class, or alternatively, Plaintiffs and the State Classes)

400. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

401. This claim is pleaded in the alternative to the breach of implied contract claim and intended third party beneficiary claim.

402. In obtaining services or employment from Defendants, Plaintiffs and Class members provided and entrusted Defendants with their PII and PHI.

403. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of monies paid for products or services or via the value of their labor (including by facilitating payments to Defendants), with an implicit understanding that Defendants would use some of their revenue to protect the PII/PHI they collect.

404. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. Defendants benefitted from the receipt of Plaintiffs' and Class members' PII/PHI, as this was used to facilitate billing and payment services, as well as from Plaintiffs' and Class members' labor, which enabled Defendants to carry out their business.

405. As a result of Defendants' conduct, Plaintiffs and Class members suffered actual damages.

406. Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to adequately implement the data privacy and security procedures for itself and the third parties that they contract with and share PII/PHI with that Plaintiffs and Class members paid for and expected, and that were otherwise mandated by federal, state, and local laws and industry standards.

407. Defendants should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds they received as a result of the conduct and Data Breach alleged herein.

CLAIMS AGAINST THE COMMUNITY DEFENDANTS ONLY

COUNT VII
VIOLATIONS OF ALABAMA DECEPTIVE TRADE PRACTICES ACT
Ala. Code § 8-19-1 et seq.
(Against the Community Defendants on Behalf of the Community Alabama Class)

408. Community Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

409. The Alabama Deceptive Trade Practices Act ("ADTPA") was created to protect Alabama consumers from fraudulent or deceptive business practices.

410. Plaintiff Angela Martin ("Alabama Plaintiff") and Alabama Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

411. As set forth more fully above, Defendants caused injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

412. Defendants failed to disclose the breach for nearly two months and breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

413. Defendants' conduct constituted, among other things, the following prohibited fraudulent, deceptive, unconscionable, and unfair business practices: (a) engaging in fraudulent, deceptive, unconscionable, and unfair conduct that creates a likelihood of confusion and misunderstanding; and (b) engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

414. Defendants' conduct was deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive, ordinary consumers, including Alabama Plaintiff. Knowledge of those facts would have been a substantial factor in Alabama Plaintiff's, as well as Alabama Class members' decision to take steps to protect their PII/PHI and to protect themselves from identity theft.

415. Defendants owed Alabama Plaintiff and Alabama Class members, among others, a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be material to

reasonable consumers; because Defendants actively concealed them; and because Defendants intended for customers to rely on the safety of their PII/PHI.

416. Alabama Plaintiff and members of the Alabama Class justifiably relied on the material representations and/or omissions by Defendants, and reasonable consumers would have been expected to rely upon these omissions, in part, because they are omissions that impact PII/PHI.

417. Defendants' conduct actually and proximately caused an actual ascertainable loss of money or property to Alabama Plaintiff (as set forth above) and members of the Alabama Class. Absent Defendants' unfair, deceptive, fraudulent and/or unconscionable conduct, Alabama Plaintiff and Alabama Class members would have behaved differently and would not have provided their PHI or PII to Defendants.

418. Accordingly, pursuant to Ala. Code § 8-19-10(a)(1), Alabama Plaintiff and Alabama Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence.

COUNT VIII
VIOLATIONS OF MISSISSIPPI DECEPTIVE TRADE PRACTICES ACT
Miss. Code § 75-24-1 et seq.
(Against the Community Defendants on Behalf of the Community Mississippi Class)

419. Community Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

420. The Mississippi Consumer Protection Act was created to protect Mississippi consumers from unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce.

421. Plaintiffs Lola Tatum and Brandy McGowen ("Mississippi Plaintiffs") and Mississippi Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

422. As set forth more fully above, Defendants caused injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

423. Defendants concealed and failed to disclose the breach for nearly two months, and in doing so, breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

424. Defendants' conduct described herein constitutes the act, use or employment of deception, false promise, misrepresentation, unfair practice and the concealment, suppression, and omission of material facts in connection with Data Breach in Mississippi, made with the intention that Plaintiff and Mississippi Class members would rely on the safety of their PII/PHI, making it unlawful under Miss. Code § 75-24-1 et seq.

425. Defendants' conduct constituted, among other things, the following unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce: (a) causing a probability of confusion or misunderstanding as to the source, sponsorship, approval, or certification of goods or services; (b) representing that goods or services are of a particular standard, quality, or grade; (c) advertising or representing goods or services with intent not to dispose of those goods or services as advertised or represented; (d) failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer; (e) making a representation of fact or statement of fact

material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is; and (f) failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

426. Defendants' conduct was unfair, unconscionable, or deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive ordinary consumers, including Mississippi Plaintiffs. Knowledge of those facts would have been a substantial factor in Mississippi Plaintiffs,' as well as Mississippi Class members' decision to rely on the safety of their PII/PHI.

427. Defendants owed Mississippi Plaintiffs and Mississippi Class members, among others, a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be material to reasonable consumers; because Defendants actively concealed them; and because Defendants intended for consumers to rely on the safety of their PII/PHI.

428. Mississippi Plaintiffs and members of the Mississippi Class justifiably relied on the material misrepresentations and/or omissions by Defendants, and reasonable consumers would have been expected to rely upon these representations and/or omissions, in part, because they are representations and/or omissions that impact decisions to take steps to protect their PII/PHI and to protect themselves from identity theft.

429. Accordingly, pursuant to Miss. Code §§ 75-24-1 *et seq.*, Mississippi Plaintiffs and Mississippi Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Mississippi Plaintiffs and Mississippi Class members are also entitled to all available statutory, exemplary, treble, and/or punitive damages and attorneys' fees based on the amount of time

reasonably expended and equitable relief necessary or proper to protect them from Defendants unlawful conduct.

COUNT IX
VIOLATIONS OF PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
73 Pa. Stat. Ann. § 201-1 et seq.
(Against the Community Defendants on Behalf of the Community Pennsylvania Class)

430. Community Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

431. The Pennsylvania Unfair Trade Practices and Consumer Protection Law was created to protect Pennsylvania consumers from fraudulent or deceptive business practices.

432. Plaintiff Kelly Kern ("Pennsylvania Plaintiff") and Pennsylvania Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

433. As set forth more fully above, Defendants caused injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

434. Defendants concealed and failed to disclose the breach for nearly two months, and in doing so, breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

435. Defendants concealed and failed to disclose that they lacked sufficient measures in place to safeguard the sensitive data entrusted to them (and which they entrusted to a vendor).

436. Defendants' conduct was fraudulent and deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in

fact, did deceive ordinary consumers, including Pennsylvania Plaintiff. Ordinary consumers, including Pennsylvania Plaintiff, would have found it material to their healthcare or employment decisions that Defendants lacked adequate security measures to adequately safeguard their PII/PHI. Knowledge of those facts would have been a substantial factor in Pennsylvania Plaintiffs,' as well as other Pennsylvania Class members' decision to obtain services or provide labor to Defendants.

437. Defendants owed Pennsylvania Plaintiff and Pennsylvania Class members, among others, a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be material to reasonable consumers; because Defendants actively concealed them; and because Defendants intended for consumers to rely on the omissions in question.

438. Pennsylvania Plaintiffs, and members of the Pennsylvania Class, justifiably relied on the material misrepresentations and/or omissions by Defendants, and reasonable consumers would have been expected to rely upon these omissions, in part, because they are omissions that impact seriously on a consumer's PII/PHI.

439. Accordingly, pursuant to the 73 Pa. Stat. Ann. § 201-1 et seq., Pennsylvania Plaintiff and Pennsylvania Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Pennsylvania Plaintiff and Pennsylvania Class members are also entitled to recover all available statutory, exemplary, treble, and/or punitive damages, costs of suit, and attorneys' fees based on the amount of time reasonable expended and equitable relief necessary, and all such other relief as the Court deems proper.

COUNT X
VIOLATIONS OF TENNESSEE CONSUMER PROTECTION ACT
Tenn. Code Ann. § 47-18-101 et seq.
(Against the Community Defendants on Behalf of the Community Tennessee Class)

440. Community Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

441. The Tennessee Consumer Protection Act ("TCPA") was created to protect Tennessee consumers from fraudulent or deceptive business practices.

442. Plaintiff Sandra Kuffrey, Plaintiff Wilhelmina Gill, and Plaintiff Timothy Ferguson ("Tennessee Plaintiffs"), Tennessee Class members, and Defendants are persons under the TCPA.

443. Tennessee Plaintiffs and Tennessee Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

444. As set forth more fully above, Defendants caused injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

445. Defendants concealed and failed to disclose the breach for nearly two months, and in doing so, breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

446. Defendants concealed and failed to disclose in any of their marketing materials, advertising, packaging, and/or any other communication that they lacked sufficient measures in place to safeguard the sensitive data entrusted to them (and which they entrusted to a vendor).

447. Defendants' conduct constitutes "[u]nfair or deceptive acts or practices affecting the conduct of any trade or commerce" in Tennessee, making it unlawful under Tenn. Code Ann. § 47-18-104(a).

448. Under the circumstances herein, Defendants' failure to disclose that they lacked sufficient and reasonable data security protections constituted fraudulent, deceptive, and unfair business practices.

449. Defendants' conduct was fraudulent and deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive ordinary consumers, including Tennessee Plaintiffs and Tennessee Class members. Ordinary consumers, including Tennessee Plaintiffs and Tennessee Class members, would have found it material to their conduct had they known that Defendants lacked sufficient data security measures.

450. Defendants owed Tennessee Plaintiffs and Tennessee Class members a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be material to reasonable consumers; because Defendants actively concealed them and because Defendants intended for consumers to rely on the omissions in question.

451. Tennessee Plaintiffs and members of the Tennessee Class justifiably relied on the material misrepresentations and/or omissions by Defendants, and reasonable consumers would have been expected to rely upon these omissions, in part, because they are omissions that impact seriously on a consumer's PII/PHI.

452. Defendants' conduct actually and proximately caused an ascertainable loss of money or property to the Tennessee Plaintiffs (as set forth above) and members of the Tennessee Class. Absent Defendants' unfair, deceptive, and/or fraudulent conduct, Tennessee Plaintiffs and Tennessee Class members would have behaved differently and would not have entrusted their most sensitive PII and PHI to Defendants.

453. Accordingly, pursuant to the aforementioned statutes, Tennessee Plaintiffs and Tennessee Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Tennessee Plaintiffs and Tennessee Class members are also entitled to recover all available statutory, exemplary, treble, and/or punitive damages, costs of suit, and attorneys' fees based on the amount of time reasonable expended and equitable relief necessary, and all such other relief as the Court deems proper.

CLAIMS AGAINST BRIGHTLINE ONLY

COUNT XI
VIOLATIONS OF CALIFORNIA'S UNFAIR COMPETITION LAW, BUS. & PROF. CODE § 17200 et seq. ("UCL")
(Against Brightline on Behalf of the Brightline California Class)

454. Plaintiff Ndifor restates and realleges all the allegations in paragraphs 1-360 above as if fully set forth herein.

455. The California Unfair Competition Law provides that:

> "[U]nfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code." (BUS. & PROF. CODE § 17200.)

456. Brightline stored the Private Information of Plaintiff Ndifor and the California Class in its computer systems and knew or should have known it did not employ reasonable, industry standard and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and California Class Members' Private Information secure and prevented the loss or misuse of such.

457. Brightline failed to disclose to Plaintiff Ndifor and the California Class that their Private Information was not secure. At no time were they on notice that their Private Information was not secure, which Brightline had a duty to disclose.

458. Had Brightline complied with these requirements, Plaintiff Ndifor and the California Class would not have suffered the damages related to the Data Breach.

459. Brightline's conduct was unlawful, in that it violated the policy set forth in (a) California's Medical Information Act, requiring the safeguard of personal health information like the Private Information compromised as a result of the Data Breach, (b) HIPAA and the FTCA, as identified above, and (c) Brightline's common law duty to safeguard PII and PHI.

460. Brightline's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting patients' and Brightline's clients' employees' Private Information from data breaches.

461. Brightline also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Brightline's acts and omissions thus amount to a violation of the law.

462. As a result of those unlawful and unfair business practices, Plaintiff Ndifor and the California Class suffered an injury-in-fact and have lost money or property, be it tangible or intangible.

463. The injuries to Plaintiff and the California Class greatly outweigh any alleged countervailing benefit to patients, consumers, or competition under all of the circumstances.

464. There were reasonably available alternatives to further Brightline's legitimate business interests, other than the misconduct alleged in this complaint.

465. Therefore, Plaintiff Ndifor and the California Class are entitled to equitable relief, including restitution of all monies paid to or received by Brightline; disgorgement of all profits accruing to Brightline because of its unfair and improper business practices; a permanent injunction enjoining Brightline's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT XII
VIOLATIONS OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56 et seq. ("CMIA")
(Against Brightline on Behalf of the Brightline California Class)

466. Plaintiff Ndifor restates and realleges all the allegations in paragraphs 1-360 above as if fully set forth herein.

467. Brightline is a "contractor," as defined in Cal. Civ. Code § 56.05(d), a "pharmaceutical company," as defined in *id.* § 56.05(1), and "a provider of health care," as defined in Cal. Civ. Code § 56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

468. Brightline is a person licensed under California under California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code § 4000 et seq. Brightline therefore qualifies as a "provider of health care" under the CMIA.

469. Plaintiff Ndifor and California Class members are "patients," as defined in CMIA, Cal. Civ. Code § 56.05(k).

470. Brightline disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Brightline's employees, which allowed the hackers to see and obtain Plaintiff Ndifor's and California Class members' medical information.

471. Brightline's negligence resulted in the release of PHI pertaining to Plaintiff Ndifor and the California Class to unauthorized persons and the breach of the confidentiality of that information.

472. Brightline's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and California Class members' medical information in a manner that preserved the confidentiality of the information contained therein is a violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

473. Brightline's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A).

474. Plaintiff Ndifor and the California Class were injured and have suffered damages, as described above, from Brightline's illegal disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

COUNT XIII
VIOLATIONS OF CALIFORNIA'S CONSUMER RECORDS ACT, CAL. CIV. CODE § 1798.82 et seq. ("CCRA")
(Against Brightline on Behalf of the Brightline California Class)

475. Plaintiff Ndifor restates and realleges all the allegations in paragraphs 1-360 above as if fully set forth herein.

476. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay. . . ."

477. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

478. The CCRA specifies certain requirements when entities subject to its purview are required to issue a security breach notification, including that such entities do not unreasonably delay such notifications.

479. Brightline unreasonably delayed before sending notice of the breach to the California Class.

480. As a result of Brightline's violation of the CCRA, Plaintiff Ndifor and the California Class were deprived of prompt notice of the Data Breach and were thus prevented from

taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff Ndifor and California Class members because their stolen information would have had less value to identity thieves.

481. As a result of Brightline's violation of the CCRA, Plaintiff Ndifor and the California Class suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

COUNT XIV
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("ICFA")
(Against Brightline on Behalf of the Brightline Illinois Class)

482. Plaintiff Jackson restates and realleges all the allegations in paragraphs 1-360 above as if fully set forth herein.

483. Plaintiff and Brightline Illinois Class members are considered to be "persons" within the meaning of the statute, 815 Ill. Comp. Stat. § 505/1(c).

484. Brightline is also a "person" within the meaning of the same statute subsection.

485. Brightline engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of ICFA, including:

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

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Brightline Illinois Class members' PHI and PII, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify Plaintiff and Brightline Illinois Class members of the Data Breach;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Brightline Illinois Class members' PII and PHI; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Brightline Illinois Class members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

486. Brightline's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Brightline's data security and ability to protect the confidentiality of PII and PHI.

487. Brightline's representations and omissions were material because they were likely to deceive reasonable consumer-patients.

488. Brightline acted intentionally and knowingly to violate ICFA, and recklessly disregarded Plaintiff's and Brightline Illinois Class members' rights.

489. As a direct and proximate result of Brightline's deceptive and unlawful acts and practices, Plaintiff and the Illinois Subclass have suffered and/or are at a heightened and continual risk of suffering injury, ascertainable losses of money or property, and monetary and non-monetary

damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII and PHI.

490. Brightline's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

491. The above deceptive and unlawful practices and acts by Brightline caused substantial injury to Plaintiff Jackson and Brightline Illinois Class members that they could not reasonably avoid.

492. Plaintiff and the Illinois Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages, treble damages, injunctive relief, and attorney's fees and costs.

COUNT XV
VIOLATIONS OF NEW JERSEY'S CONSUMER FRAUD ACT
(Against Brightline on Behalf of the Brightline New Jersey Class)

493. Plaintiff Milner restates and realleges all the allegations in paragraphs 1-360 above as if fully set forth herein.

494. Brightline is a "person," as defined by N.J.S.A. § 56:8-1(d).

495. Brightline sells "merchandise," as defined by N.J.S.A. § 56:8-1(c) & (e).

496. The New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. §§ 56:8-2 prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

497. New Jersey CFA claims for unconscionable commercial practice need not allege any fraudulent statement, representation, or omission by the defendant. *See Dewey v. Volkswagen AG*, 558 F. Supp. 2d 505, 525 (D.N.J. 2008); *see also Cox v. Sears Roebuck & Co*., 138 N.J. 2, 19 (1994).

498. "The standard of conduct that the term 'unconscionable' implies is lack of 'good faith, honesty in fact and observance of fair dealing.'" *Cox*, 138 N.J. 2 at 18 (quoting *Kugler v. Romain*, 58 N.J. 522, 544 (1971)). "In addition, '[i]ntent is not an essential element' for allegations related to unconscionable commercial practices to succeed." *Fenwick v. Kay Am. Jeep, Inc*., 72 N.J. 372, 379 (1977).

499. Brightline's handling and treatment of Plaintiff Milner's (and her child's) and Brightline New Jersey Class members' Private Information was unconscionable because:

a. Plaintiff and Brightline New Jersey Class members had no choice but to provide their Private Information to Brightline in order to use Brightline's services;

b. To the extent that written contracts exist between Plaintiff and Brightline New Jersey Class members on the one hand and Brightline on the other hand, those written contracts were written by Brightline and were not negotiable;

c. Once Plaintiff and Brightline New Jersey Class members provided their Private Information to Brightline, protection of that Private Information was solely in Brightline's control. There is no way for Plaintiff or Brightline New Jersey Class members to take any reasonable steps on their own to protect the Private Information in Brightline's hands; nor is there any way

that Plaintiff and Brightline New Jersey Class members would have any knowledge that it would be necessary for them to take steps on their own to protect their Private Information;

d. Brightline knew, or should have known, that its data security was inadequate and that it needed to take additional security measures to protect Plaintiff's and Brightline New Jersey Class members' Private Information, but failed to do so, even though Brightline had a non-delegable duty to protect Plaintiff's and Brightline New Jersey Class members Private Information from wrongdoers;

e. Once Brightline became aware of the Data Breach, it failed to timely notify Plaintiff and Brightline New Jersey Class members of the Breach, thus depriving them the opportunity to take measures to protect themselves from the effects of Brightline's failure to protect their Private Information; and

f. Brightline's practices for handing and protecting Plaintiff's and Brightline New Jersey Class members' Private Information was contrary to public policy in that Brightline failed to follow FTC and HIPAA guidelines with respect to the protection of Private Information – including PHI – and otherwise failed to follow industry standards for providing reasonable security and privacy measures to protect Plaintiff's and Brightline New Jersey Class members' Private Information, which was a direct and proximate cause of the Data Breach.

500. Brightline's handling and treatment of Plaintiff's and Brightline New Jersey Class members' Private Information was deceptive because Brightline:

a. Misrepresented that it would protect the privacy and confidentiality of Plaintiff's and Brightline New Jersey Class members' Private Information, including by implementing and maintaining reasonable security measures;

b. Misrepresented that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Brightline New Jersey Class members' Private Information, including duties imposed by the FTC Act, HIPAA, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163 *et seq.*;

c. Omitted, suppressed, and concealed the material fact that it did not properly secure Plaintiff's and Brightline New Jersey Class members' Private Information; and

Omitted, suppressed, and concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Brightline New Jersey Class members' Private Information, including duties imposed by the FTCA, HIPAA, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163 *et seq.*

501. Brightline's representations and omissions were material because they were likely to deceive reasonable consumer-patients about the adequacy of Brightline's data security and ability to protect the confidentiality of patient Private Information.

502. Brightline intended to mislead Plaintiff and Brightline New Jersey Class members and induce them to rely on its omissions of material fact.

503. Brightline acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff's and Brightline New Jersey Class members' rights.

504. As a direct and proximate result of Brightline's unconscionable and deceptive practices, Plaintiff and Brightline New Jersey Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Brightline's services; loss of the value of access to their Private Information; and the value of identity protection services now made necessary by the Data Breach.

505. Plaintiff and Brightline New Jersey Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

COUNT XVI
VIOLATIONS OF THE TENNESSEE CONSUMER PROTECTION ACT, TENN. CODE ANN. § 47-18-101 et seq.
(Against Brightline on Behalf of the Brightline Tennessee Class)

506. Plaintiff Castro restates and realleges all the allegations in paragraphs 1-360 above as if fully set forth herein.

507. Tennessee's Identity Theft Deterrence Act ("ITDA"), under T.C.A § 47-18-2106, states that any violation of the ITDA "constitutes a violation of the Tennessee Consumer Protection Act[,]" ("CPA"). The ITDA further states: "For the purpose of application of the [CPA], any

violation of this part shall be construed to constitute an unfair or deceptive act or practice affecting trade or commerce and subject to the penalties and remedies as provided in that act, in addition to the penalties and remedies set forth in this part."

508. Brightline violated the ITDA because Brightline did not follow its provisions in notifying Plaintiff and the Brightline Tennessee Class about the Data Breach.

509. During the Data Breach, Brightline suffered a "breach of system security" as the ITDA defines that term. Upon information and belief, Brightline maintained the Private Information of Plaintiff and Brightline Tennessee Class members in an unencrypted form, as defined in Tenn. Code Ann. § 47-18-2107(a).

510. The ITDA defines "information holder" to include Brightline because Brightline conducts business in Tennessee.

511. In Tenn. Code Ann. § 47-18-2107(a)(4), the ITDA defines "personal information" to include Plaintiff's and the Brightline Tennessee Class's PII, including their names in combination with the Social Security numbers, driver's license numbers, or any "[a]ccount, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account[.]"

512. Following discovery of the Data Breach, the ITDA required Brightline to notify all Tennessee residents whose "personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security[.]" On information and belief, Brightline's ongoing delay in notifying Plaintiffs and the Brightline Tennessee Class about the Data Breach was not "due to the legitimate needs of law enforcement" as defined by ITDA.

513. Brightline failed to disclose the Data Breach to Plaintiffs and the Brightline Tennessee Class within 45 days of discovering it, meaning it violated the CPA.

514. As a direct and proximate cause of Brightline's ITDA and CPA violations, Plaintiff and the Brightline Tennessee Class have suffered damages, including (i) the compromise, publication, and/or theft of the Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (iv) the continued risk to their Private Information, which remains in Brightline's possession and is subject to further unauthorized disclosures so long as Brightline fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession, and (v) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and the Tennessee Subclass.

515. Plaintiff and the Brightline Tennessee Class are entitled to damages as well as injunctive relief, including, but not limited to, ordering Brightline to: (i) strengthen its data security systems, monitoring procedures, and data breach notification procedures; and (ii) immediately provide adequate credit monitoring to Plaintiff and the Brightline Tennessee Class.

CLAIMS AGAINST IMAGINE360 ONLY

COUNT XVII
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT (ICFA)
(Against Imagine360 on Behalf of the Imagine360 Illinois Class)

516. Imagine360 Plaintiff Collins restates and realleges all the allegations in paragraphs 1-360 above as if fully set forth herein. Plaintiff Collins and Imagine360 Illinois Class members are considered to be "persons" within the meaning of the statute, 815 Ill. Comp. Stat. § 505/1(c).

517. Imagine360 is also a "person" within the meaning of the same statute subsection.

518. Imagine360 engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of ICFA, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Collins' and the Imagine360 Illinois Class members' PII and PHI, which was a proximate and direct cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Collins' and Imagine360 Illinois Class members' PHI and PII, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify Plaintiff Collins and Imagine360 Illinois Class members of the Data Breach;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Collins' and Imagine360 Illinois Class members' PII and PHI; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Collins' and Imagine360 Illinois Class members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

519. Imagine360's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Imagine360's data security and ability to protect the confidentiality of PII and PHI.

520. Imagine360's representations and omissions were material because they were likely to deceive reasonable consumer-patients

521. Imagine360 acted intentionally and knowingly to violate ICFA, and recklessly disregarded Plaintiff Collins' and Imagine360 Illinois Class members' rights.

522. As a direct and proximate result of Imagine360's deceptive and unlawful acts and practices, Plaintiff Collins and the Imagine360 Illinois Subclass have suffered and/or are at a heightened and continual risk of suffering injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII and PHI.

523. Imagine360's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

524. The above deceptive and unlawful practices and acts by Imagine360 caused substantial injury to Plaintiff Collins and Imagine360 Illinois Class members that they could not reasonably avoid.

525. Plaintiff Collins and the Imagine360 Illinois Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages, treble damages, injunctive relief, and attorneys' fees and costs.

COUNT XVIII
VIOLATIONS OF PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
73 Pa. Stat. Ann. § 201-1 *et seq.*
(Against Imagine360 on Behalf of the Imagine360 Pennsylvania Class)

526. Imagine360 Plaintiff McGee re-alleges and incorporates by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

527. The Pennsylvania Unfair Trade Practices and Consumer Protection Law was created to protect Pennsylvania consumers from fraudulent or deceptive business practices.

528. Plaintiff McGee and the Imagine360 Pennsylvania Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Imagine360.

529. As set forth more fully above, Imagine360 caused injury and damages including, inter alia, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

530. Imagine360 concealed and failed to disclose the breach for nearly five months, and in doing so, breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

531. Imagine360 concealed and failed to disclose that they lacked sufficient measures in place to safeguard the sensitive data entrusted to them (and which they entrusted to a vendor).

532. Imagine360's conduct was fraudulent and deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and,

in fact, did deceive ordinary consumers, including Imagine360 Plaintiff McGee. Ordinary consumers, including Plaintiff McGee, would have found it material to their healthcare or employment decisions that Imagine360 lacked adequate security measures to adequately safeguard their PII/PHI. Knowledge of those facts would have been a substantial factor in Plaintiff McGee's as well as other Imagine360 Pennsylvania Class members' decision to obtain services from Imagine360.

533. Imagine360 owed Plaintiff McGee and Imagine360 Pennsylvania Class members, among others, a duty to disclose these facts because they were known and/or accessible exclusively to Imagine360 who had exclusive and superior knowledge of the facts; because the facts would be material to reasonable consumers; because Imagine360 actively concealed them; and because Imagine360 intended for consumers to rely on the omissions in question.

534. Plaintiff McGee and members of the Imagine360 Pennsylvania Class justifiably relied on the material misrepresentations and/or omissions by Imagine360, and reasonable consumers would have been expected to rely upon these omissions, in part, because they are omissions that seriously impact a consumer's PII/PHI.

535. Accordingly, pursuant to the 73 Pa. Stat. Ann. § 201-1 et seq., Plaintiff McGee and Imagine360 Pennsylvania Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Plaintiff McGee and Imagine360 Pennsylvania Class members are also entitled to recover all available statutory, exemplary, treble, and/or punitive damages, costs of suit, and attorneys' fees based on the amount of time reasonable expended and equitable relief necessary, and all such other relief as the Court deems proper.

CLAIMS AGAINST INTELLIHARTX ONLY

COUNT XIX
VIOLATIONS OF THE ARIZONA CONSUMER FRAUD ACT
A.R.S. §§ 44-1521 et seq.
(Against ITx on Behalf of the ITx Arizona Class)

536. The ITx Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

537. Plaintiff Jose Cabrales ("Plaintiff" for the purposes of this Count) brings this Count on his own behalf and on behalf of the ITx Arizona Class.

538. ITx is a "person" as defined by A.R.S. §44-1521(6).

539. ITx sold Plaintiff and ITx Arizona Class Members "merchandise" as defined by A.R.S. § 44-1521, in the form of services in connection with the revenue services ITx provided to Plaintiff's and ITx Arizona Class Members' healthcare providers.

540. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

A.R.S. § 44-1522(A).

541. ITx used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. § 44-1522(A).

542. ITx omitted and concealed material facts, which it knew about and had the duty to disclose—namely, ITx's failure to ensure Fortra provided adequate security protections for Plaintiff's and ITx Arizona Class Members' PII/PHI.

543. This omission was designed to mislead consumers, including Plaintiff and ITx Arizona Class Members.

544. ITx omitted and concealed those material facts even though in equity and good conscience those facts should have been disclosed and did so with the intent that others would rely on the omission, suppression, and concealment.

545. Upon information and belief, ITx intentionally omitted and concealed material facts—like its failure to ensure Fortra maintained adequate cyber and data privacy and security protections—with the intention that consumers rely on those omissions.

546. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

547. Plaintiff and ITx Arizona Class Members were ignorant of the truth and relied on the concealed facts in providing PII/PHI to ITx and incurred damages as a consequence and proximate result.

548. But for ITx's omissions, the damage to Plaintiff and ITx Arizona Class Members would not have occurred.

549. ITx knew or should have known that Fortra's computer system and data security practices were inadequate to safeguard Plaintiff's and ITx Arizona Class Members' PII/PHI, and that the risk of a data breach or theft was highly likely. ITx failed to ensure Fortra had such measures in place. ITx's actions in engaging in these deceptive acts and practices were intentional, knowing, willful, wanton, and reckless with respect to the rights of Plaintiff and ITx Arizona Class Members.

550. Specifically, ITx failed to comply with the standards outlined by the FTC Act. ITx was or should have been aware of these standards. ITx's oversight measures pertaining to its vendors, including Fortra, did not follow the FTC's guidelines, and thus, ITx failed to guarantee Fortra's systems operated at the minimum standards required.

551. Plaintiff and ITx Arizona Class Members were ignorant of the truth and relied on the concealed facts in providing their PII/PHI and incurred damages as a consequent and proximate result.

552. Plaintiff and Class Members seek all available relief under A.R.S. §§ 44- 1521 et seq., including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT XX
VIOLATIONS OF THE MISSOURI MERCHANDISING PRACTICES ACT ("MMPA")
Mo. Rev. Stat. § 407
(Against ITx on Behalf of the ITx Missouri Class)

553. The ITx Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

554. Plaintiffs Victoria Evans, Nicholas Timmons, and Robert Terwilliger ("Plaintiffs" for the purposes of this Count) bring this Count on their own behalf and on behalf of the ITx Missouri Class.

555. ITx is a "person" within the meaning of the MMPA (Mo. Rev. Stat. §407.010(5)).

556. ITx engaged in a "trade" or "commerce" within the meaning of the MMPA with regard to the advertisement and offers of sales for services which are supposed to keep Plaintiffs' and the ITx Missouri Class Members' PII/PHI safe and secure.

557. ITx engaged in unlawful practices and deceptive conduct during its business that violated the MMPA including omissions related its failure to guarantee its vendors, including

Fortra, maintained adequate data security safeguards to protect Plaintiffs' and ITx Missouri Class Members' PII/PHI, all in violation of Mo. Rev. Stat. §407.020.1.

558. By the acts and conduct alleged herein, ITx committed unfair or deceptive acts and practices. These acts and conduct include, but are not limited to, ITx's omissions that it failed to ensure its vendors maintained adequate security measures to protect and keep Plaintiffs' and ITx Missouri Class Members' PII/PHI safe.

559. ITx's unlawful conduct also included omitting material facts, such as failing to disclose:

a. ITx failed to guarantee Fortra maintained adequate data security systems, practices, and protocols to prevent data loss;

b. ITx's failure to mitigate the risks of a data breach and loss of data by neglecting to ensure Fortra was capable of safeguarding data;

c. ITx's failure to ensure Fortra implemented policies and procedures to prevent, detect, contain, and correct security violations; and

d. ITx's failure to ensure Fortra was capable of protecting against any reasonably-anticipated threats or hazards to the security or integrity of electronic PII/PHI.

560. ITx's omissions were material to Plaintiffs and ITx Missouri Class Members and were omitted in order to induce consumers' reliance regarding the safety and security of their PII/PHI in their receipt of healthcare services.

561. ITx's deceptive practices misled the Plaintiffs and ITx Missouri Class Members and would cause a reasonable person to enter into the transactions that resulted in damages and did in fact cause reasonable persons to enter into the transactions.

562. As a direct and proximate cause of ITx's deceptive practices and unlawful conduct, the Plaintiffs and ITx Missouri Class Members have suffered, and continue to suffer, an ascertainable loss of money and economic injuries.

563. For violations of the MMPA, Plaintiffs on behalf of themselves and the members of the ITx Missouri Class seek to recover actual damages sustained; punitive damages; reasonable attorneys' fees and costs; and any other relief to which they are entitled.

COUNT XXI
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. Ann. § 56:8-1 *et seq.* ("NJ CFA")
(Against ITx on Behalf of the ITx New Jersey Class)

564. The ITx Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

565. ITx Plaintiff Lauren Perrone ("Plaintiff" for purposes of this Count) brings this Count on her own behalf and on behalf of the ITx New Jersey Class.

566. ITx is a "person" within the meaning of N.J. Stat. Ann. § 56:8-1(d).

567. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1 et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

568. ITx's unconscionable and deceptive practices include:

a. Failing to ensure Fortra implemented adequate data security and privacy measures to protect Plaintiff's and ITx New Jersey Class Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to ensure Fortra was capable of identifying and remediating foreseeable security and privacy risks despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and ITx New Jersey Class Members' PII/PHI, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately guarantee the security of Plaintiff's and ITx New Jersey Class Members' PII/PHI, especially when ITx utilized Fortra's file transfer and data storage services; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Class Members' PII/PHI, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

569. ITx's omissions were material because they were likely to deceive reasonable consumers about ITx's commitment to guarantee the adequacy of its vendor's, such as Fortra, data security.

570. ITx's omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the ITx New Jersey Class Members, that their PII/PHI would not be expo

571. and misled Plaintiff and the ITx New Jersey Class Members into believing they did not need to take actions to secure their identities.

572. ITx intended to mislead Plaintiff and the ITx New Jersey Class Members and induce them to rely on their omissions.

573. ITx acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff's and the ITx New Jersey Class Members' rights.

574. As a direct and proximate result of ITx's unconscionable and deceptive practices, Plaintiff's and the New Jersey Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; the expense of purchasing multi-year identify theft protection; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

575. Plaintiff and the ITx New Jersey Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

COUNT XXII
VIOLATION OF THE OHIO DECEPTIVE TRADE PRACTICES ACT
Ohio Rev. Code §§ 4165.01 et seq.
(Against ITx on Behalf of the ITx Ohio Class)

576. The ITx Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1-360 above as if fully set forth herein.

577. Plaintiffs Thomas Kelly and Kristi McDavitt ("Plaintiffs" for the purposes of this Count) bring this Count on their own behalf and on behalf of the ITx Ohio Class.

578. ITx, Plaintiffs, and ITx Ohio Class Members are a "person" under Ohio Rev. Code § 4165.01(D).

579. ITx advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

580. ITx engaged in deceptive trade practices by, inter alia, failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act, soliciting and collecting Plaintiffs' and Ohio Class Members' PII/PHI with knowledge that its file transfer and data storage vendor, Fortra, stored Plaintiffs' and Ohio Class Members' PII/PHI in an unsecure electronic environment, failing to take proper oversight measures to ensure Fortra maintained adequate data security, and failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Ohio Class's PII/PHI and other personal information from further unauthorized disclosure, release, and data breaches.

581. The foregoing practices violated Ohio Rev. Code § 4165.02.

582. ITx acted intentionally, knowingly, and maliciously in violating the Act and recklessly disregarded Plaintiffs and Ohio Class Members' rights. ITx knew or should have known of the security deficiencies in Fortra's data systems. Consumers, including Plaintiffs and Ohio Class Members, lacked this knowledge and consumers lack expertise in information security. Even if they did have this expertise, consumers do not have access to Fortra's data systems or the opportunity to ensure ITx guaranteed the security of their PII/PHI.

583. As a direct and proximate result of ITx's deceptive trade practices, Plaintiffs and Ohio Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity

theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

584. Plaintiffs and Ohio Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs, and any other relief that is just and proper.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against each of the Track 4 Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing yet another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Consolidated Class Action Complaint so triable.

Dated: April 18, 2024

Respectfully submitted,

By: *Jeff Ostrow*

Jeff Ostrow FBN 121452
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 332-4200
ostrow@kolawyers.com

MORGAN & MORGAN COMPLEX LITIGATION GROUP
John Allen Yanchunis FBN 324681
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 275-5272
jyanchunis@forthepeople.com

MDL Co-Lead Counsel for Plaintiffs

CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & AGNELLO, P.C.
James E. Cecchi (*pro hac vice*)
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
jcecchi@carellabyrne.com

MDL Track Coordination and Settlement Counsel for Plaintiffs

SIRI & GLIMSTAD LLP
Mason A Barney
745 Fifth Ave., Suite 500
New York, NY 10151

Telephone: (212) 532-1091
mbarney@sirillp.com

SHUB & JOHNS LLC
Benjamin F. Johns (*pro hac vice*)
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
bjohns@shublawyers.com

FEDERMAN & SHERWOOD
William B. Federman
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
P: 405-235-1560
F: 405-239-2112
wbf@federmanlaw.com

LYNCH CARPENTER, LLP
Nicholas A. Colella
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
412-322-9243
nickc@lcllp.com

Plaintiffs' Track Four Leads

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing has been served via the CM/ECF system on all counsel of record on this 18th day of April, 2024.

*/s/ Jeff Ostrow*_____
Jeff Ostrow

ClassAction.org
