STATE OF WISCONSIN **CIRCUIT COURT** **DANE COUNTY**

KELLY GORDER, EMILY DEANN HARBISON, MICHAEL WEBSTER, CHRISTANTHI OPITZ, ON BEHALF OF D.T., A MINOR, TAYLOR NICOLE ZURFLUH-TAYLOR, JILLIAN ZACHAR, BONNIE HELD, CARESSA BRADENBURG, MARIANNE FROM, ANGELIQUE SKIPPER, and RUSSELL FROM, on behalf of himself and minors M.F. and O.F., individually, and on behalf of all others similarly situated, Plaintiffs, v. FCDG MANAGEMENT, LLC d/b/a FIRST CHOICE DENTAL, Defendant.	Case No.: 2024CV002164

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Kelly Gorder, Emily Deann Harbison, Michael Webster, Christanthi Opitz, on behalf of D.T., a minor, Taylor Nicole Zurfluh-Taylor, Jillian Zachar, Bonnie Held, Caressa Bradenburg, Marianne From, Angelique Skipper, and Russell From, on behalf of himself and minors M.F. and O.F. (collectively, "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against Defendant FCDG Management, LLC d/b/a First Choice Dental ("First Choice" or "FCD" or "Defendant"). Plaintiffs bring this action by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief and reasonable investigation by their counsel as to all other matters, as follows:

INTRODUCTION

1. First Choice is a group of twelve dental clinics providing comprehensive dental care across Dane County.[1]

2. As part of its operations, First Choice collects, maintains, and stores its patients' and members' personally identifiable information ("PII") and protected health information ("PHI" and collectively with PII, "Private Information").[2]

3. On October 22, 2023, First Choice experienced a data breach (the "Data Breach") when it "detected a ransomware event on its network, whereby an unauthorized actor gained access to FCD's network, encrypted some of FCD's data, and attempted to extort a ransom payment."[3]

4. Worryingly, First Choice already admitted that cybercriminals compromised its patients' and members' PII and PHI—including their names, dates of birth, Social Security numbers, passport numbers, driver's license numbers, government identification numbers, credit card numbers, debit card numbers, and health information (all together "PII/PHI" or "Private Information").[4]

5. On July 12, 2024, First Choice mailed a notice to individuals whose information was accessed in the Data Breach.[5]

6. Because First Choice stored and handled Plaintiffs' and Class members' highly sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

---

[1] *About Us,* FIRST CHOICE DENTAL, https://firstchoicedental.com/about/about-us/ (last visited Nov. 14, 2024).

[2] *First Choice Dental Cyber Security Update*, FIRST CHOICE DENTAL (July 12, 2024) https://firstchoicedental.com/blog/first-choice-dental-cyber-security-update/.

[3] *Id.*

[4] *Id.*

[5] *Id.*

7. Ultimately, First Choice failed to fulfill this obligation, as unauthorized cybercriminals breached First Choice's information systems and databases and stole vast quantities of Private Information belonging to First Choice's patients, including Plaintiffs and Class members. The Data Breach—and the successful exfiltration of Private Information—were the direct, proximate, and foreseeable results of multiple failings on the part of First Choice.

8. The Data Breach occurred because First Choice failed to implement reasonable security protections to safeguard its information systems and databases. Thereafter, First Choice failed to timely detect this Data Breach. Moreover, before the Data Breach occurred, First Choice failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been made aware of this fact, they would never have provided their sensitive information to First Choice.

9. First Choice's subsequent handling of the breach was also deficient, for several reasons.

10. First Choice's attempt to ameliorate the effects of this Data Breach with one year of credit monitoring is inadequate. Much of the Private Information that was stolen is immutable and one year of credit monitoring is nothing in the face of a life-long heightened risk of identity theft. First Choice took six months to complete its investigation of the Data Breach, and it took FCS ***almost nine months*** to begin notifying victims that their Private Information was stolen in the Data Breach.

11. As a result of First Choice's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs and Class members suffered injuries, but not limited to:

a. Lost or diminished value of their Private Information;

b. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

c. Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;

d. Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;

e. Charges and fees associated with fraudulent charges on their accounts; and

f. The continued and increased risk of compromise to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

12. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard Plaintiffs' and Class members' Private Information; its failure to reasonably provide timely notification to Plaintiffs and Class members that their Private Information had been compromised; and for Defendant's failure to inform Plaintiffs and Class members concerning the status, safety, location, access, and protection of their Private Information.

PARTIES

Plaintiff Kelly Gorder

13. Plaintiff Kelly Gorder is and at all relevant times hereto has been a citizen of Boulder, Colorado. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

14. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

15. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI.

16. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft or fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

17. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Emily Deann Harbison

18. Plaintiff Emily Deann Harbison is and at all relevant times hereto has been a citizen of Milton, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

19. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

20. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI.

21. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft or fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

22. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Michael Webster

23. Plaintiff Webster is and at all relevant times hereto has been a citizen of Madison, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

24. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard his PII/PHI including monitoring his PII/PHI closely. He has not knowingly transmitted his PII/PHI over unsecured or unencrypted internet connections.

25. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of his PII/PHI.

26. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

27. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Christanthi Opitz, on behalf of D.T., a minor

28. Plaintiff D.T. is and at all relevant times hereto has been a resident and citizen of Madison, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

29. Prior to this Data Breach, Plaintiff and D.T. had taken steps to protect and safeguard D.T.'s PII/PHI including monitoring D.T.'s PII/PHI closely. Plaintiff and D.T. have not knowingly transmitted D.T.'s PII/PHI over unsecured or unencrypted internet connections.

30. D.T. has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the

information that was targeted and stolen in the Data Breach. D.T. has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of D.T.'s PII/PHI.

31. Since learning about the breach, D.T. has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

32. D.T. will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Taylor Nicole Zurfluh-Taylor

33. Plaintiff Taylor Nicole Zurfluh-Taylor is and at all relevant times hereto has been a citizen of Waunakee, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

34. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

35. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI.

36. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft or fraud, to

review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

37. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Jillian Zachar

38. Plaintiff Jillian Zachar is a citizen and resident of Dane County, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

39. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

40. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI.

41. Since learning about the breach, Plaintiff has taken *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, including investigating the Data Breach, thoroughly reviewing financial statements and other personal information, continually monitoring her account activity, and taking other steps in an attempt to preemptively detect and deter actual instances of identity theft or fraud.

42. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Bonnie Held

43. Plaintiff Bonnie Held is and at all relevant times hereto has been a citizen of Madison, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

44. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

45. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI.

46. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

47. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Caressa Bradenburg

48. Plaintiff Caressa Bradenburg is and at all relevant times hereto has been a citizen of Arena, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

49. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

50. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI.

51. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

52. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Russell From

53. Plaintiff Russell From is and at all relevant times hereto has been a citizen of Middleton Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 22, 2024, from Defendant.

54. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard his PII/PHI including monitoring his PII/PHI closely. He has not knowingly transmitted his PII/PHI over unsecured or unencrypted internet connections.

55. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the

information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of his PII/PHI.

56. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

57. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Marianne From

58. Plaintiff Marianne From is and at all relevant times hereto has been a citizen of Middleton, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 22, 2024, from Defendant.

59. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

60. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI.

61. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to

review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

62. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Angelique Skipper

63. Plaintiff Angelique Skipper is and at all relevant times hereto has been a citizen of Middleton, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 16, 2024, from Defendant.

64. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

65. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI.

66. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

67. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Russell From on behalf of M.F., a minor

68. Plaintiff Russell From and M.F. are and at all relevant times hereto have been citizens of Middleton, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 20, 2024, from Defendant.

69. Prior to this Data Breach, Plaintiff has taken steps to protect and safeguard M.F.'s PII/PHI including monitoring M.F.'s PII/PHI closely. Plaintiff has not knowingly transmitted M.F.'s PII/PHI over unsecured or unencrypted internet connections.

70. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff and/or his guardians have suffered and continue to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of M.F.'s PII/PHI.

71. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

72. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Plaintiff Russell From on behalf of O.F., a minor

73. Plaintiff Russell From and O.F. are and at all relevant times hereto have been citizens of Middleton, Wisconsin. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about July 20, 2024, from Defendant.

74. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard O.F.'s PII/PHI including monitoring O.F.'s PII/PHI closely. Plaintiff has not knowingly transmitted O.F.'s PII/PHI over unsecured or unencrypted internet connections.

75. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Plaintiff and/or her guardians have suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of O.F.'s PII/PHI.

76. Since learning about the breach, Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud.

77. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

Defendant FCDG Management, LLC d/b/a First Choice Dental

78. Defendant FCDG Management LLC d/b/a/ First Choice Dental is a Wisconsin domestic limited liability company with its principal place of business located at 440 Science Drive, Suite 100 Madison, Wisconsin 53711. Defendant conducts business in Dane County and throughout Wisconsin.

JURISDICTION AND VENUE

79. This Court has jurisdiction over Defendant because it is a resident and citizen of the State of Wisconsin and has its principal place of business in Dane County.

80. Venue is proper in this Court pursuant to Wis. Stat. § 801.50(2) because Defendant resides in this County, and a substantial part of the events or omissions giving rise to Plaintiffs' and Class members' claims occurred in Dane County.

FACTUAL ALLEGATIONS

A. First Choice – Background

81. First Choice constitutes fourteen dental clinics across Dane County. [6] As part of its normal operations, First Choice collects, maintains, and stores large volumes of Private Information belonging to its current and former patients and members.

82. First Choice failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information of First Choice's current and former patients—Plaintiffs and Class members.

83. Current and former patients of First Choice, such as Plaintiffs and Class members, made their Private Information available to First Choice with the reasonable expectation that First Choice would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

84. This expectation was objectively reasonable and based on an obligation imposed on First Choice by statute, regulations, industry standards and customs, and standards of general due care.

85. Unfortunately for Plaintiffs and Class members, First Choice failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it

[6] *Locations,* FIRST CHOICE DENTAL, https://firstchoicedental.com/locations/ (last visited Nov. 14, 2024).

failed to protect Plaintiffs and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

86. According to its public statements, unauthorized individuals breached First Choice's information systems at some undisclosed time prior to October 22, 2023.[7] The cybercriminals engaged in a ransomware attack, encrypting some of First Choice's data, and demanded a ransom from First Choice.[8]

87. First Choice posted a notice of the Data Breach on its website on December 21, 2023, and issued a notice through the Wisconsin State Journal.[9]

88. Sometime in May 2024, First Choice purportedly completed its review of the Data Breach.[10]

89. On July 12, 2024, First Choice issued notice of the Data Breach to all affected individuals—Plaintiffs and Class members.[11]

90. Omitted from the notice were the date that the cybercriminal first gained access to First Choice's data systems, how long the cybercriminals had access to patient data, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again.[12] To date, these critical facts have not

---

[7] *First Choice Dental Cyber Security Update*, FIRST CHOICE DENTAL (July 12, 2024) https://firstchoicedental.com/blog/first-choice-dental-cyber-security-update/.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *See id.*

been explained or clarified to Plaintiffs and Class members, who retain a vested interest in ensuring that their Private Information remains protected.

91. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

92. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

93. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully encrypted data.[13]

94. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[14]

95. Thus, on information and belief, Plaintiffs' and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

---

[13] *Id*.

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

96. First Choice estimates that the Private Information belonging to at least 227,287 individuals had their Private Information compromised in the Data Breach.[15]

C. First Choice's Many Failures Both Prior to and Following the Breach

97. Defendant collects and maintains vast quantities of Private Information belonging to Plaintiffs and Class members as part of its normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

98. Defendant inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

99. Defendant also failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been aware that Defendant did not have adequate safeguards in place to protect such sensitive Private Information, they would never have provided such information to Defendant.

100. In addition to the failures that led to the successful Breach, Defendant's failings in handling the Breach and responding thereto exacerbated the resulting harm to the Plaintiffs and Class members.

101. Defendant's delay in informing victims of the Data Breach that their Private Information was compromised virtually ensured that the cybercriminals who stole this Private Information could monetize, misuse and/or disseminate that Private Information before the Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

[15] *Data Breach Notifications*, MAINE ATTY GEN, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/223c815b-8525-491d-ab29-41d003ecfe00.html (last visited Nov. 14, 2024).

102. Additionally, First Choice's attempt to ameliorate the effects of this data breach with limited complimentary credit monitoring is woefully inadequate. Plaintiffs' and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, cause irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data, is immutable.

103. In short, Defendant's myriad failures allowed unauthorized individuals to access, misappropriate, and misuse Plaintiffs' and Class members' Private Information.

D. Data Breaches Pose Significant Threats

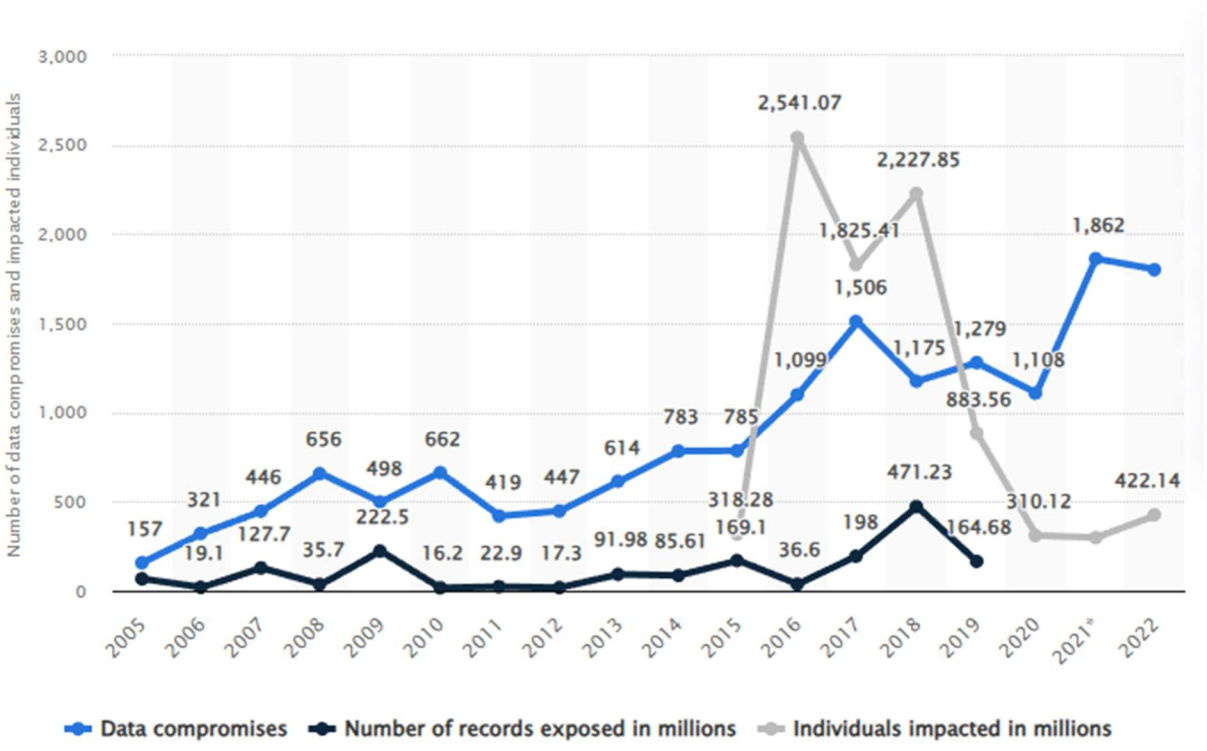
104. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII is an invaluable commodity and a frequent target of hackers.

105. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[16] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just 8 shy of the

[16] *2022 End of Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 25, 2023), https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.

record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.[17]

106. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[18] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[19]



[17] *2022 Healthcare Data Breach Report*, THE HIPAA JOURNAL (Jan. 24, 2023) https://www.hipaajournal.com/2022-healthcare-data-breach-report/.
[18] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
[19] *Id.*

107. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with social security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[20]

108. The severity of the consequences of compromised Private Information belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory groups can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[21]

109. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[22] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and Social Security numbers, which can be changed, medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[23] With this bounty of ill-gotten information,

---

[20] *What is your identity worth on the dark web?* CYBERNEWS (Sept. 28, 2021) https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

[21] *Identity Theft and Your Social Security Number*, UNITED STATES SOCIAL SECURITY ADMINISTRATION (July 2021) https://www.ssa.gov/pubs/EN-05-10064.pdf.

[22] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, FIERCE HEALTHCARE (Jan. 26, 2021) https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

[23] *Id.*

cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[24] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[25] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[26]

110. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[27] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[28]

111. Instances of Medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[29]

112. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendant charged with maintaining and

[24] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (Mar. 15, 2021) https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare; *see also* Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS (Aug. 25, 2016) https://www.consumerreports.org/health/medical-identity-theft-a1699327549/.
[25] *Id.*
[26] *Id.*
[27] *Medical Identity Theft*, AARP (Mar. 25, 2022) https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[28] *Id.*
[29] *Id.*

securing patient PII should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendant knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[30]

113. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard customer and patient information.[31]

114. Given the nature of Defendant's Data Breach, as well as the potential length of the time Defendant's networks were breached and the long delay in notification to victims thereof, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class members' Private Information can easily obtain Plaintiffs' and Class members' tax returns, open fraudulent credit card accounts in Class members' names, or perpetuate medical fraud under their names.

115. Based on the foregoing, the information compromised in the Data Breach is significantly because much of the information compromised in this Data Breach—such as names,

[30] Steve Alder, *Healthcare Data Breach Statistics*, HIPAA JOURNAL (Oct. 24, 2024) https://www.hipaajournal.com/healthcare-data-breach-statistics.
[31] *See, e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).

Social Security numbers, and medical information—is impossible to "close" and difficult, if not impossible, to change.

116. To date, Defendant has offered its consumers only limited identity theft monitoring services. The services offered are inadequate to protect Plaintiffs and Class members from the threats they will face for years to come, particularly in light of the Private Information at issue here.

117. Despite the prevalence of public announcements of data breach and data security compromises, FCD's own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from misappropriation. As a result, the injuries to Plaintiffs and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former patients.

E. First Choice Had a Duty and Obligation to Protect Private Information

118. Defendant has an obligation to protect the Private Information belonging to Plaintiffs and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. Third, Defendant imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiffs and Class members provided, and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violation

119. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq*.

120. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . ." 45 CFR § 164.402.

121. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires entities to provide notice of a data breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

122. Defendant failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiffs and Class members from unauthorized access and disclosure.

123. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to 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 rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, 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);

h. Failing 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);

i. Failing 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);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. 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.*

124. Upon information and belief, Defendant also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

2. FTC Act Requirements and Violations

125. The FTC has promulgated numerous guides for businesses that 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).

126. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[32] The guidelines note businesses should protect the personal information that they keep; 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 security problems.[33] The guidelines also recommend that businesses

[32] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMM'N (October 2016) https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[33] *Id.*

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 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.[34] Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

127. 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.

128. 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.

129. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

130. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

[34] *Id.*

131. Similarly, the Wisconsin data breach notification law, Wis. Stat. 134.98, obligates entities whose principal place of business is located in Wisconsin, or who maintain personal information concerning residents of Wisconsin, to provide notice to victims of unauthorized acquisition of personal information within 45 days of discovery of a data breach. Wis. Stat. 134.94(3).

132. Defendant was fully aware of its obligation to protect the Private Information of its current and former patients, including Plaintiffs and Class members. Defendant is a sophisticated and technologically savvy business that relies extensively on technology systems and networks to maintain its practice, including storing its patients' PII, protected health information, and medical information in order to operate its business.

133. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiffs and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiffs' and Class members' Private Information.

3. Industry Standards and Noncompliance

134. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

135. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and

Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[35]

136. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

137. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor

[35] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on Nov. 12, 2024).

authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[36]

138. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness.

139. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

4. First Choice's Privacy Policy and Promises To Maintain Privacy of Patients' PHI

140. Defendant publishes a "Privacy Policy" wherein Defendant promises that "First Choice Dental is committed to respecting your right to privacy" and that

[36] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Nov. 12, 2024).

"First Choice Dental does not disclose, give, sell or transfer any personal information . . . to third parties except as required by law."[37]

141. Additionally, Defendant publishes a "Notice of Privacy Practices" wherein Defendant promises that:

a. "This Notice describes how health information about you may be used and disclosed[.]"[38]

b. "The privacy of your health information is important to us."[39]

c. "We are required by applicable federal and state law to maintain the privacy of your health information."[40]

d. "We must follow the privacy practices that are described in the Notice while it is in effect. This Notice takes effect 04/14/2003 and will remain in effect until we replace it."[41]

e. "We support your right to the privacy of your health information."[42]

f. "Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this Notice."[43]

[37] *Privacy Policy,* FIRST CHOICE DENTAL, https://firstchoicedental.com/sitemap/privacy-policy/ (last visited Nov. 14, 2024).

[38] *Notice Of Privacy Practices*, FIRST CHOICE DENTAL (April 14, 2003) https://orthoii-forms.com/Custom/2675/HealthHistory/HIPAA.aspx?custid=2675.

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

142. Defendant failed to live up to its own stated policies and promises with regards to data privacy and data security as cybercriminals were able to infiltrate its systems and steal the Private Information belonging to Plaintiffs and Class members.

F. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

143. Like any data hack, the Data Breach presents major problems for all affected.[44]

144. The FTC warns the public to pay particular attention to how they keep personally identifying information. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[45]

145. The ramifications of Defendant's failure to properly secure Plaintiffs' and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

146. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

147. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

148. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing

[44] Paige Schaffer, *Data Breaches' Impact on Consumers*, INSURANCE THOUGHT LEADERSHIP (July 29, 2021) https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.
[45] *Warning Signs of Identity Theft*, FEDERAL TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Nov. 14, 2024).

increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal *Preventive Medicine Reports*, public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[46] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[47]

149. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

150. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[48] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[49]

151. The theft of medical information, beyond the theft of more traditional forms of PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.[50] Medical identity theft is especially

---

[46] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, PREVENTIVE MEDICINE REPORTS, Volume 17 (January 23, 2020), https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.
[47] *Id.*
[48] *Cost of a Data Breach Report 2023*, IBM SECURITY, https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.
[49] *Id.*
[50] *Medical Identity Theft*, AARP (March 25, 2022) https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[51]

152. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with one year of credit monitoring. However, this is inadequate to protect victims of the Data Breach from the lifelong risk of harm imposed on them by Defendant's failures.

153. Moreover, the credit monitoring offered by Defendant is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

154. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with time spent to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges,

[51] *Id.*

cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

155. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within the limited time of credit monitoring offered by Defendant.

156. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Private Information, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

157. Plaintiffs retain an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFFS

Plaintiff Kelly Gorder

158. Plaintiff entrusted her PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII or PHI.

159. Plaintiff would not have allowed Defendant to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her information.

160. Plaintiff has been forced to spend approximately five (5) hours dealing with and responding to the direct consequences of the Data Breach, which include monitoring her accounts for suspicious activity and changing her account passwords. This is uncompensated time that has been lost forever and cannot be recaptured. Today, she still spends approximately one (1) hour per week reviewing her accounts for suspicious activity as a result of the Data Breach.

161. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

162. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

163. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety

and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

164. Plaintiff has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

165. As a result of the Data Breach, Plaintiff experienced fraudulent charges on her credit card with American Express—which forced her to cancel her card and wait for a replacement several separate times.

166. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

167. Knowing that thieves stole her PII/PHI and knowing that her information is already on the dark web, has caused Plaintiff great anxiety.

168. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

169. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Emily Deann Harbison

170. Plaintiff entrusted her PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII or PHI.

171. Plaintiff would not have allowed Defendant to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her information.

172. Plaintiff has been forced to spend approximately two (2) hours dealing with and responding to the direct consequences of the Data Breach, which include researching the Data Breach, monitoring her accounts for suspicious activity, and changing the passwords on her accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

173. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

174. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

175. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety

and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

176. Plaintiff has suffered actual injury in the form of experiencing an increase in spam calls, which, upon information and belief, was caused by the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

177. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

178. Knowing that thieves stole her PII/PHI and knowing that her information will likely be sold on the dark web, has caused Plaintiff great anxiety.

179. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

180. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Michael Webster

181. Plaintiff entrusted his PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his PII or PHI.

182. Plaintiff would not have allowed Defendant to collect and maintain his PII/PHI had he known that Defendant would not take reasonable steps to safeguard his information.

183. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

184. Plaintiff stores all documents containing his PII/PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

185. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of his PII/PHI—a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

186. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

187. Plaintiff has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

This misuse of his PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

188. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII/PHI resulting from the compromise of his PII/PHI, especially his date of birth, in combination with his medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

189. Knowing that thieves stole his PII/PHI and knowing that his information will likely be sold on the dark web, has caused Plaintiff great anxiety.

190. Plaintiff has a continuing interest in ensuring that his PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

191. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Christanthi Opitz on behalf of D.T.

192. Plaintiff Christanthi Opitz entrusted D.T.'s PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that

information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to D.T.'s PII or PHI.

193. Plaintiff would not have allowed Defendant to collect and maintain D.T.'s PII/PHI had she known that Defendant would not take reasonable steps to safeguard D.T.'s information.

194. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring D.T.'s accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

195. Plaintiff stores all documents containing D.T.'s PII/PHI in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for the online accounts that D.T. has.

196. D.T. has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI—a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

197. Plaintiff has suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of D.T.'s privacy and the substantial risk of fraud and identity theft which D.T. now faces.

198. D.T. has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of D.T.'s PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources,

including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

199. As a result of the Data Breach, D.T. experienced multiple unauthorized transactions on D.T.'s payment card in late 2023, and again in mid-2024, requiring D.T. to obtain replacement cards on multiple instances.

200. D.T. has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

201. Knowing that thieves stole D.T.'s PII/PHI and knowing that D.T.'s information will likely be sold on the dark web, has caused D.T. great anxiety.

202. Plaintiff has a continuing interest in ensuring that D.T.'s PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

203. As a result of the Data Breach, D.T. is presently, and will continue to be, at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Zurfluh-Taylor

204. Plaintiff entrusted her PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-

standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII or PHI.

205. Plaintiff would not have allowed Defendant to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her information.

206. Plaintiff has been forced to spend approximately eight (8) hours dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, placing credit freezes on her credit with all three credit bureaus, self-monitoring her accounts, and changing passwords on her accounts. This is uncompensated time that has been lost forever and cannot be recaptured. Today, she still spends approximately thirty (30) minutes to one (1) hour per week reviewing her accounts for suspicious activity as a result of the Data Breach.

207. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

208. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

209. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

210. Plaintiff has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. To

make matters worse, many of these messages appear to be targeted phishing attempts. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

211. As a result of the Data Breach, Plaintiff also experienced fraudulent charges on a Chase credit card for several hundred dollars on or around February 16, 2024. During a call with Chase bank, Plaintiff confirmed that the charges were fraudulent. Notably, Chase bank was also the account that Plaintiff disclosed to Defendant. Given the fraudulent activity, Plaintiff was unable to use the credit card with Chase bank for approximately one week.

212. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

213. Knowing that thieves stole her PII/PHI and knowing that her information will likely be sold on the dark web, has caused Plaintiff great anxiety.

214. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

215. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Jillian Zachar

216. Plaintiff entrusted her PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII or PHI.

217. Plaintiff would not have allowed Defendant to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her information.

218. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include researching the Data Breach, thoroughly reviewing financial statements and other personal information, monitoring the activity and transactions in her accounts, and taking other steps in an attempt to mitigate the harms resulting from the Data Breach. This is uncompensated time that has been lost forever and cannot be recaptured.

219. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

220. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

221. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

222. Plaintiff has suffered actual injury in the form of experiencing an increase in spam calls and texts, which, upon information and belief, was caused by the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

223. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

224. Knowing that thieves stole her PII/PHI and knowing that her information will likely be sold on the dark web, has caused Plaintiff great anxiety.

225. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

226. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Bonnie Held

227. Plaintiff has been a patient of First Choice Dental for approximately the last 10 years.

228. Plaintiff entrusted her PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII or PHI.

229. Plaintiff would not have allowed Defendant to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her information.

230. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, reviewing dark web alerts, parsing through phishing emails, self-monitoring her financial accounts and reviewing her credit reports. This is uncompensated time that has been lost forever and cannot be recaptured.

231. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

232. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in and has been diminished as a result of the Data Breach.

233. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

234. Plaintiff has suffered actual injury in the form of experiencing an increase in spam and phishing calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach, and has experienced anxiety as a result of receipt of phishing emails and dark web alerts, which have increased in frequency since the Data Breach.

235. Further, Plaintiff's PII/PHI compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. Plaintiff has encountered alerts from various identity theft protection services notifying that her PII, such as her Social Security number and email address, were found on the Dark Web, which, upon information and belief, was caused by the Data Breach. Specifically, Plaintiff received a dark web alert from Discover Identity Theft Protection on October 31, 2024, informing her that her Social Security number was compromised. Additionally, Plaintiff has received multiple alerts from MyIDCare dating back to May 2024, and from Kroll Monitoring dating back to September 2024, notifying her that her PII was found on the Dark Web. Notably, Plaintiff only began receiving dark web alerts following the Data Breach.

236. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and

texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

237. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

238. Knowing that thieves stole her PII/PHI and knowing that her information is already on the dark web, has caused Plaintiff great anxiety.

239. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

240. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Caressa Brandenburg

241. Plaintiff entrusted her PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII or PHI.

242. Plaintiff would not have allowed Defendant to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her information.

243. Plaintiff has been forced to at least three hours dealing with and responding to the direct consequences of the Data Breach, which include spending time researching the Data Breach,

exploring credit monitoring and identity theft insurance options, changing passwords to all of her online accounts, and monitoring those accounts for unauthorized activity following the Data Breach. This is uncompensated time that has been lost forever and cannot be recaptured.

244. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

245. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

246. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

247. Plaintiff has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

248. As a result of the Data Breach, Plaintiff experienced fraudulent charges on her credit card and, in turn, had to replace her credit card.

249. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

250. Knowing that thieves stole her PII/PHI and knowing that her information will likely be sold on the dark web, has caused Plaintiff great anxiety.

251. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

252. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Russell From

253. Plaintiff Russell From is a patient of the Defendant who started to use Defendant's services in 2019.

254. As a condition of obtaining services from Defendant, he was required to provide his PII/PHI and other confidential information to Defendant.

255. Plaintiff entrusted his PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify his of any data security incidents related to his PII or PHI.

256. Plaintiff would not have allowed Defendant to collect and maintain his PII/PHI had he known that Defendant would not take reasonable steps to safeguard his information. On or about July 22, 2024, Plaintiff Russell From received notice from Defendant alerting him that his Private Information, including his date of birth, Social Security Number and PHI, had been accessed by cybercriminals during the Data Breach.

257. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

258. Plaintiff stores all documents containing his PII/PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

259. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of his PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

260. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

261. Plaintiff has suffered actual injury in the form of experiencing a dramatic increase in spam calls, texts, and/or emails attempting to get him to reset his password or open a suspicious attachment, which, upon information and belief, was caused by the Data Breach. This misuse of his PII was caused, upon information and belief, by the fact that cybercriminals are able to easily

use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

262. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII/PHI resulting from the compromise of his PII/PHI, especially his date of birth, in combination with his medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

263. Knowing that thieves stole his PII/PHI and knowing that his information will likely be sold on the dark web, has caused Plaintiff great anxiety.

264. Plaintiff has a continuing interest in ensuring that his PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

265. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Marianne From

266. Plaintiff Marianne From is a patient of the Defendant who started to use Defendant's services in 2019.

267. As a condition of obtaining services from Defendant, she was required to provide her PII/PHI and other confidential information to Defendant.

268. Plaintiff entrusted her PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII or PHI.

269. Plaintiff would not have allowed Defendant to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her information.

270. On or about July 22, 2024, Plaintiff Marianne From received notice from Defendant alerting her that her Private Information, including her date of birth, email and PHI, had been accessed by cybercriminals during the Data Breach.

271. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

272. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

273. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

274. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

275. Plaintiff has suffered actual injury in the form of experiencing a dramatic increase in spam calls, texts, and/or emails attempting to get her to reset her password or open a suspicious attachment, which, upon information and belief, was caused by the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

276. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

277. Knowing that thieves stole her PII/PHI and knowing that her information will likely be sold on the dark web, has caused Plaintiff great anxiety.

278. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

279. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Angelique Skipper

280. Plaintiff Angelique Skipper is a patient of the Defendant.

281. As a condition of obtaining services from Defendant, she was required to provide her PII/PHI and other confidential information to Defendant.

282. Plaintiff entrusted her PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII or PHI.

283. Plaintiff would not have allowed Defendant to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her information.

284. On or about July 16, 2024, Plaintiff Marianne From received notice from Defendant alerting her that her Private Information, including her date of birth and PHI, had been accessed by cybercriminals during the Data Breach.

285. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

286. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

287. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

288. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

289. Plaintiff has suffered actual injury in the form of experiencing a dramatic increase in spam calls, texts, and/or emails attempting to get her to reset her password or open a suspicious attachment, which, upon information and belief, was caused by the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

290. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

291. Knowing that thieves stole her PII/PHI and knowing that her information will likely be sold on the dark web, has caused Plaintiff great anxiety.

292. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

293. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Russell From on behalf of M.F., a minor

294. Plaintiff M.F. is a patient of the Defendant who started to use the Defendant's services in 2019.

295. As a condition of obtaining services from Defendant, Plaintiff Russell From was required to provide M.F.'s PII/PHI and other confidential information to Defendant.

296. Plaintiff Russell From entrusted M.F.'s PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify his of any data security incidents related to M.F.'s PII or PHI.

297. Plaintiff Russell From would not have allowed Defendant to collect and maintain M.F.'s PII/PHI had he known that Defendant would not take reasonable steps to safeguard M.F.'s information.

298. On or about July 20, 2024, Plaintiff Russell From received notice from Defendant alerting him that M.F.'s Private Information, including his date of birth and PHI, had been accessed by cybercriminals during the Data Breach.

299. Plaintiff Russell From has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and

self-monitoring M.F.'s accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

300. Plaintiff Russell From stores all documents containing M.F.'s PII/PHI in a safe and secure location. Moreover, Plaintiff Russell From diligently choose unique usernames and passwords for the online accounts that M.F. has.

301. Plaintiff M.F. has suffered actual injury in the form of damages to, and diminution in, the value of his PII/PHI – a form of intangible property that Plaintiff and/or his guardians entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

302. Plaintiff Russell Fromhas also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and have anxiety and increased concerns due to the loss of Plaintiff's privacy and the substantial risk of fraud and identity theft which he now faces.

303. Plaintiff Russell From and M.F. have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII/PHI resulting from the compromise of his PII/PHI, especially his date of birth, in combination with his medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

304. Knowing that thieves stole M.F.'s PII/PHI and knowing that his information will likely be sold on the dark web, has caused Plaintiff Russell From great anxiety.

305. Plaintiff Russell From and M.F. have a continuing interest in ensuring that M.F.'s PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

306. As a result of the Data Breach, Plaintiff M.F. is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Russell From on behalf of O.F., a minor

307. Plaintiff O.F. is a patient of the Defendant who started to use the Defendant's services in 2019.

308. As a condition of obtaining services from Defendant, Plaintiff Russell From was required to provide O.F.'s PII/PHI and other confidential information to Defendant.

309. Plaintiff Russell From entrusted O.F.'s PII/PHI and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to O.F.'s PII or PHI.

310. Plaintiff Russell From would not have allowed Defendant to collect and maintain O.F.'s PII/PHI had she known that Defendant would not take reasonable steps to safeguard O.F.'s information.

311. On or about July 20, 2024, Plaintiff Russell From received notice from Defendant alerting him that O.F.'s Private Information, including O.F.'s date of birth and PHI, had been accessed by cybercriminals during the Data Breach.

312. Plaintiff Russell From has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and

self-monitoring O.F.'s accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

313. Plaintiff Russell From stores all documents containing her PII/PHI in a safe and secure location. Moreover, Plaintiff Russell From diligently chooses unique usernames and passwords for the online accounts that O.F. has.

314. Plaintiff O.F. has suffered actual injury in the form of damages to, and diminution in, the value of O.F.'s PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This information was compromised in, and has been diminished as a result of, the Data Breach.

315. Plaintiff Russell From has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of O.F.'s privacy and the substantial risk of fraud and identity theft which O.F. now faces.

316. Plaintiff O.F. has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of O.F.'s PII/PHI resulting from the compromise of O.F.'s PII/PHI, especially her date of birth, in combination with her medical history, which is now in the hands of cyber criminals and other unauthorized third parties.

317. Knowing that thieves stole O.F.'s PII/PHI and knowing that her information will likely be sold on the dark web, has caused Plaintiff Russell From great anxiety.

318. Plaintiffs Russell From and O.F. have a continuing interest in ensuring that O.F.'s PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

319. As a result of the Data Breach, Plaintiff O.F. is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

CLASS REPRESENTATION ALLEGATIONS

320. Plaintiffs bring this action on behalf of themselves and, pursuant to Wis. Stat. § 803.08 a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendant, Defendant's executives and officers, any Judge assigned to this case, as well as the Court's staff and immediate family members. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

321. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process. On information and belief, the number of affected individuals is estimated to be 228,287.[52] The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

322. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

---

[52] *Data Breach Notifications*, MAINE ATTY GEN, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/223c815b-8525-491d-ab29-41d003ecfe00.html (last visited Nov. 14, 2024).

a. Whether First Choice had a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using, and/or safeguarding their Private Information;

b. Whether First Choice knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether First Choice's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether First Choice's failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether First Choice failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether First Choice adequately, promptly, and accurately informed Plaintiffs and Class members that their Private Information had been compromised;

g. How and when First Choice actually learned of the Data Breach;

h. Whether First Choice's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the accessibility of the Private Information of Plaintiffs and Class members;

i. Whether First Choice adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

j. Whether First Choice engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class members;

k. Whether Plaintiffs and Class members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of First Choice's wrongful conduct; and

l. Whether Plaintiffs and Class members are entitled to restitution as a result of First Choice's wrongful conduct.

323. Typicality: Plaintiffs' claims are typical of the claims of the Class as Plaintiffs and all members of the Class had their Private Information compromised in the Data Breach. Plaintiffs' claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiffs are entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

324. Adequacy: Plaintiffs are adequate class representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

325. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class, a class action is superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual

prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class 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 the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

CAUSES OF ACTION

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

326. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

327. Plaintiffs and the Class entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and not disclose their PII/PHI to unauthorized third parties.

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

329. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

330. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class members' PII/PHI.

331. Defendant owed to Plaintiffs and Class members at least the following duties:

a. to exercise reasonable care in handling and using the PII/PHI in its care and custody;

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

c. to promptly detect attempts at unauthorized access; and

d. to notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

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

333. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

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

335. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class, as patients, entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining healthcare and other related services from Defendant.

336. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

337. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

338. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

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

340. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII/PHI by:

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

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

341. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal

information and PII/PHI of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs' and Class members' injury.

342. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harms from the Data Breach and Plaintiffs and Class members' injuries-in-fact.

343. Defendant has admitted that the PII/PHI of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

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

345. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

346. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

347. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

348. Defendant also violated the Wisconsin data breach notification law, Wis. Stat. § 134.98 which requires companies that do business in Wisconsin to notify their customers within 45 days of a data breach. And § 134.98(4) provides that "[f]ailure to comply with this section . . . may be evidence of negligence or a breach of a legal duty."

349. Defendant violated § 134.98 insofar as it became aware of its Data Breach on October 22, 2023, but then issued notice on its website on December 21, 2023—a full 60 days later (i.e., over two weeks beyond the statutory deadline). Even worse, Defendant did not send breach notification letters to individuals whose PII/PHI has been exposed in the Data Breach until July 16, 2024—approximately *nine months* after Defendant became aware of the Breach.

350. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII/PHI.

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

352. Defendant breached its respective duties to Plaintiffs and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

353. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data

breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

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

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

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

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

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

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

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

361. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

362. Plaintiffs and Class members were required to provide their PII/PHI to Defendant as a condition of receiving healthcare and other related services provided by Defendant. Plaintiffs and Class members provided their PII/PHI to Defendant and/or its third-party agents in exchange for Defendant's healthcare and other related services.

363. Plaintiffs and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

364. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

365. Plaintiffs and the Class members accepted Defendant's offers by disclosing their PII/PHI to Defendant and/or its third-party agents, in exchange for healthcare and other related services.

366. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

367. In its Privacy Policy and Notice of Privacy Practices, Defendant represented that it has a legal duty to protect Plaintiffs' and Class Member's PII/PHI.

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

369. After all, Plaintiffs and Class members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

370. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

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

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

373. Defendant materially breached the contracts it entered with Plaintiffs and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information;

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

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

375. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *infra*).

376. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

377. Plaintiffs and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

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

378. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

379. Wis. Stat. § 995.50(1) provides that:

a. "The right of privacy is recognized in this state."

b. "One whose privacy is unreasonably invaded is entitled to the following relief [including] . . . [e]quitable relief . . . [c]ompensatory damages . . . [and] [a] reasonable amount for attorney fees."

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

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

382. The unauthorized acquisition (i.e., theft) by an unauthorized third party of Plaintiffs and Class members' PII/PHI is highly offensive to a reasonable person.

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

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

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

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

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

388. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

389. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

390. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII/PHI are still maintained by Defendant within its inadequate cybersecurity system and policies.

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

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

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

393. With the exception of Paragraphs 341-357 and in the alternative to the breach of implied contract claim above, Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

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

395. Plaintiffs and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using Plaintiffs' and Class members' PII/PHI to provide services and (2) from the receipt of payments for such services.

396. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members.

397. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

398. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII/PHI.

399. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

400. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' PII/PHI and payments because Defendant failed to adequately protect their PII/PHI.

401. Plaintiffs and Class members have no adequate remedy at law.

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

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

403. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

404. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII/PHI; (2) to timely notify Plaintiffs and Class members of a data breach and disclosure of their PII/PHI; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

405. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

406. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

407. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII/PHI.

408. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

409. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Violations of Wisconsin Statute § 146.82 (1)
(On Behalf of Plaintiffs and the Class)

410. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

411. Wis. Stat. § 146.82 (1) provides that:

a. "All patient health care records shall remain confidential."

b. "Patient health care records may be released only to the persons designated in this section or to other persons ***with the informed consent of the patient*** or of a person authorized by the patient." (emphasis added).

412. Furthermore, Wis. Stat. § 146.84 (1)(bm) provides that "[a]ny person, including the state or any political subdivision of the state, who negligently violates s. 146.82 [] shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $1,000 and costs and reasonable actual attorney fees."

413. Here, Defendant negligently violated § 146.82 when it abrogated the confidentiality Plaintiffs' and Class members' health care records when it was released without their consent or authorization. And because of such negligence, Plaintiffs and Class members suffered numerous injuries (as detailed *supra*) and incurred actual damages.

414. Thus, Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law including, but not limited to, actual damages, exemplary damages, costs, and reasonable actual attorney fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

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

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

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

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

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

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: November 20, 2024

Respectfully submitted,

/s/ Samuel J. Strauss
Samuel J. Strauss (SBN: 1113942)
Alex Phillips (SBN: 1098356)
Raina Borrelli (*pro hac vice*)
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
aphillips@straussborrelli.com
sam@straussborrelli.com
raina@straussborrelli.com

David S. Almeida (SBN: 1086050)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
Telephone: (312) 576-3024
david@almeidalawgroup.com

Interim Co-Lead Class Counsel

Nickolas J. Hagman (SBN: 1085424)
Daniel O. Herrera*
Mohammed A. Rathur*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
nhagman@caffertyclobes.com
dherrera@caffertyclobes.com
mrathur@caffertyclobes.com

Jennifer Crancer (SBN: 1118726)
Philip J. Krzeski (*pro hac vice*)
CHESTNUT CAMBRONNE PA
100 Washington Ave. South, Suite 1700

Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
pkrzeski@chestnutcambronne.com
jcrancer@chestnutcambronne.com

Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Telephone: (929) 677-5144
Facsimile: (646) 417-5967
tbean@sirillp.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Telephone: (513) 345-8291
jgoldenberg@gs-legal.com

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

Brett R. Cohen*
LEEDS BROWN LAW, P.C.
One Old Country Road - Suite 347
Carle Place, NY 11514
Telephone: (516) 873-9550
bcohen@leedsbrownlaw.com

* *Pro Hac Vice* forthcoming

Additional Counsel for Plaintiffs and the Proposed Class