IN THE CIRCUIT COURT OF THE FIRST JUDICIAL CIRCUIT IN AND FOR OKALOOSA COUNTY, FLORIDA

IN RE: BRIDGEWAY CENTER
CYBER INCIDENT LITIGATION

Lead Case No.: 2024-CA-1395

JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Jeff Beaver, Justin Beck, Jennifer Nelson and Kimberly Davidson (collectively "Plaintiffs"), individually, and on behalf of all other similarly situated individuals ("Class Members" further defined below), file this Consolidated Class Action Complaint against Bridgeway Center, Inc. ("Defendant") and allege the following:

I. NATURE OF THE ACTION

1. Defendant provides mental health services. Defendant operates in multiple locations in Okaloosa County, Florida.

2. Plaintiffs and Class Members are individuals who entrusted Defendant with their personally identifiable information ("PII") and protected health information ("PHI") (collectively "Private Information") for the purpose of obtaining mental health services.

3. Plaintiffs and Class Members provided their Private Information to Defendant with the expectation that it would be kept confidential and secure. The reasonable expectation of Plaintiffs and Class Members turned out to be wrong.

4. Defendant betrayed Plaintiffs' trust and that of the other Class Members by failing to properly safeguard and protect their Private Information and thereby enabling cybercriminals to steal their Private Information.

5. This class action seeks to redress Defendant's unlawful, willful, and wanton failure to protect the Private Information of 65,386 individuals that was disclosed in a data breach that was discovered in February 2024 ("Data Breach"), in violation of its legal obligations, including obligations under the Health Insurance Portability and Accountability Act.[1]

6. The Data Breach occurred as a result of unauthorized third-party actors who were able to infiltrate Defendant's inadequately secured system and gain access to Defendant's network between February 21, 2024, through February 23, 2024.[2]

7. The Private Information exposed to cybercriminals included individuals' names; Social Security numbers, driver license numbers, military identification numbers, date of birth, therapist/doctor notes, mental or physical condition/treatment, diagnosis information, medical procedure information, dates of service, medical record number, sickness certificate, and prescription information.[3]

8. Due to Defendant's negligence, cybercriminals obtained everything they needed to commit identity theft and wreak havoc on the financial and personal lives of tens of thousands of individuals.

9. For the rest of their lives, Plaintiffs and Class Members will have to deal with the danger of identity thieves possessing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/acc276d1-ebb6-412e-9848-0cf2b0c82249.shtml.

[2] *Id*.

[3] *Id*.

the Data Breach. Plaintiffs and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

10. Plaintiffs bring this action individually and on behalf of the a class of individuals, seeking compensatory damages, statutory damages, punitive damages, restitution, injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

Plaintiffs

11. Plaintiff, Jeff Beaver, is domiciled in and is a citizen of Crestview, Florida. Plaintiff received notification from Defendant that his Private Information was exposed in the Data Breach.

12. Plaintiff, Justin Beck, is domiciled in and is a citizen of Okaloosa, Florida. Plaintiff received notification from Defendant that his Private Information was exposed in the Data Breach.

13. Plaintiff, Jennifer Nelson, is domiciled in and is a citizen of Crestview, Florida. Plaintiff received notification from Defendant that her Private Information was exposed in the Data Breach.

14. Plaintiff, Kimberly Davidson, is domiciled in and is a citizen of Okaloosa, Florida. Plaintiff received notification from Defendant that her Private Information was exposed in the Data Breach.

Defendant

15. Defendant provides mental health services. Defendant operates in multiple locations in Okaloosa County, Florida. Defendant's principal place of business is located at 205 Shell Avenue SE, Building A, Fort Walton Beach, Florida.

III. JURISDICTION AND VENUE

16. The Court has subject matter jurisdiction over this action seeking declaratory relief, injunctive relief, and damages in excess of $50,000.00 (exclusive of court costs, attorney's fees, and interest), pursuant to Article V, section 5(b), of the Florida Constitution and Florida Statutes §§ 26.012 and 86.011.

17. This Court has personal jurisdiction over the Defendant and over this action, pursuant to Florida Statutes §48.193. Defendant personally or through its agents operated, conducted, engaged in, or carried on a business or business venture in Fort Walton Beach, Florida; committed tortious acts in Florida; and engaged in significant business activity within Florida.

18. Venue is similarly proper in Okaloosa pursuant to section 47.011, Florida Statutes, for the reasons stated in the above paragraph.

IV. FACTUAL ALLEGATIONS

The Data Breach

19. On February 22, 2024, Defendant noticed suspicious activity on its network. A subsequent forensic investigation determined that unauthorized third-party actors had infiltrated Defendant's inadequately secured system and gained access to Defendant's network.[4] During this unauthorized infiltration, the unauthorized cybercriminals gained access to tens of thousands of patients' most sensitive Private Information, including their: names; Social Security numbers,

[4] *Id.*

driver license numbers, military identification numbers, date of births, therapist/doctor notes, mental or physical condition/treatment, diagnosis information, medical procedure information, dates of service, medical record number, sickness certificate, and prescription information.

20. Despite the breadth and sensitivity of the PII/PHI it collected, Defendant failed to properly secure the information in it collected and stored. As a result, it allowed unauthorized cybercriminals to access the Private Information of 65,386 patients.

21. Based on the notice letter received by Plaintiffs, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiffs' Private Information was stolen in the Data Breach.

22. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Private Information and has engaged in (and will continue to engage in) misuse of the Private Information, including marketing and selling Plaintiffs' and Class Members' Private Information on the dark web.

23. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiffs and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

24. Nevertheless, Defendant failed to spend sufficient resources on preventing external access, detecting outside infiltration, and training its employees to identify email-borne threats and defend against them.

25. Defendant was grossly negligent and disregarded the obvious and substantial risks of such an attack—an attack that was undetected for multiple months.

26. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' Private Information from unauthorized disclosure.

27. To make matters worse, even after discovering the Data Breach on February 22, 2024, it took several additional months for Defendant to notify the affected patients. Indeed, it was not until May 8, 2024, that Defendant began sending its belated notice to Plaintiffs and the Class.[5] Thus, in addition to failing to reasonably protect Plaintiffs and Class Members' Private Information, Defendant then failed to provide timely notice of the Data Breach to those individuals' whose highly sensitive Private Information was accessed by unauthorized cybercriminals.

28. Defendant's actions represent a flagrant disregard of its patients' rights, both as to privacy and property.

29. The stolen Private Information at issue has great value to the hackers, due to the large number of individuals affected and the fact the sensitive information that was part of the data that was compromised.

Plaintiffs' Experiences and Harms

Plaintiff Jeff Beaver

30. Plaintiff Beaver is a former patient of Bridgeway. She entrusted his Private Information to Bridgeway in exchange for medical services. Pursuant to HIPAA, Bridgeway was required to protect and maintain the confidentiality of Personal Information entrusted to it.

31. Plaintiff Beaver and Class Members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would

[5] *Id*.

comply with its obligations to keep such information confidential and secure from unauthorized access.

32. Plaintiff Beaver received a notice letter from Defendant dated May 8, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

33. Plaintiff Beaver is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

34. Plaintiff Beaver stores any documents containing his Private Information in a safe and secure location. Plaintiff Beaver has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

35. Because of the Data Breach, Plaintiff Beaver's Private Information is now in the hands of cyber criminals.

36. Plaintiff Beaver has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

37. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and protected health information, Plaintiff Beaver is now imminently at risk of crippling future identity theft and fraud.

38. Since the Data Breach, Plaintiff Beaver has experienced a large number of unsolicited calls and texts. These suspicious calls and texts began recently and have continued. Plaintiff Beaver attributes the foregoing fraudulent and suspicious activity to the Data Breach given the time proximity and the fact he has never experienced anything like this prior to now.

39. Approximately four months ago, Plaintiff Beaver was notified that his confidential information was on the Dark Web by Discover Bank.

40. As a result of the Data Breach, Plaintiff Beaver has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Beaver has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

41. The letter Plaintiff Beaver received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter advised Plaintiffs and all Class Members to take such protective steps, instructing them to, among other things, "remain vigilant against incidents of identity theft and fraud, to review account statements and to monitor your credit reports for suspicious or unauthorized activity."[6] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and frauds.[7] Accordingly, at Defendant's suggestion, Plaintiff Beaver is desperately trying to mitigate the damage that Defendant has caused him.

42. As a result of the Data Breach, Plaintiff Beaver has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and

[6] *See* Sample Breach letter, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/acc276d1-ebb6-412e-9848-0cf2b0c82249.shtml.
[7] *Id.*

misusing his Private Information. Plaintiff Beaver fears that criminals will use his information to commit identity theft.

43. Plaintiff Beaver anticipates spending considerable time and money on an ongoing basis.

44. Plaintiff Beaver has also suffered injury directly and proximately caused by the Data Breach, including, but not limited to: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Beaver's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Beaver's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Beaver's Private Information; and (e) continued risk to Plaintiff Beaver's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Justin Beck

45. Plaintiff Beck is a former patient of Bridgeway. He entrusted his Private Information to Bridgeway in exchange for medical services. Pursuant to HIPAA, Bridgeway was required to protect and maintain the confidentiality of Personal Information entrusted to it.

46. Plaintiff and Class Members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

47. Plaintiff Beck received a notice letter from Defendant dated May 8, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

48. Plaintiff Beck is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

49. Plaintiff Beck stores any documents containing his Private Information in a safe and secure location. Beck has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

50. Because of the Data Breach, Plaintiff Beck's Private Information is now in the hands of cyber criminals.

51. Plaintiff Beck has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

52. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and protected health information, Plaintiff Beck is now imminently at risk of crippling future identity theft and fraud.

53. Since the Data Breach, Plaintiff Beck became aware of fraudulent transactions on his bank account. These fraudulent transactions occurred in May 2024, on the same account and debit card that he used at Bridgeway. In addition, since the Data Breach, Plaintiff Beck has experienced a large number of calls advising him that he has been prequalified for various loans. These suspicious calls began in early March of 2024, and have continued since. Plaintiff Beck attributes the foregoing fraudulent and suspicious activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now, and, to his knowledge, his Private Information has never been exposed in any other Data Breach.

54. As a result of the Data Breach, Plaintiff Beck has had no choice but to spend numerous hours attempting to mitigate the harm caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Beck has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

55. The letter Plaintiff Beck received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter advised Plaintiff and all Class Members to take such protective steps, instructing them to, among other things, "remain vigilant against incidents of identity theft and fraud, to review account statements and to monitor your credit reports for suspicious or unauthorized activity."[8] In addition, the Data Breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and frauds.[9] Accordingly, at Defendant's suggestion, Plaintiff is desperately trying to mitigate the damage that Defendant has caused him.

56. As a result of the Data Breach, Plaintiff Beck has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and

[8] *See* Sample Breach letter, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/acc276d1-ebb6-412e-9848-0cf2b0c82249.shtml.
[9] *Id.*

misusing his Private Information. Plaintiff Beck fears that criminals will use his information to commit identity theft.

57. Plaintiff Beck anticipates spending considerable time and money on an ongoing basis.

58. Plaintiff Beck has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Beck's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Beck's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Beck's Private Information; and (e) continued risk to Plaintiff Beck's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Jennifer Nelson

59. Plaintiff Nelson is a former patient of Bridgeway. She entrusted her Private Information to Bridgeway in exchange for medical services. Pursuant to HIPAA, Bridgeway was required to protect and maintain the confidentiality of Personal Information entrusted to it.

60. Plaintiff Nelson and Class members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

61. Plaintiff Nelson received a notice letter from Defendant dated May 8, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

62. Plaintiff Nelson is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

63. Plaintiff Nelson stores any documents containing her Private Information in a safe and secure location. Plaintiff Nelson has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

64. Because of the Data Breach, Plaintiff Nelson's Private Information is now in the hands of cyber criminals.

65. Plaintiff Nelson has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

66. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and protected health information, Plaintiff Nelson is now imminently at risk of crippling future identity theft and fraud.

67. As a result of the Data Breach, Plaintiff Nelson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Nelson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

68. The letter Plaintiff Nelson received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter advised Plaintiffs and all Class Members to take such protective steps, instructing them to, among other things, "remain vigilant against incidents of identity theft and fraud, to review account statements and to monitor your credit reports for suspicious or unauthorized activity."[10] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and frauds.[11] Accordingly, at Defendant's suggestion, Plaintiff Nelson is desperately trying to mitigate the damage that Defendant has caused her.

69. As a result of the Data Breach, Plaintiff Nelson has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Nelson fears that criminals will use her information to commit identity theft.

70. Plaintiff Nelson anticipates spending considerable time and money on an ongoing basis.

71. Plaintiff Nelson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Nelson's Private

[10] *See* Sample Breach letter, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/acc276d1-ebb6-412e-9848-0cf2b0c82249.shtml.
[11] *Id.*

Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Nelson's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Nelson's Private Information; and (e) continued risk to Plaintiff Nelson's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Kimberly Davidson

72. Plaintiff Davidson is a former patient of Bridgeway. She entrusted her Private Information to Bridgeway in exchange for medical services. Pursuant to HIPAA, Bridgeway was required to protect and maintain the confidentiality of Personal Information entrusted to it.

73. Plaintiff Davidson and Class members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

74. Plaintiff Davidson received a notice letter from Defendant dated May 8, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

75. Plaintiff Davidson is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

76. Plaintiff Davidson stores any documents containing her Private Information in a safe and secure location. Plaintiff Davidson has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

77. Because of the Data Breach, Plaintiff Davidson's Private Information is now in the hands of cyber criminals.

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

79. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and protected health information, Plaintiff Davidson is now imminently at risk of crippling future identity theft and fraud.

80. As a result of the Data Breach, Plaintiff Davidson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Davidson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

81. The letter Plaintiff Davidson received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter advised Plaintiffs and all Class Members to take such protective steps, instructing them to, among other things, "remain vigilant against incidents of identity theft and fraud, to review account statements and to monitor

your credit reports for suspicious or unauthorized activity."[12] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and frauds.[13] Accordingly, at Defendant's suggestion, Plaintiff Davidson is desperately trying to mitigate the damage that Defendant has caused her.

82. As a result of the Data Breach, Plaintiff Davidson has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Davidson fears that criminals will use her information to commit identity theft.

83. Plaintiff Davidson anticipates spending considerable time and money on an ongoing basis.

84. Plaintiff Davidson has suffered actual injury in the form of a notification that her Private Information was leaked on the dark web.

85. Plaintiff Davidson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Davidson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Davidson's Private Information that was entrusted to Defendant; (d) damages

[12] *See* Sample Breach letter, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/acc276d1-ebb6-412e-9848-0cf2b0c82249.shtml.
[13] *Id.*

unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Davidson's Private Information; and (e) continued risk to Plaintiff Davidson's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

The Value of PHI and PII

86. Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

87. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[14]

88. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[23] For example, Private Information can be sold at a price ranging from $40 to $200.[24] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[25]

89. Theft of PHI is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

90. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[26]

91. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

92. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

93. This was a financially motivated Breach, as the reason the cyber criminals go through the trouble of running a targeted ransomware campaign against companies like Defendant is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. "[I]f there is reason to believe that your Private Information has been stolen, you should assume that it can end up for sale on the dark web."[15]

94. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to Private Information, they ***will*** use it.[16]

---

[15] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[16] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

95. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

96. Indeed, hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[17]

97. Identity theft victims must spend countless hours and large amounts of money repairing the impact of identity theft as well as protecting themselves in the future.[18]

98. While some harm has begun already, the full scope of the harm has yet to be realized.

99. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered actual identity theft, have been damaged, and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized

[17] *Data Breaches Are Frequent*, *supra* n.14.

[18] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

activity for years to come. Even more seriously is the identity restoration that individuals must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

100. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;
b. Trespass, damage to, and theft of their personal property including Private Information;
c. Improper disclosure of their Private Information;
d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;
e. Damages flowing from Defendant's untimely and inadequate notification of the data breach, including the uncertainty of whether they need to replace their driver's licenses;
f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves have already used that information to defraud other victims of the Data Breach;
g. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class members' Private Information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their Private Information; and

l. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

101. Defendant itself acknowledged the harm caused by the Data Breach because it instructed Plaintiffs and Class Members to "remain vigilant for suspicious activity and to regularly review your financial statements and credit reports."[19] The Notice further suggested that Plaintiffs and Class Members should, among other things, "remain vigilant with respect to reviewing your account statements and credit reports," to "[c]arefully review your credit reports and bank, credit card, and other account statements," to "[b]e proactive and create alerts on credit cards and bank accounts to notify you of activity," to "consider placing a fraud alert on your credit file," to "consider implementing a security freeze," and to "be on the lookout for suspicious emails, such as phishing schemes."[20] Thus, as seemingly acknowledged by Defendant, the twenty-four months of single-bureau credit monitoring is woefully inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk, including medical identity theft.

[19] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-361.pdf.

[20] *Id.*

102. At Defendant's suggestion, Plaintiffs and Class Members are desperately trying to mitigate the damage that Defendant has caused them. Given the kind of Private Information Defendant made accessible to cybercriminals, Plaintiffs and Class Members are certain to incur additional damages.

103. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' Private Information.

104. None of this should have happened.

Defendant was Aware of the Risk of Cyber-Attacks

105. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest data breaches: Target,[21] Yahoo,[22] Marriott International,[23] Chipotle, Chili's,

[21] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[22] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[23] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

Arby's,[24] and others.[25]

106. Data thieves regularly target healthcare entities like Defendant's due to the highly sensitive information that they collect and maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

107. Therefore, Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry, prior to Defendant's Data Breach, and Defendant's failures to adequately design, implement and monitor systems to protect the Private Information.

108. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

109. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in 2019 alone.

110. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida

[24] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[25] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

111. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[26] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[27] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

112. As a medical service provider, Defendant should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

113. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their

[26] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[27] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

accesses to obtain Private Information." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[28]

114. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[29]

115. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[30]

116. Defendant was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., 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 (Private Information)."[31]

---

[28] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[29] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360. arn-of-targeted-ransomware.

[30] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack

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

117. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive Private Information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive Private Information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[32]

Defendant Is Obligated Under HIPAA to Safeguard PHI

118. Defendant is required by the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1302d, *et seq*. ("HIPAA") to safeguard patient PHI. Under HIPAA health insurance providers have an affirmative duty to keep patients' PHI private.

119. Defendant is an entity covered by under HIPAA, which sets minimum federal standards for privacy and security of PHI. As a covered entity, Defendant has a statutory duty under HIPAA to safeguard Plaintiffs' and Class Members' PHI.

120. HIPAA establishes national standards for the protection of PHI. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. This includes compliance with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (Standards for Privacy of Individually Identifiable Health Information"), and the Security

[32] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

121. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

122. Under C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

123. HIPAA requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

124. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under C.F.R. § 164.306(e), and to "[i]implement technical policies and procedures for electronic information systems that maintain electronic protected

health information to allow access only to those persons or software programs that have been granted access rules." 45 C.F.R. § 164.312(a)(1).

125. Further, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[33]

126. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiffs or Class Members consent to the disclosure of their PHI to cybercriminals.

127. Accordingly, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

128. Given the application of HIPAA to Defendant, and that Plaintiffs and Class Members entrusted their PHI to Defendant for the purposes of receiving healthcare services, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

Defendant Could Have Prevented the Data Breach

129. Data breaches are preventable.[34] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have

[33] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, *Breach Notification Rule*, U.S. Dep't of Health & Human Services.

[34] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

been prevented by proper planning and the correct design and implementation of appropriate security solutions."[35] he added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[36]

130. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[37]

131. In a Data Breach like this, many failures laid the groundwork for the Breach.

132. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[38] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large

[35] *Id.* at 17.

[36] *Id.* at 28.

[37] *Id.*

[38] FTC, *Protecting Private Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

133. Upon information and belief, Defendant failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

134. Among other things, Defendant's protection software and endpoint detection were not sufficient to recognize, block, or detect the attack.

135. Defendant further had far too much confidential unencrypted information held on its systems.[39]

136. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed. The FTC, among others, has repeatedly emphasized the importance of disposing of unnecessary Private Information, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[40] Defendant, rather than following this basic standard of care, kept tens of thousands

[39] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[40] FTC, *Protecting Private Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf at p. 6.

of former patients' unencrypted Private Information on its network. This greatly expanded the number of victims harmed in the Breach.

V. CLASS ACTION ALLEGATIONS

137. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

138. Plaintiffs bring this action against Defendant on behalf of themselves and all other individuals similarly situated under Fla. R. Civ. P. 1.220. Plaintiffs assert all claims on behalf of a nationwide class ("Class") defined as follows:

> All persons whose Personal Information was compromised as a result of the Data Breach, including those who received notification letters from Defendant.

139. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

140. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

141. The proposed Class meets the requirements of Rule 1.220.

142. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals affected in the Data Breach amounts to more than 65,000 individuals.

143. **Ascertainability:** Members of the Class are readily identifiable from information in Defendant's possession, custody and control.

144. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of

every other Class member because Plaintiffs and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Defendant.

145. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

146. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

147. **Commonality and Predominance:** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over

any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

VI. CAUSES OF ACTION

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

148. Plaintiffs incorporate by reference paragraphs 1-147 as though fully alleged herein.

149. Defendant solicited, gathered, and stored the Private Information of Plaintiffs and the Class.

150. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and Class Members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

151. Defendant owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

152. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts, including those in Florida and the Eleventh Circuit, and legislatures, have recognized the existence of a specific duty owed by medical providers to reasonably safeguard the Private Information of their patients.

153. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to cyberattacks. Duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;
b. To protect the Private Information in its possession using reasonable and adequate security procedures and systems;
c. To adequately and properly audit, test, and train its employees to protect patient information;
d. To use adequate network security systems;
e. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;
f. To implement processes to quickly detect a data breach, security incident, or intrusion; and
g. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

154. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the Private Information that Plaintiffs and the Class had entrusted to it.

155. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

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

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to use adequate network security systems;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's Private Information;

f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

g. Failing to abide by reasonable retention and destruction policies for Private Information; and

h. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their Private Information, *see* Fla. Stat. § 501.171.

156. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

157. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

158. The damages Plaintiffs and the Class have suffered (as alleged above) were and are reasonably foreseeable.

159. The damages Plaintiffs and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

160. Plaintiffs and the Class have suffered injury, including as described *supra*, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

161. Plaintiffs incorporate by reference paragraphs 1-147 as though fully alleged herein.

162. Plaintiffs and Class Members were required to provide Defendant with their Private Information in order to receive medical care and treatment.

163. When Plaintiffs and Class Members provided their Private Information to Defendant when seeking medical services or employment, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Private Information and to timely notify them in the event of a Data Breach.

164. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and Class Members' Private Information, Defendant had an implied duty to safeguard their Private Information through the use of reasonable industry standards.

165. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant more than four months to warn Plaintiffs and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiffs and Class Members whether or not their driver's license numbers were compromised, leaving Plaintiffs and Class Members unsure as to the extent of the information that was compromised.

166. Plaintiffs and the Class have suffered injury, including as described *supra*, and are entitled to actual and punitive damages in an amount to be proven at trial, as well as an award of nominal damages.

167. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and Class Members' Private Information.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

168. Plaintiffs incorporate by reference paragraphs 1-147 as though fully alleged herein.

169. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

170. As a healthcare provider, and recipient of patients' Private Information, Defendant has a fiduciary relationship to its patients, including Plaintiffs and Class Members.

171. Because of that fiduciary relationship, Defendant was provided with and stored sensitive and valuable Private Information related to Plaintiffs and the Class. Plaintiffs and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

172. Defendant owed a fiduciary duty under common law to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

173. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiffs' and Class Members' medical records.

174. Defendant's patients, including Plaintiffs and Class Members, have a privacy interest in personal medical matters, and Defendant had a fiduciary duty not to disclose medical data concerning its patients.

175. As a result of the parties' relationship, Defendant had possession and knowledge of confidential Private Information of Plaintiffs and Class Members, information not generally known.

176. Plaintiffs and Class Members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

177. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information;
b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;
c. failing to design and implement information safeguards to control these risks;
d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;
e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its patients; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive Private Information.

178. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

179. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including: (i) theft of their Private Information; (ii) costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information; (iii) costs associated with purchasing credit monitoring and identity theft protection services; (iv) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach; (v) the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; (vi) damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and (vii) emotional distress from the unauthorized disclosure of Private Information to cybercriminal who likely have nefarious intentions, who have opportunities to commit identity theft or fraud, and who may sell their Private Information to additional unauthorized criminals.

180. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

181. Plaintiffs incorporate by reference paragraphs 1-147 as though fully alleged herein.

182. Plaintiffs and Class Members conferred a monetary benefit to Defendant when they provided their Private Information and payment to their healthcare or insurance providers, who in turn used a portion of the payment to engage Defendant's services, including Defendant's guardianship of the Private Information.

183. Defendant knew that Plaintiffs and Class Members conferred a monetary benefit to Defendant when it accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of Private Information to Defendant from Plaintiffs' and Class Members' healthcare or insurance providers is an integral part of Defendant's business. Without collecting and maintaining Plaintiffs and Class Members' Private Information, Defendant would have dramatically diminished business and profits.

184. Defendant was supposed to use some of the monetary benefit provided to it from Plaintiffs and Class Members to secure the Private Information belonging to Plaintiffs and Class Members by paying for costs of adequate data management and security.

185. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiffs and Class Members because Defendant failed to implement necessary security measures to protect the Private Information of Plaintiffs and Class Members.

186. Defendant gained access to the Plaintiffs' and Class Members' Private Information through inequitable means because Defendant failed to disclose that it used inadequate security measures.

187. Plaintiffs and Class Members were unaware of the inadequate security measures and would not have entrusted their Private Information to Defendant had they known of the inadequate security measures.

188. To the extent that this cause of action is pled in the alternative to the others, Plaintiffs and Class Members have no adequate remedy at law.

189. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

190. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

191. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds from the monetary benefit that it unjustly received from them.

FIFTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of Plaintiffs and the Class)

192. Plaintiffs incorporate by reference paragraphs 1-147 as though fully alleged herein.

193. This count is brought under Section 86, Florida Statutes.

194. As previously alleged and pleaded, Defendant owes duties of care to Plaintiffs and Class Members that requires it to adequately secure their Private Information.

195. Defendant still possesses the Private Information of Plaintiffs and Class Members.

196. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members.

197. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis,

and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

e. Ordering that Defendant's segment Plaintiffs' and the Class's Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

f. Ordering that Defendant cease transmitting Private Information via unencrypted email;

g. Ordering that Defendant cease storing Private Information in email accounts;

h. Ordering that Defendant conduct regular database scanning and securing checks;

i. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

j. Ordering Defendant to implement and enforce adequate retention policies for Private Information, including destroying, in a reasonably secure manner, Private Information once it is no longer necessary for the it to be retained; and

k. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and Private Information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, nominal damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

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

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

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

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

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: July 30, 2024

Respectfully submitted,

/s/ *Jeff Ostrow*
Jeff Ostrow (FBN 121452)
Kristen Lake Cardoso (FBN 44401)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: 954-525-4100
ostrow@kolawyers.com
cardoso@kolawyers.com

Mariya Weekes (FBN 56299)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: 786.879.8200

mweekes@milberg.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Tel: 405.389.4989
abm@murphylegalfirm.com

Counsel for Plaintiffs and the Putative Class

**Pro Hac Vice* application to be submitted