UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 21-MD-02994-RAR

IN RE:

MEDNAX SERVICES, INC.,
CUSTOMER DATA SECURITY BREACH LITIGATION

CONSOLIDATED COMPLAINT FOR DAMAGES

Plaintiffs, Gregory Baum, as legal guardian of a minor child whose initials are A.B., Abigail Bean, as legal guardian of a minor child whose initials are C.B., Chaya Clark, as legal guardian of minor children whose initials are J.C., J.C., and E.M., Chelsea Cohen, as parent and legal guardian of A.H., Kashari Fulks, Jessica Jay, as legal guardian of a minor child whose initials are B.J., Gerald Lee, Joseph Larsen, parent/legal guardian on behalf of A.L., Brooke Nielsen, Michael Rumely, as legal guardian of minor children whose initials are H.R. and M.R., Matias Soto, as legal guardian of a minor child whose initials are M.S., A.W. by and through her Next Friend, B.W. (collectively, "Plaintiffs") by and through the undersigned lead counsel, bring this Consolidated Complaint pursuant to Pretrial Order (PTO) No. 44 against Defendants identified below. Plaintiffs bring this Consolidated Amended Complaint for Damages on behalf of themselves and their minor children resulting from the unauthorized disclosure of their private medical information by Defendants.

Mednax is a physician-led healthcare organization that partners with hospitals, health systems, and healthcare facilities to offer clinical services spanning the continuum of care, as well as revenue cycle management, patient engagement and perioperative improvement consulting solutions. The Company is registered with the U.S. Securities and Exchange Commission.

Pediatrix, a Mednax company, is the nation's largest provider of maternal-fetal, newborn and pediatric subspecialty services and delivers comprehensive, customized health solutions designed to enhance the patient experience.

Mednax and Pediatrix collaborate with their partners and affiliates "to develop customized solutions that benefit hospitals, patients and payors," and tout on their website that they are "trusted by patients, hospitals, and referring physicians to *take great care of the patient, every day and in every way*."

Defendants are health care providers as defined under state and federal law. As such, Defendants are legally, morally, and ethically duty bound to keep confidential all information which they receive, collect, store and maintain about their patients. The medical information contains both Protected Health Information ("PHI") and Personally Identifiable Information ("PII"). Privacy of medical information and the promise of confidentiality is necessary and essential to the physician/patient relationship. When confidentiality of medical information is breached, harm is immediate and irreversible.

Health care providers are required to maintain confidential medical information in a secure electronic format. Any infiltration into or release of confidential medical information to any person or persons who are not authorized to have such information results in permanent harm to the patient. Health care providers are heavily regulated and required to maintain the strictest security protections for confidential patient information. Unlike typical "Data Breach" cases, disclosures of medical information cannot be remedied as one cannot un-know what is known.

If a health care provider experiences a wrongful disclosure of medical information, it is required to quickly notify its patients of the disclosure, take immediate action to obtain the information that was wrongfully released, investigate the harm to the patients, and take affirmative

steps to mitigate that harm. Timely notification is the first step and key to ongoing protection of client information as the health care provider's obligation of privacy does not end with the wrongful disclosure.

On June 19, 2020, Mednax discovered that some person or persons infiltrated its computer systems which housed its patients' confidential health information. The first breach occurred between June 17, 2020, and June 22, 2020. Despite learning of the breach while it was occurring, Mednax took no steps to lockdown the system to protect the medical records from disclosure. As such, the breach was allowed to continue for three additional days after discovery. Further, there was a second breach of the Mednax systems where records containing PHI and PII were disclosed. This second breach occurred a few weeks after the first, on July 2, 2020 and July 3, 2020.

At some point after both breaches, Mednax conducted an investigation and discovered that the infiltrators obtained personal health information of nearly 1.3 million patients, including names of the patients and their parents or guardians, addresses, email addresses, dates of birth, health insurance information, treatment dates and locations, treatment information, diagnoses, prescription drug information, and billing information. Despite discovering the disclosure in June, Defendants failed to notify Plaintiffs of the disclosure for almost six months. Further, Defendants took no affirmative steps to get the stolen information back or to mitigate the harm caused to Plaintiffs.

TABLE OF CONTENTS

I. NATURE OF THE CASE

1. This is a multi-district class action brought by Plaintiffs, individually and behalf of the other Class Members, seeking to redress Defendants' willful and reckless violations of their privacy rights. Plaintiffs and the other Class Members are patients of Defendants and/or their parents/guardians who entrusted their Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to Defendants. Defendants betrayed Plaintiffs' trust by failing to properly safeguard and protect their PHI and PII and by publicly disclosing their PHI and PII without authorization in violation of numerous laws and statutes.

2. This action pertains to Defendants' unauthorized disclosure of the Plaintiff's PHI and PII that occurred between the dates of June 17, 2020 to June 22, 2020 and July 2, 2020 and July 3, 2020. (the "Breach" or the "Healthcare Data Breach").

3. Defendants disclosed Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendants' failure to safeguard and protect their PHI and PII.

4. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiffs' and the other Class Members' names, addresses, email addresses, dates of birth, medical records, patient account numbers, health insurance information, Social Security numbers, and/or limited treatment or clinical information, such as diagnosis, provider names, dates of service, and other medical information.

5. Defendants flagrantly disregarded Plaintiffs' and the other Class Members' privacy and property rights by intentionally, willfully, and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII from unauthorized disclosure. Plaintiffs' and the other Class Members' PHI and PII were

improperly handled, inadequately protected, readily able to be copied by thieves and not kept in accordance with basic security protocols. Defendants' procurement of the information and sharing of same also represents a flagrant disregard of Plaintiffs' and the other Class Members' rights, both as to privacy and property.

6. Plaintiffs have standing to bring this action because as a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiffs have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) loss of medical expenses, and/or (iii) the additional damages set forth in detail below, which are incorporated herein by reference.

7. Defendants' wrongful actions and/or inaction and the resulting Breach mean that Plaintiffs and the other Class Members now face a present, immediate and continuing increased risk of identity theft, identity fraud, and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII is subject to a reported data breach—such as the Healthcare Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiffs' and the other Class Members' PHI and PII and not yet used the information will do so at a later date or re-sell it.

8. Plaintiffs and Class members have also suffered and are entitled to damages for the lost benefit of their bargain with the Defendants. Plaintiffs and members of the Class paid Defendants for their services, including protecting their PII and PHI. The lost benefit of the

bargain is measured by the difference between the value of what Plaintiffs and the members of the Class should have received when they paid for their services, and the value of what they actually did receive; services without adequate privacy safeguards. Plaintiffs and members of the Class have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiffs and the members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

9. Additionally, because of Defendants' conduct, Plaintiffs and members of the Class have been harmed in that Defendants have breached their common law fiduciary duty of confidentiality owed to Plaintiffs and members of the Class.

10. Accordingly, Plaintiffs and the other Class Members seek redress against Defendants in the form of for actual damages, statutory damages, punitive damages, and restitution, with attorney fees, costs, and expenses, under the consumer protection statutes of the various states including, Missouri, California, and Florida, and other state's personal and medical privacy laws and state consumer protection and unfair and deceptive practices acts Plaintiffs further sue Defendants for, among other causes of action, breach of fiduciary duty of confidentiality of medical records, breach of implied contract, negligence, negligence *per se*, and negligent training and supervision. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendants' data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, other remedies as the Court sees necessary and properly incurred in bringing this action, and all other remedies this Court deems proper.

11. Plaintiffs, individually and on behalf of the other Class Members, seek all (i) actual damages, economic damages, and/or nominal damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

II. JURISDICTION AND VENUE

12. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs and members of the Class are citizens of states that differ from Defendants.

13. This Court has personal jurisdiction over Defendants because Defendants conduct business in and have sufficient minimum contacts with Florida and Defendant Mednax's principal place of business is Florida.

14. Venue is likewise proper in this District as to Defendants under 28 U.S.C. § 1391(a)(1) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District. Defendants conduct business through this District (including promoting, selling, marketing, and distributing the MEDNAX and Pediatrix brands and services at issue).

III. PARTIES

15. Plaintiff A.W. ("Plaintiff A.W.") is a minor child residing in Blue Springs, Missouri and is the natural daughter of Plaintiff B.W. Plaintiff A.W. was a patient of, and received, medical services from Defendants.

16. Plaintiff B.W. ("Plaintiff B.W.") is an adult residing in Blue Springs, Missouri and is a citizen of Missouri. She is the Natural Mother, and the Next Friend, of Plaintiff A.W.

17. On or around December 19, 2020, Plaintiff B.W. received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying her that Plaintiff A.W.'s PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that Plaintiff A.W.'s name, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by Plaintiff A.W.'s providers) may have been involved.

18. As a result of the Healthcare Data Breach notice, Plaintiff B.W. spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts on behalf of herself and Plaintiff A.W. This time has been lost forever and cannot be recaptured.

19. Additionally, Plaintiff B.W. is very careful about sharing her and Plaintiff A.W.'s sensitive PHI and PII. She has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

20. Plaintiff B.W. stores any documents containing her and Plaintiff A.W.'s sensitive PHI and PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

21. Plaintiff B.W. suffered actual injury in the form of damages to and diminution in the value of her and Plaintiff A.W.'s PHI and PII: forms of intangible property that Plaintiff B.W. entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

22. Plaintiff B.W. suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of her and Plaintiff A.W.'s privacy.

23. Plaintiff B.W. and Plaintiff A.W. have suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her and Plaintiff A.W.'s PHI and PII, especially her and Plaintiff A.W.'s Social Security numbers, in combination with her and Plaintiff A.W.'s names, being placed in the hands of unauthorized third parties and possibly criminals.

24. Plaintiff B.W. has a continuing interest in ensuring that her and Plaintiff A.W.'s PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

25. Plaintiff B.W., on behalf of her child A.W., has suffered actual injury from having Plaintiff A.W.'s PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of her bargain with Defendants.

26. Plaintiff A.W.'s PHI and PII, including her Social Security number, has been found available for purchase on the dark web.

27. Plaintiff B.W.'s PHI and PII, including her Social Security number, has been found available for purchase on the dark web.

28. The compromise of their PHI and PII through their publication has drastically increased Plaintiff A.W.'s and Plaintiff B.W.'s risk of identity theft. It is now a matter of when, not if, they will have additional damages and problems.

29. Because Plaintiff A.W.'s and Plaintiff B.W.'s PHI and PII were found on a popular marketplace, it can be assumed that their PHI and PII has already been used and sold for higher prices in smaller forums on the dark web first.

30. By the time that an individual's stolen PHI and PII makes it to an auction or online sale site, it usually has already been used, sold for higher prices, or have been broken up into pieces

of the data. These secondary sites are essentially scalpers. First copies usually sell for much more and are bartered in forums on the dark web. Most original hackers do not sell the majority of the data for the first one to two years. The individual's PHI and PII— such as PHI and PII belonging to Plaintiff A.W. and Plaintiff B.W. — is now being sold by thieves to thieves on the dark web.

31. Considering the geographic distribution of Plaintiffs and the inclusion of multiple Plaintiffs' PHI and PII in one sample database, it can be reasonably assumed that the data likely came from the same source data breach.

32. Plaintiff A.W. and Plaintiff B.W. will now have to freeze their credit and enroll in credit and identity monitoring to combat the long-lasting ramifications of the Healthcare Data Breach.

33. Plaintiff A.W. and Plaintiff B.W.'s need for extensive credit monitoring is a reasonably certain consequence of Defendants' breach of their duties, as described further below.

34. Defendants did not offer Plaintiffs A.W. or B.W. credit or identity monitoring.

35. Plaintiff B.W. is in the process of trying to freeze Plaintiff A.W.'s credit.

36. Plaintiff B.W. had an expectation that Plaintiff A.W.'s PHI and PII would not be disclosed.

37. Had Plaintiff B.W. been informed her child's PHI and PII could be exposed to unauthorized third parties, she would have sought medical treatment from a different provider.

38. Plaintiff B.W. had to provide her own PII, including her Social Security number, for her child to be treated.

39. Plaintiff B.W. has enrolled in identity theft protection as a result of the Healthcare Data Breach.

40. As a result of the Healthcare Data Breach, Plaintiffs B.W. and A.W. will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

41. Plaintiff Michael Rumely ("Plaintiff Rumely") is the legal guardian of H.R. and M.R. They are citizens and residents of California. Plaintiff Rumely's minor children were patients of, and received medical services from, Defendants.

42. In or around December 2020, Plaintiff Rumely received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying him that his children's PHI/PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that his children's names, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by his children's providers) may have been involved.

43. As a result of the Healthcare Data Breach notice, Plaintiff Rumely spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts on behalf of himself and H.R. and M.R. This time has been lost forever and cannot be recaptured.

44. Additionally, Plaintiff Rumely is very careful about sharing H.R.'s and M.R.'s sensitive PHI and PII. He has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

45. Plaintiff Rumely stores any documents containing H.R.'s and M.R.'s sensitive PHI and PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

46. Plaintiff Rumely, on behalf of H.R. and M.R., has suffered actual injury in the form of damages to and diminution in the value of H.R.'s and M.R.'s PHI and PII; forms of intangible

property that Plaintiff Rumely entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

47. Plaintiff Rumely suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of H.R.'s and M.R.'s privacy.

48. Plaintiff Rumely, on behalf of H.R. and M.R., has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from H.R.'s and M.R.'s PHI and PII, especially their Social Security numbers, in combination with their names, being placed in the hands of unauthorized third parties and possibly criminals.

49. Plaintiff Rumely has a continuing interest in ensuring that H.R.'s and M.R.'s PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

50. Plaintiff Rumely, on behalf of his children, has suffered actual injury from having his children's PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of his bargain with Defendants.

51. Defendants did not offer Plaintiff Rumely or his children credit or identity monitoring.

52. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Rumely enrolled his family in Norton LifeLock theft protection, which costs between $300.00 - $500.00 a year.

53. Plaintiff Rumely had an expectation that his children's PHI and PII would not be disclosed.

54. Had Plaintiff Rumely been informed his children's PHI and PII could be exposed to unauthorized third parties, he would have sought medical treatment from a different provider.

55. As a result of the Healthcare Data Breach, Plaintiff Rumely, on behalf of his children, will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

56. Plaintiff Abigail Bean ("Plaintiff Bean") is the legal guardian of C.B. and they are citizens and residents of Oklahoma. Plaintiff Bean's minor child, C.B., was a patient of, and received medical services from, Defendants.

57. In or around late December 2020, Plaintiff Bean received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying her that her child's PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that her child's name, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by her child's provider) may have been involved.

58. As a result of the Healthcare Data Breach notice, Plaintiff Bean spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts on behalf of herself and C.B. This time has been lost forever and cannot be recaptured.

59. Additionally, Plaintiff Bean is very careful about sharing C.B.'s sensitive PHI and PII. She has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

60. Plaintiff Bean stores any documents containing C.B.'s sensitive PHI and PII in a safe and secure location or destroys the documents.

61. Plaintiff Bean, on behalf of C.B., has suffered actual injury in the form of damages to and diminution in the value of C.B.'s PHI and PII: a form of intangible property that Plaintiff Bean entrusted to Defendants for the purpose of obtaining services from Defendants, which was compromised in and as a result of the Healthcare Data Breach.

62. Plaintiff Bean, on behalf of C.B., suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of C.B.'s privacy.

63. Plaintiff Bean, on behalf of C.B., has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from C.B.'s PHI and PII, especially the child's Social Security number, in combination with the child's name, being placed in the hands of unauthorized third parties and possibly criminals.

64. Plaintiff Bean has a continuing interest in ensuring that C.B.'s PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

65. Plaintiff Bean, on behalf of her child, has suffered actual injury from having her child's PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of her bargain with Defendants.

66. Defendants did not offer Plaintiff Bean or her child credit or identity monitoring.

67. As a direct and proximate result of the Data Breach, Plaintiff Bean enrolled in Norton LifeLock identity theft protection.

68. The Norton LifeLock identity theft protection costs $23.80 a month.

69. Plaintiff Bean had to provide her own PII for her child to be seen by the provider.

70. Plaintiff Bean was required to disclose her name, address, birthdate, health insurance information, medical information, payment information, and potentially her child's and her Social Security numbers.

71. Plaintiff Bean had an expectation that her child's PHI and PII would not be disclosed.

72. Had Plaintiff Bean been informed that her child's PHI and PII could be exposed to unauthorized third parties, she would have sought medical treatment from a different provider.

73. As a result of the Healthcare Data Breach, Plaintiff Bean, on behalf of her child, will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

74. Plaintiff Jessica Jay ("Plaintiff Jay") is the legal guardian of B.J. and they are citizens and residents of Washington. Plaintiff Jay's minor child, B.J., was a patient of, and received medical services from, Defendants.

75. In or around December 2020, Plaintiff Jay received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying her that her child's PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that her child's name, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by her child's provider) may have been involved.

76. As a result of the Healthcare Data Breach notice, Plaintiff Jay spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts on behalf of herself and B.J. This time has been lost forever and cannot be recaptured.

77. Additionally, Plaintiff Jay is very careful about sharing B.J.'s sensitive PHI and PII. She has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

78. Plaintiff Jay stores any documents containing B.J.'s sensitive PHI and PII in a safe and secure location or destroys the documents.

79. Plaintiff Jay, on behalf of B.J., has suffered actual injury in the form of damages to and diminution in the value of B.J.'s PHI and PII: forms of intangible property that Plaintiff Jay entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

80. Plaintiff Jay, on behalf of B.J., suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of B.J.'s privacy.

81. Plaintiff Jay, on behalf of B.J., has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from B.J.'s PHI and PII, especially the child's Social Security number, in combination with the child's name, being placed in the hands of unauthorized third parties and possibly criminals.

82. Plaintiff Jay has a continuing interest in ensuring that B.J.'s PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

83. Plaintiff Jay, on behalf of her child, has suffered actual injury from having her child's PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of her bargain with Defendants.

84. Defendants did not offer Plaintiff Jay or her child credit or identity monitoring.

85. Plaintiff Jay was required to disclose her health history, Social Security number, address, telephone number, and spouse's name, among other things to the provider that was affiliated with Defendants.

86. Plaintiff Jay had an expectation that her child's PHI and PII would not be disclosed.

87. Had Plaintiff Jay been informed her child's PHI and PII could be exposed to unauthorized third parties, she may have sought medical treatment from a different provider.

88. As a result of the Healthcare Data Breach, Plaintiff Jay, on behalf of her child, will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

89. Plaintiff Matias Soto ("Plaintiff Soto") is the legal guardian of M.S. and they are citizens and residents of Texas. Plaintiff Soto's minor child, M.S., was a patient of, and received medical services from, Defendants.

90. In or around early January 2021, Plaintiff Soto received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying him that his child's PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that his child's name, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by his child's provider) may have been involved.

91. As a result of the Healthcare Data Breach notice, Plaintiff Soto spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts on behalf of himself and M.S. This time has been lost forever and cannot be recaptured.

92. Additionally, Plaintiff Soto is very careful about sharing M.S.'s sensitive PHI and PII. He has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

93. Plaintiff Soto stores any documents containing M.S.'s sensitive PHI and PII in a safe and secure location or destroys the documents.

94. Plaintiff Soto, on behalf of M.S., has suffered actual injury in the form of damages to and diminution in the value of M.S.'s PHI and PII: forms of intangible property that Plaintiff Soto entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

95. Plaintiff Soto, on behalf of M.S., suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of M.S.'s privacy.

96. Plaintiff Soto, on behalf of M.S., has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from M.S.'s PHI and PII, especially the child's Social Security number, in combination with the child's name, being placed in the hands of unauthorized third parties and possibly criminals.

97. Plaintiff Soto has a continuing interest in ensuring that M.S.'s PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

98. Plaintiff Soto, on behalf of his child, has suffered actual injury from having his child's PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of his bargain with Defendants.

99. PII belonging to M.S., Plaintiff Soto's child, including the child's Social Security number, has been found available for purchase on the dark web.

100. The compromise of the child's PHI and PII through its publication has drastically increased M.S.'s risk of identity theft. It is now a matter of when, not if, the child will have

additional damages and problems.

101. To the best of Plaintiff Soto's knowledge, M.S. has never been involved in another data breach. As such, and given the temporal relationship, it may be reasonably assumed that the offer of sale of M.S.'s PII is tied to the Healthcare Data Breach.

102. Because M.S.'s PII was found on a popular marketplace, it can be assumed that the child's PII has already been used and sold for higher prices in smaller forums on the dark web first.

103. By the time that an individual's stolen PII makes it to an auction or online sale site, it usually has already been used, sold for higher prices, or have been broken up into pieces of the data. These secondary sites are essentially scalpers. First copies usually sell for much more and are bartered in forums on the dark web. Most original hackers do not sell the majority of the data for the first one to two years. The individual's PHI and PII— such as PHI and PII belonging to M.S. — is now being sold by thieves to thieves on the dark web.

104. Considering the geographic distribution of Plaintiffs and the inclusion of multiple Plaintiffs' PII in one sample database, it can be reasonably assumed that the data likely came from the same source data breach.

105. Plaintiff Soto, on behalf of M.S., will now have to freeze M.S.'s credit and enroll in credit and identity monitoring to combat the long-lasting ramifications of the Healthcare Data Breach.

106. M.S.'s need for extensive credit monitoring is a reasonably certain consequence of Defendants' breach of their duties, as described further below.

107. Defendants did not offer Plaintiff Soto or his child credit or identity monitoring.

108. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Soto enrolled in credit monitoring services and has placed a fraud alert with Equifax for himself. The credit monitoring services cost $12.90/month.

109. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Soto has now spent at least $100.00 on credit monitoring services.

110. Plaintiff Soto was required to disclose his name, health insurance information, and possibly his Social Security number in order for his child to be seen by the provider affiliated with Defendants.

111. Plaintiff Soto had an expectation that his child's PHI and PII would not be disclosed.

112. Had Plaintiff Soto been informed his child's PHI and PII could be exposed to unauthorized third parties, he would have sought medical treatment from a different provider.

113. As a result of the Healthcare Data Breach, Plaintiff Soto, on behalf of his child, will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

114. Plaintiff Gregory Baum ("Plaintiff Baum") is the legal guardian of A.B. and they are citizens and residents of Oklahoma. Plaintiff Baum's minor child, A.B., was a patient of, and received medical services from, Defendants.

115. In or around late December 2020, Plaintiff Baum received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying him that his child's PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that his child's name, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by his child's provider) may have been involved.

116. As a result of the Healthcare Data Breach notice, Plaintiff Baum spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance

options, and self-monitoring accounts on behalf of himself and A.B. This time has been lost forever and cannot be recaptured.

117. Additionally, Plaintiff Baum is very careful about sharing A.B.'s sensitive PHI and PII. He has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

118. Plaintiff Baum stores any documents containing A.B.'s sensitive PHI and PII in a safe and secure location or destroys the documents.

119. Plaintiff Baum, on behalf of A.B., has suffered actual injury in the form of damages to and diminution in the value of A.B.'s PHI and PII: forms of intangible property that Plaintiff Baum entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

120. Plaintiff Baum, on behalf of A.B., suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of A.B.'s privacy.

121. Plaintiff Baum, on behalf of A.B., has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from A.B.'s PII/PHI, especially the child's Social Security number, in combination with the child's name, being placed in the hands of unauthorized third parties and possibly criminals.

122. Plaintiff Baum has a continuing interest in ensuring that A.B.'s PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

123. Plaintiff Baum, on behalf of his child, has suffered actual injury from having his child's PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of his bargain with Defendants.

124. PII belonging to A.B., Plaintiff Baum's child, including the child's Social Security number, has been found available for purchase on the dark web.

125. The compromise of the child's PHI and PII through its publication has drastically increased A.B.'s risk of identity theft. It is now a matter of when, not if, the child will have additional damages and problems.

126. To the best of Plaintiff Baum's knowledge, A.B. has never been involved in another data breach. As such, and given the temporal relationship, it may be reasonably assumed that the offer of sale of A.B.'s PII is tied to the Healthcare Data Breach.

127. Because A.B.'s PHI and PII was found on a popular marketplace, it can be assumed that the child's PHI and PII has already been used and sold for higher prices in smaller forums on the dark web first.

128. By the time that an individual's stolen PHI and PII makes it to an auction or online sale site, it usually has already been used, sold for higher prices, or have been broken up into pieces of the data. These secondary sites are essentially scalpers. First copies usually sell for much more and are bartered in forums on the dark web. Most original hackers do not sell the majority of the data for the first one to two years. The individual's PHI and PII— such as PHI and PII belonging to A.B. — is now being sold by thieves to thieves on the dark web.

129. Considering the geographic distribution of Plaintiffs and the inclusion of multiple Plaintiffs' PHI and PII in one sample database, it can be reasonably assumed that the data likely came from the same source data breach.

130. Plaintiff Baum, on behalf of A.B., will now have to freeze A.B.'s credit and enroll in credit and identity monitoring to combat the long-lasting ramifications of the Healthcare Data Breach.

131. A.B.'s need for extensive credit monitoring is a reasonably certain consequence of Defendants' breach of their duties, as described further below.

132. Defendants did not offer Plaintiff Baum or his child credit or identity monitoring.

133. At the time of the Data Breach, Plaintiff Baum was already enrolled in credit monitoring services through his homeowner's insurance. The credit monitoring costs $12.00/year

and provides up to $25,000.00 in coverage. The coverage covers anyone in Plaintiff Baum's household.

134. As a direct and proximate result of the Data Breach, Plaintiff Baum elected to continue enrollment in the credit monitoring service.

135. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Baum has now spent at least $24.00 on credit monitoring services.

136. Plaintiff Baum had an expectation that his child's PHI and PII would not be disclosed.

137. Had Plaintiff Baum been informed his child's PHI and PII could be exposed to unauthorized third parties, he would have sought medical treatment from a different provider.

138. As a result of the Healthcare Data Breach, Plaintiff Baum, on behalf of his child, will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

139. Plaintiff Joseph Larsen ("Plaintiff Larsen") is the parent and legal guardian of a minor whose initials are A.L., and is a citizen and resident of Phoenix, Arizona. A.L. was a patient of, and received, medical services from, Defendants.

140. In or around December 16, 2020, Plaintiff Larsen received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying him that his child's PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that his child's name, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by his child's provider) may have been involved.

141. As a result of the Healthcare Data Breach notice, Plaintiff Larsen spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts on behalf of himself and A.L. This time has been lost forever and cannot be recaptured.

142. Additionally, Plaintiff Larsen is very careful about sharing his and A.L.'s sensitive PHI and PII. He has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

143. Plaintiff Larsen stores any documents containing his and A.L.'s sensitive PHI and PII in a safe and secure location or destroys the documents. Plaintiff Larsen keeps hard copies locked in a safe and digital information is encrypted on a zero knowledge cloud service.

144. Plaintiff Larsen, on behalf of himself and A.L., has suffered actual injury in the form of damages to and diminution in the value of his and A.L.'s PHI and PII: forms of intangible property that Plaintiff Larsen entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

145. Plaintiff Larsen, on behalf of himself and A.L., suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of his and A.L.'s privacy.

146. Plaintiff Larsen, on behalf of himself and A.L., has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his and A.L.'s PHI and PII, especially their Social Security numbers, in combination with their names, being placed in the hands of unauthorized third parties and possibly criminals.

147. Plaintiff Larsen has a continuing interest in ensuring that his and A.L.'s PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

148. Plaintiff Larsen, on behalf of himself and his child, has suffered actual injury from having his and his child's PHI and PII exposed as a result of the Healthcare Data Breach including,

but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of his bargain with Defendants.

149. PHI and PII belonging to A.L., Plaintiff Larsen's child, including the child's Social Security number, has been found available for purchase on the dark web.

150. Plaintiff Larsen's PHI and PII, including his Social Security number, has also been found available for purchase on the dark web.

151. The compromise of the child's and Plaintiff Larsen's PHI and PII through their publication has drastically increased A.L.'s and Plaintiff Larsen's risk of identity theft. It is now a matter of when, not if, the child and Plaintiff Larsen will have additional damages and problems.

152. To the best of Plaintiff Larsen's knowledge, A.L. has never been involved in another data breach. As such, and given the temporal relationship, it may be reasonably assumed that the offer of sale of A.L.'s PHI and PII is tied to the Healthcare Data Breach.

153. Because A.L.'s and Plaintiff Larsen's PHI and PII was found on a popular marketplace, it can be assumed that the child's and Plaintiff Larsen's PHI and PII have already been used and sold for higher prices in smaller forums on the dark web first.

154. By the time that an individual's stolen PHI and PII makes it to an auction or online sale site, it usually has already been used, sold for higher prices, or have been broken up into pieces of the data. These secondary sites are essentially scalpers. First copies usually sell for much more and are bartered in forums on the dark web. Most original hackers do not sell the majority of the data for the first one to two years. The individual's PHI and PII— such as PHI and PII belonging to A.L. and Plaintiff Larsen — is now being sold by thieves to thieves on the dark web.

155. Considering the geographic distribution of Plaintiffs and the inclusion of multiple Plaintiffs' PHI and PII in one sample database, it can be reasonably assumed that the data likely came from the same source data breach.

156. Plaintiff Larsen, on behalf of A.L. and himself, will now have to freeze A.L.'s and his credit and has had to enroll in credit and identity monitoring to combat the long-lasting ramifications of the Healthcare Data Breach.

157. A.L.'s and Plaintiff Larsen's need for extensive credit monitoring is a reasonably certain consequence of Defendants' breach of their duties, as described further below.

158. Defendants did not offer Plaintiff Larsen or his child credit or identity monitoring.

159. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Larsen enrolled in credit monitoring services through LifeLock. The credit monitoring will cost $60.00/year. Plaintiff Larsen is currently in a trial period. The credit monitoring will monitor his child's PHI and PII.

160. Plaintiff Larsen had an expectation that his child's PHI and PII would not be disclosed.

161. Had Plaintiff Larsen been informed his child's PHI and PII could be exposed to unauthorized third parties, he would have sought medical treatment from a different provider.

162. As a result of the Healthcare Data Breach, Plaintiff Larsen, on behalf of himself and his child, will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

163. Plaintiff Kashari Fulks ("Plaintiff Fulks") is, and at all times mentioned herein was, an individual citizen of the State of North Carolina residing in the City of Charlotte. Plaintiff Fulks is a patient of, and received, medical services from, Defendants.

164. In or around December 2020, Plaintiff Fulks received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying her that her PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. Ms. Fulks was not yet married when she received the Notice of Security Incident, which was addressed to Kashari Davis, her maiden name. The "Notice of Security Event" specifically stated that her name, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers),

and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by her provider) may have been involved.

165. As a result of the Healthcare Data Breach notice, Plaintiff Fulks spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts. This time has been lost forever and cannot be recaptured.

166. Additionally, Plaintiff Fulks is very careful about sharing her sensitive PHI and PII. She has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

167. Plaintiff Fulks stores any documents containing her sensitive PHI and PII in a safe and secure location or destroys the documents.

168. Plaintiff Fulks has suffered actual injury in the form of damages to and diminution in the value of her PHI and PII: forms of intangible property that Plaintiff Fulks entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

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

170. Plaintiff Fulks has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PHI and PII, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and possibly criminals.

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

172. Plaintiff Fulks has suffered actual injury from having her PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present

and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of her bargain with Defendants.

173. Plaintiff Fulks had an expectation that her PHI and PII would not be disclosed.

174. Had Plaintiff Fulks been informed her PHI and PII could be exposed to unauthorized third parties, she would have sought medical treatment from a different provider.

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

176. Plaintiff Brooke Nielsen ("Plaintiff Nielsen") is a citizen and resident of the state of Virginia. Plaintiff Nielsen received medical services from Defendants.

177. In or around January 2021, Plaintiff Nielsen received a "Notification to American Anesthesiology Patients of Business Associate Data Security Event" dated January 13, 2021, from Defendant American Anesthesiology notifying her that her PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The Notification specifically stated that her contact information (such as her name, guarantor name, address, email address, and dates of birth), her state identification number, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, payment details, submitted claims and appeals, and patient account identifiers used by her provider) may have been involved.

178. As a result of the Healthcare Data Breach notice, Plaintiff Nielsen spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

179. Additionally, Plaintiff Nielsen is very careful about sharing her sensitive PHI and PII. She has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

180. Plaintiff Nielsen stores any documents containing her sensitive PHI and PII in a safe and secure location or destroys the documents.

181. Plaintiff Nielsen has suffered actual injury in the form of damages to and diminution in the value of her PHI and PII: forms of intangible property that Plaintiff Nielsen entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

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

183. Plaintiff Nielsen has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PHI and PII, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and possibly criminals.

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

185. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Nielsen has become a victim of identity theft and has suffered actual identity theft.

186. As a direct and proximate result of the Healthcare Data Breach, twelve bank accounts have been opened in Plaintiff Nielsen's name.

187. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Nielsen's credit score has been negatively affected.

188. As a direct and proximate result of the Data Breach, Plaintiff Nielsen had to pay American Anesthesiology $81.47 upon discovering the bill was marked as overdue and unpaid

and had been sent to collections, although the $81.47 was from a bill her insurance had already paid in 2017.

189. Plaintiff Nielsen has further suffered actual injury from having her PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of her bargain with Defendants.

190. Plaintiff Nielsen had an expectation that her PHI and PII would not be disclosed.

191. Plaintiff Nielsen has spent at least 60-80 hours responding to the Healthcare Data Breach, including filing police reports.

192. Plaintiff Nielsen has spent time freezing her credit as a result of the Healthcare Data Breach.

193. Plaintiff Nielsen has enrolled in credit monitoring as a result of the Healthcare Data Breach.

194. Had Plaintiff Nielsen been informed her PHI and PII could be exposed to unauthorized third parties, she would have sought medical treatment from a different provider.

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

196. Plaintiff Gerald Lee ("Plaintiff Lee") is a citizen and resident of the state of South Carolina. Plaintiff Lee was a patient of, and received, medical services from, Defendants.

197. In or around January 2021, Plaintiff Lee received a "Notification to American Anesthesiology Patients of Business Associate Data Security Event" dated January 13, 2021, from Defendant American Anesthesiology notifying him that his PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The Notification specifically stated that his contact information (such as his name, guarantor name, address, email address, and dates of birth), his state identification number, health insurance information (payor name, payor contract dates, policy

information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, payment details, submitted claims and appeals, and patient account identifiers used by his provider) may have been involved.

198. As a result of the Healthcare Data Breach notice, Plaintiff Lee spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

199. Additionally, Plaintiff Lee is very careful about sharing his sensitive PHI and PII. He has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

200. Plaintiff Lee stores any documents containing his sensitive PHI and PII in a safe and secure location or destroys the documents.

201. Plaintiff Lee has suffered actual injury in the form of damages to and diminution in the value of his PII/PHI: forms of intangible property that Plaintiff Lee entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

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

203. Plaintiff Lee has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PHI and PII, especially his Social Security number, in combination with his name, being placed in the hands of unauthorized third parties and possibly criminals.

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

205. Plaintiff Lee has suffered actual injury from having his PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of his bargain with Defendants.

206. PHI and PII belonging to Plaintiff Lee, including his Social Security number, has been found available for purchase on the dark web.

207. The compromise of Plaintiff Lee's PHI and PII through its publication has drastically increased his risk of identity theft. It is now a matter of when, not if, he will have additional damages and problems.

208. Because Plaintiff Lee's PHI and PII was found on a popular marketplace, it can be assumed that his PHI and PII has already been used and sold for higher prices in smaller forums on the dark web first.

209. By the time that an individual's stolen PHI and PII makes it to an auction or online sale site, it usually has already been used, sold for higher prices, or have been broken up into pieces of the data. These secondary sites are essentially scalpers. First copies usually sell for much more and are bartered in forums on the dark web. Most original hackers do not sell the majority of the data for the first one to two years. The individual's PHI and PII— such as PHI and PII belonging to Plaintiff Lee — is now being sold by thieves to thieves on the dark web.

210. Considering the geographic distribution of Plaintiffs and the inclusion of multiple Plaintiffs' PHI and PII in one sample database, it can be reasonably assumed that the data likely came from the same source data breach.

211. Plaintiff Lee will now have to freeze his credit and enroll in credit and identity monitoring to combat the long-lasting ramifications of the Healthcare Data Breach.

212. Plaintiff Lee's need for extensive credit monitoring is a reasonably certain

consequence of Defendants' breach of their duties, as described further below.

213. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Lee has experienced a dramatic increase in spam calls, including individuals purporting to be realtors.

214. Plaintiff Lee had an expectation that his PHI and PII would not be disclosed.

215. Plaintiff Lee has spent at least $500.00-$1000.00 responding to the Healthcare Data Breach.

216. Plaintiff Lee has spent at least 24 hours responding to the Healthcare Data Breach.

217. Plaintiff Lee did not enroll in the credit monitoring offered by American Anesthesiology as a result of the Healthcare Data Breach. He did not trust American Anesthesiology and did not want to take its advice since it had already exposed his identity.

218. Had Plaintiff Lee been informed his PHI and PII could be exposed to unauthorized third parties, he would have tried to seek medical treatment from a different provider.

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

220. Plaintiff Chelsea Cohen ("Plaintiff Cohen") is the parent and legal guardian of A.H., and at all times mentioned herein Plaintiff was an individual citizen of the State of Maryland residing in Maryland.

221. In or around December 2020, Plaintiff Cohen received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying her that her child's PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that her child's name, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment

information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by her child's provider) may have been involved.

222. As a result of the Healthcare Data Breach notice, Plaintiff Cohen spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts on behalf of herself and A.H. This time has been lost forever and cannot be recaptured.

223. Additionally, Plaintiff Cohen is very careful about sharing A.H.'s sensitive PHI and PII. She has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

224. Plaintiff Cohen stores any documents containing A.H.'s sensitive PHI and PII in a safe and secure location or destroys the documents.

225. Plaintiff Cohen, on behalf of A.H., has suffered actual injury in the form of damages to and diminution in the value of A.H.'s PHI and PII: forms of intangible property that Plaintiff Cohen entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

226. Plaintiff Cohen, on behalf of A.H., suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of A.H.'s privacy.

227. Plaintiff Cohen, on behalf of A.H., has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from A.H.'s PHI and PII, especially the child's Social Security number, in combination with the child's name, being placed in the hands of unauthorized third parties and possibly criminals.

228. Plaintiff Cohen has a continuing interest in ensuring that A.H.'s PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

229. Plaintiff Cohen, on behalf of her child, has suffered actual injury from having her child's PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of her bargain with Defendants.

230. PII belonging to A.H., Plaintiff Cohen's child, including the child's Social Security number, has been found available for purchase on the dark web.

231. The compromise of the child's PHI and PII through its publication has drastically increased A.H.'s risk of identity theft. It is now a matter of when, not if, the child will have additional damages and problems.

232. To the best of Plaintiff Cohen's knowledge, A.H. has never been involved in another data breach. As such, and given the temporal relationship, it may be reasonably assumed that the offer of sale of A.H.'s PHI and PII is tied to the Healthcare Data Breach.

233. Because A.H.'s PHI and PII was found on a popular marketplace, it can be assumed that the child's PHI and PII has already been used and sold for higher prices in smaller forums on the dark web first.

234. By the time that an individual's stolen PHI and PII makes it to an auction or online sale site, it usually has already been used, sold for higher prices, or have been broken up into pieces of the data. These secondary sites are essentially scalpers. First copies usually sell for much more and are bartered in forums on the dark web. Most original hackers do not sell the majority of the data for the first one to two years. The individual's PHI and PII— such as PHI and PII belonging to A.H. — is now being sold by thieves to thieves on the dark web.

235. Considering the geographic distribution of Plaintiffs and the inclusion of multiple Plaintiffs' PHI and PII in one sample database, it can be reasonably assumed that the data likely came from the same source data breach.

236. Plaintiff Cohen, on behalf of A.H., will now have to freeze A.H.'s credit and enroll in credit and identity monitoring to combat the long-lasting ramifications of the Healthcare Data Breach.

237. A.H.'s need for extensive credit monitoring is a reasonably certain consequence of Defendants' breach of their duties, as described further below.

238. Defendants did not offer Plaintiff Cohen or her child credit or identity monitoring.

239. As a direct and proximate result of the Healthcare Data Breach, Plaintiff Cohen enrolled in credit monitoring.

240. Plaintiff Cohen had an expectation that her child's PHI and PII would not be disclosed.

241. As a result of the Healthcare Data Breach, Plaintiff Cohen, on behalf of her child, will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

242. Plaintiff Chaya Clark ("Plaintiff Clark") is the parent and legal guardian of three minor children (J.C., J.C., and E.M., hereinafter the "children" or "three children") who are patients of, and received, medical services from, Defendants. Plaintiff Clark and her minor children are residents and citizens of the State of South Carolina.

243. In or around January 2021, Plaintiff Clark received a "Notice of Security Event" dated December 16, 2020, from Defendant Mednax notifying her that her children's PHI and PII may have been accessed as a result of the Healthcare Data Breach of Defendant's computer systems that took place between June 17, 2020 and June 22, 2020. The "Notice of Security Event" specifically stated that her children's names, guarantor name, address, email address, and dates of birth, health insurance information (payor name, payor contract dates, policy information

including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Records Numbers), and billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by her children's provider) may have been involved.

244. As a result of the Healthcare Data Breach notice, Plaintiff Clark spent time dealing with the consequences of the Healthcare Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Event, exploring credit monitoring and identity theft insurance options, and self-monitoring accounts on behalf of herself and her children. This time has been lost forever and cannot be recaptured.

245. Additionally, Plaintiff Clark is very careful about sharing her children's sensitive PII/PHI. She has never knowingly transmitted unencrypted sensitive PHI and PII over the internet or any other unsecured source.

246. Plaintiff Clark stores any documents containing her children's sensitive PHI and PII in a safe and secure location or destroys the documents.

247. Plaintiff Clark, on behalf of her children, has suffered actual injury in the form of damages to and diminution in the value of her children's PHI and PII: forms of intangible property that Plaintiff Clark entrusted to Defendants for the purpose of obtaining services from Defendants, that were compromised in and as a result of the Healthcare Data Breach.

248. Plaintiff Clark, on behalf of her children, suffered lost time, annoyance, interference, and inconvenience as a result of the Healthcare Data Breach and has anxiety and increased concerns for the loss of her children's privacy.

249. Plaintiff Clark, on behalf of her children, has suffered present and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her

children's PII, especially the children's Social Security numbers, in combination with the children's names, being placed in the hands of unauthorized third parties and possibly criminals.

250. Plaintiff Clark has a continuing interest in ensuring that her children's PHI and PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

251. Plaintiff Clark, on behalf of her children, has suffered actual injury from having her children's PHI and PII exposed as a result of the Healthcare Data Breach including, but not limited to: (a) loss of privacy; (b) present and impending injury arising from the increased risk of fraud and identity theft; and (c) loss of the benefit of her bargain with Defendants.

252. PII belonging to Plaintiff Clark's three children, including the children's Social Security numbers, have been found available for purchase on the dark web.

253. The compromise of the children's PHI and PII through their publication has drastically increased the children's risk of identity theft. It is now a matter of when, not if, the children will have additional damages and problems.

254. To the best of Plaintiff Clark's knowledge, her three children have never been involved in another data breach. As such, and given the temporal relationship, it may be reasonably assumed that the offer of sale of the three children's PHI and PII is tied to the Healthcare Data Breach.

255. Because the three children's PHI and PII was found on a popular marketplace, it can be assumed that the children's PHI and PII has already been used and sold for higher prices in smaller forums on the dark web first.

256. By the time that an individual's stolen PHI and PII makes it to an auction or online sale site, it usually has already been used, sold for higher prices, or have been broken up into pieces of the data. These secondary sites are essentially scalpers. First copies usually sell for much more and are bartered in forums on the dark web. Most original hackers do not sell the majority of the data for the first one to two years. The individual's PHI and PII— such as PHI and PII belonging to Plaintiff Clark's three children — is now being sold by thieves to thieves on the dark web.

257. Considering the geographic distribution of Plaintiffs and the inclusion of multiple Plaintiffs' PHI and PII in one sample database, it can be reasonably assumed that the data likely came from the same source data breach.

258. Plaintiff Clark, on behalf of her three minor children, will now have to freeze their credit and enroll in credit and identity monitoring to combat the long-lasting ramifications of the Healthcare Data Breach.

259. The children's need for extensive credit monitoring is a reasonably certain consequence of Defendants' breach of their duties, as described further below.

260. Defendants did not offer Plaintiff Clark or her children credit or identity monitoring.

261. Plaintiff Clark had an expectation that her children's PHI and PII would not be disclosed.

262. As a result of the Healthcare Data Breach, Plaintiff Clark, on behalf of her children, will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

263. Defendant Mednax is a healthcare services provider with its principal place of business at 1301 Concord Terrace, Sunrise, FL 33323.

264. Defendant Pediatrix is a Mednax company and healthcare services provider with its principal place of business at 1301 Concord Terrace, Sunrise, FL 33323.

265. Defendant American Anesthesiology, Inc. ("Defendant AA") is a former Mednax company and is now owned by North American Partners in Anesthesia and is a healthcare services provider with its principal place of business at 68 South Service Rd., Suite 350, Melville, NY.

IV. BACKGROUND FACTS

A. Defendants' Business

266. Defendants are a national healthcare services partner and provider offering

newborn, anesthesia, maternal-fetal, radiology and teleradiology, pediatric cardiology, and other pediatric subspecialty care services in 39 states and Puerto Rico.[1]

267. In addition, Defendants operate a consulting services branch that provides administrative services and solutions to optimize performance, resources and capacity within hospitals and healthcare providers.[2]

268. In 2019, Defendant Mednax reported revenues of over $3.5 billion and had 4,327 physicians within its network including Defendant Pediatrix and Defendant AA.[3]

269. In the ordinary course of receiving treatment and health care services from Defendants, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Driver's license numbers;
- Tribal identification numbers;
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Beneficiary information;

[1] *2019 Annual Report*, Mednax Health Solutions Partner (2019), at 3. Available at https://mednax.gcs-web.com/static-files/79b9289b-61f7-41a9-9394-81b99c902169 (last visited Jan. 4, 2021).
[2] *Id* at 7.
[3] *Id* at Selected Highlights.

- Provider information;
- Address, phone number, and email address, and;
- Health insurance information.

270. Defendants and their affiliated partners ("Agents") provide each of their customers with a HIPAA compliant Notice of its Privacy Practices (the "Privacy Notice") in respect to how they handle customers' sensitive information.[4]

271. The Privacy Notice provides, in relevant part, the following:

> I. WHO WE ARE
>
> This Notice of Privacy Practices ("Notice") describes the privacy practices of MEDNAX Services, Inc., and its affiliated entities, its physicians, nurses and other personnel ("we" or "us"). It applies to services furnished to you at all of the offices where we provide services.
>
> II. OUR PRIVACY OBLIGATIONS
>
> **We are required by law to maintain the privacy of your health information** ("Protected Health Information" or "PHI") and to provide you with this Notice of our legal duties and privacy practices with respect to your PHI. **We are also obligated to notify you following a breach of unsecured PHI.** When we use or disclose your PHI, we are required to abide by the terms of this Notice (or other notice in effect at the time of the use or disclosure).

Id. (emphasis added).

272. Thus, because of the highly sensitive and personal nature of the information Defendants acquire and store with respect to its patients, Defendants promise in their Privacy Notice to, among other things, maintain the privacy of patients' health information.[5]

273. As a condition of receiving medical care and treatment at Defendants' Agents'

[4] *See Notice of Privacy Practices*, Mednax, https://www.mednax.com/notice-of-privacy-practices/ (last visited Jan. 5, 2021).
[5] *Id*.

facilities, Defendants require that their patients entrust them with highly sensitive personal information.

274. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

275. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

276. Plaintiffs and the Class Members relied on Defendants to keep their Protected Health Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

277. Defendants are required to maintain the strictest privacy and confidentiality of Plaintiffs and the proposed Class Members' medical records and other PHI and PII.

278. Pediatrix outlines its Duties in its Notice of Privacy Practices online at the following site: https://www.mednax.com/policy-statement/.

B. Value of Personally Identifiable Information

279. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit

[6] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 22, 2021).

card number can sell for $5 to $110 on the dark web.[7] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[8]

280. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> 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.[9]

281. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[7] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 22, 2021).

[8] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 22, 2021).

[9] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 22, 2021).

282. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[10]

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

284. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[11]

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

286. The fraudulent activity resulting from the Healthcare Data Breach may not come to light for years.

---

[10] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed June 21, 2021).

[11] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed June 21, 2021).

287. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[12]

288. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

290. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendant's computer systems, amounting to more than one million individuals detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

291. Defendants failed to offer the majority of the Plaintiffs any type of credit monitoring. Given the large number of Plaintiffs' PII that has been found available for purchase

[12] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed June 15, 2021).

on the dark web, Defendants' lack of relief provided to Plaintiffs and Class Members is both negligent and alarming.

292. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

293. Defendants' wrongful actions and/or inaction and the resulting Breach have also placed Plaintiffs and the other Class Members at a present, immediate, and continuing increased risk of identity theft, identity fraud[13] and medical fraud.

294. Identity theft occurs when someone uses an individual's PHI and PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, Fighting Back against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/ about-identity-theft.html (last visited Jan. 18, 2013). The Federal Trade Commission estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

295. The Federal Trade Commission correctly sets forth that "Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit." *Id.*

[13] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia,* credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

296. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PHI and PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

297. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[14] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[15]

298. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud

[14] *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

[15] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35-38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology,* cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

299. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html). Thus, a person whose PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

300. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems; because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

301. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in

medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

302. The Healthcare Data Breach substantially increased Plaintiffs' and the other Class Members' risk of being victimized by "phishing." "Phishing" is an attempt to acquire information (and sometimes, indirectly, money), such as usernames, passwords and credit card details by masquerading as a trustworthy entity through an electronic communication. *See* http://www.onguardonline.gov/articles/0003-phishing (last visited Jan. 18, 2013).

303. Communications purporting to be from popular social websites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and often directs users to enter details at a fake website that looks and feels almost identical to the legitimate one. When criminals have access to PHI and PII from a large group of similarly situated victims, it is much more feasible to develop a believable phishing spoof email. They can then get this group of victims to reveal additional private information, such as credit cards, bank accounts, and the like.

C. Defendants had an Obligation to Protect Personal and Medical Information under Federal Law and the Applicable Standard of Care

304. Certain allegations are made upon information and belief.

305. Defendants were entrusted by their patients with their patients' most personal and private information.

306. Defendants had a duty to their patients to protect them from wrongful and unauthorized disclosures of their patients' PHI and PII.

307. As healthcare providers, Defendants are required to train and supervise their employees regarding the policies and procedures as well as the State and Federal laws for safeguarding patient information.

308. Defendants are covered entities pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendants must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

309. Defendants are covered entities pursuant to the Health Information Technology Act ("HITECH")[16]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

310. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

311. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

312. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

[16] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

313. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

314. HIPAA's Security Rule requires Defendants to do the following:

a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d) Ensure compliance by their workforce.

315. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

316. HIPAA also requires Defendants 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." 45 C.F.R. § 164.312(a)(1).

317. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[17]

318. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

319. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

320. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or
>
> (iii) Transmitted or maintained in any other form or medium.[18]

321. HIPAA and HITECH obligated Defendants to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that

[17] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).
[18] 45 C.F.R. § 160.103

had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

322. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

323. HIPAA further obligated Defendants to ensure that their workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

324. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[19] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good

[19] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[20]

325. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and
>
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[21]

326. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

327. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their rolls in facility security.

328. Defendants failed to provide proper notice to Plaintiffs of the disclosure.

---

[20]https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

[21] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

329. Defendants failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

330. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Healthcare Data Breach, the criminal(s) and/or their customers now have Plaintiffs' and the other Class Members' compromised PHI and PII.

331. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendants' wrongful actions and/or inaction and the resulting Healthcare Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud[22] and medical fraud.

332. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

[22]According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia,* credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

D. Defendants were on Notice of Cyber Attack Threats in the Healthcare Industry and of the Inadequacy of their Data Security

333. Defendants were on notice that companies in the healthcare industry were targets for cyberattacks.

334. Defendants were on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[23]

335. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[24]

336. As implied by the above quote from the AMA, stolen Personal and Medical Information can be used to interrupt important medical services themselves. This is an imminent and certainly impending risk for Plaintiffs and Class members.

---

[23] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[24] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

337. Defendants were on notice that the federal government has been concerned about healthcare company data encryption. Defendants knew they kept protected health information in their email accounts, and yet it appears Defendants did not encrypt these email accounts.

338. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[25]

339. As covered entities or business associates under HIPAA, Defendants should have known about their weakness toward email-related threats and sought better protection for the Personal and Medical Information accumulating in their employees' business email accounts.

340. In the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"[26]

---

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

[26]Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results* (Mar. 27, 2019),

341. The report from Proofpoint was published March 27, 2019, and summarized findings of recent healthcare industry cyber threat surveys and recounted good, common-sense steps that the targeted healthcare companies should follow to prevent email-related cyberattacks.

342. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's ongoing training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[27]

343. "Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment."[28] The fake link will typically mimic a familiar website and require the input of credentials. Once inputted, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware.[29] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[30]

344. Phishing attacks are generally preventable with the implementation of a variety of

---

https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results.

[27] *Id.*

[28] Josh Fruhlinger, *What is Phishing? How This Cyber-Attack Works and How to Prevent It*, CSO Online (Sept. 4, 2020), https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (last visited Jan. 5, 2021).

[29] *Id.*

[30] *What is Phishing?*, Malwarebytes, https://www.malwarebytes.com/phishing/ (last visited Jan. 5, 2021).

proactive measures such as purchasing and using some sort of commonly available anti-malware security software (such as the ubiquitous Malwarebites). Most cybersecurity tools have the ability to detect when a link or an attachment is not what it seems.[31]

345. Other proactive measures include, for example, sandboxing inbound e-mail (*i.e.*, an automated process that segregates e-mail with attachments and links to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely), inspecting and analyzing web traffic, penetration testing (which can be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents), and employee education.

346. ProtonMail Technologies publishes a guide for IT Security to small businesses (i.e., companies without the heightened standard of care applicable in the healthcare industry). In its 2019 guide, ProtonMail dedicates a full chapter of its e-book guide to the danger of phishing and ways to prevent a small business from falling prey to it. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[32]

347. The guidance that ProtonMail provides non-healthcare industry small businesses is likely still not adequate for companies like MEDNAX and Pediatrix, with the heightened

[31] *Id.*

[32] *The ProtonMail Guide to IT Security for Small Businesses*, PROTONMAIL (2019), available at https://protonmail.com/it-security-complete-guide-for-businesses.

healthcare standard of care based on HIPAA, CMIA, and the increased danger from the sensitivity and wealth of Personal and Medical Information they retain However, ProtonMail's guidance is informative for showing how inadequately Defendants protected the Personal and Medical Information of the Plaintiffs and the Class. ProofPoint lists numerous tools under the heading, "How to Prevent Phishing":

a) **Training:** "Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. *This training should be continuous as well. . . .*"

b) **Limit Public Information:** "Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories . . . ."

c) **Carefully check emails:** "First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the 'From' address to see if it is odd . . . . If an email looks suspicious, employees should report it."

d) **Beware of links and attachments:** "Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment…"

e) **Do not automatically download remote content:** "Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it."

f) **Hover over hyperlinks:** "Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL." [Proofpoint notes that there are tools online available for retrieving original URLs from shortened ones.]

g) **If in doubt, investigate:** "Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email."

h) **Take preventative measures:** "Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims to come from, making it easier to identify potential phishing attacks."[33]

348. As mentioned, these are basic, common-sense email security measures that every business, whether in healthcare or not, should be doing. By adequately taking these common-sense solutions, Defendants could have prevented the Healthcare Data Breach from occurring.

E. Defendants Could Have Prevented the Healthcare Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' Personal and Medical Information

349. Data breaches are preventable.[34] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate

[33] *Id.*

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

security solutions."[35] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[36]

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

351. Defendants required Plaintiffs and Class members to surrender their Personal and Medical Information – including but not limited to their names, addresses, Social Security numbers, medical information, and health insurance information – and were entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such Personal and Medical Information.

352. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Healthcare Data Breach, starting with Defendants' failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiffs' and Class members' Personal and Medical Information.

353. Defendants maintained the Personal and Medical Information in a reckless manner. In particular, the Personal and Medical Information was maintained and/or exchanged, unencrypted, in Microsoft Office 365 business email accounts that were maintained in a condition vulnerable to cyberattacks.

[35] *Id.* at 17.
[36] *Id.* at 28.
[37] *Id.*

354. Defendants knew, or reasonably should have known, of the importance of safeguarding Personal and Medical Information and of the foreseeable consequences that would occur if Plaintiffs' and Class members' Personal and Medical Information was stolen, including the significant costs that would be placed on Plaintiffs and Class members as a result of a breach.

355. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class members' Personal and Medical Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure Plaintiffs' and Class members' Personal and Medical Information from those risks left that information in a dangerous condition.

356. Defendants disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequate robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' Personal and Medical Information; (iii) failing to take standard and reasonably available steps to prevent the Healthcare Data Breach; (iv) concealing the existence and extent of the Healthcare Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Healthcare Data Breach.

V. THE UNAUTHORIZED DISCLOSURE

357. On or about June 19, 2020, Defendants discovered that unauthorized third-party hackers gained access to certain Microsoft Office 365-hosted business email accounts through a successful phishing event.

358. Despite discovering the infiltration on June 19, 2020, which began on June 17, 2020, the infiltration was allowed to continue through June 22, 2020.

359. Defendants began filing with various state Attorneys General sample "Notice of Data Security Incident" letters that mirrored the language of the Notice sent to Plaintiffs and Class Members.

360. Plaintiffs' and Class Members' unencrypted personal information was acquired by an unauthorized person or persons as a result of the Healthcare Data Breach.

361. Pursuant to their notification to the various governmental entities, Defendants reasonably believe Plaintiffs' and Class Members' unencrypted personal information was acquired by an unauthorized person as a result of the Healthcare Data Breach.

362. The disclosure of the PHI and PII at issue was a result of the Defendants' inadequate safety and security protocols governing PHI and PII.

363. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiffs' and the other Class Members' names, dates of birth, medical records, patient account numbers, health insurance information, Social Security numbers, and/or limited treatment or clinical information, such as diagnosis, provider names, dates of service, and other medical information.

364. The security, confidentiality, or integrity of Plaintiffs' and Class Members' unencrypted personal information was compromised as a result of the Breach.

365. Defendants reasonably believe the security, confidentiality, or integrity of Plaintiffs' and Class Members' unencrypted personal information was compromised as a result of the Healthcare Data Breach.

366. Plaintiffs' and Class Members' unencrypted personal information that was acquired by an unauthorized person as a result of the Healthcare Data Breach was viewed by unauthorized persons.

367. Defendants reasonably believe Plaintiffs' and Class Members' unencrypted personal information that was acquired by an unauthorized person as a result of the Healthcare Data Breach was viewed by unauthorized persons.

368. It is reasonable to infer that Plaintiffs' and Class Members' unencrypted personal information that was acquired by an unauthorized person or persons as a result of the Healthcare Data Breach was viewed by unauthorized persons.

369. It should be presumed that Plaintiffs' and Class members' unencrypted personal information that was acquired by an unauthorized person or persons as a result of the Healthcare Data Breach was viewed by unauthorized persons.

370. It is reasonable for recipients, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

A. The U.S. Department of Health and Human Services Breach Report

371. A breach report regarding the Healthcare Data Breach filed by Defendants with the Secretary of the U.S. Department of Health and Human Services states that 1,290,670 individuals were impacted by the Healthcare Data Breach (the "Breach Report"). The Breach Report also characterizes the Healthcare Data Breach as a "hacking/IT incident" and further indicates that the breached information was accessed through email.

372. The Breach Report was filed in accordance with 45 CFR § 164.408(a).

373. Plaintiffs' and Class Members' medical information is Protected Health Information as defined by 45 CFR § 160.103.

374. Pursuant to 45 CFR § 164.408(a), breach reports are filed with the Secretary of the U.S. Department of Health and Human Services "following the discovery of a breach of unsecured protected health information."

375. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

376. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

377. Plaintiffs' and Class Members' medical information is unsecured Protected Health Information as defined by 45 CFR § 164.402.

378. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Healthcare Data Breach.

379. Defendants reasonably believe Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Healthcare Data Breach.

380. Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a

result of the Healthcare Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized person or persons.

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

382. Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Healthcare Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized person or persons.

383. Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized person or persons in a manner not permitted under 45 CFR Subpart E as a result of the Healthcare Data Breach.

384. Defendants reasonably believe Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Healthcare Data Breach.

385. It is reasonable to infer that Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Healthcare Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized person or persons.

386. It should be presumed that unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E, and which was

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

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

388. Based upon Defendants' post disclosure ongoing duty, it is reasonable to assume that Defendants believe that their patients are at risk for future identity theft as warnings of possible identity theft was included in the Breach Notice.

B. Defendants' Failed Response

389. It is apparent from the Notice sent to Plaintiffs and the Class and from the sample "Notice of Data Security Incident" letters sent to state Attorneys General that the PHI contained within these Office 365 accounts was not encrypted.

390. Following the phishing event, Defendants began working with a forensic firm to investigate the Healthcare Data Breach. Based upon the investigation, the hackers were able to access certain business email accounts between the dates of June 17, 2020 and June 22, 2020 where Plaintiffs' and Class members' PHI and PII was being held, unencrypted and unprotected.

391. Defendants have also reported a subsequent breach that took place from July 2, 2020 to July 3, 2020.

392. Upon information and belief, the unauthorized third-party gained access to the PHI and PII and has engaged in (and will continue to engage in) misuse of the PHI and PII, including marketing and selling Plaintiffs' and Class members' PHI and PII on the dark web.

393. Despite knowing that over 1 million patients across the nation were in danger as a result of the Healthcare Data Breach, Defendants did nothing to warn Plaintiffs or Class members until six months after learning of the Breach – an unreasonable amount of time under any objective standard and a violation of their obligations under federal statutes.

394. Defendants chose to complete their investigation and develop a list of talking points before giving Plaintiffs and Class Members the information they needed to protect themselves against further privacy violations, loss of medical expenses, fraud and identity theft.

395. In spite of the severity of the Healthcare Data Breach, Defendants have done very little to protect Plaintiffs and the Class, which is obvious by the subsequent data breach in July 2020 and the lack of assistance offered to Plaintiffs and the Class. For example, in the Notice, Defendants only encourage victims "to carefully review credit reports and statements sent from providers as well as [victims'] insurance compan[ies] to ensure that all account activity is valid." The Notice also mentions a free credit reporting service Plaintiffs and Class Members, many of which are children, can contact but fails to offer any free identity theft monitoring service to a majority of the Class.[38]

396. In effect, Defendants are shirking their responsibility for the harm and increased risk of harm they have caused Plaintiffs and members of the Class, including the distress and financial burdens the Healthcare Data Breach has placed upon the shoulders of the Healthcare Data Breach victims.

[38] For a very limited number of patients or guarantors whose Social Security numbers, driver's license numbers, non-resident and alien registration numbers, and/or financial account information was compromised, Defendants arranged to offer complimentary identity monitoring services. *See* https://emailevent.kroll.com/ (last accessed Jan. 13, 2021).

397. Defendants failed to adequately safeguard Plaintiffs' and Class Members' PHI and PII, allowing cyber criminals to access this wealth of priceless information for nearly six months before warning the victims to be on the lookout, and offer them no remedy or relief.

398. Defendants failed to spend sufficient resources on monitoring external incoming emails and training their employees to identify email-borne threats and defend against them.

399. Defendants had obligations created by state consumer protection law, reasonable industry standards, common law, state statutory law, and their assurances and representations to their patients to keep patients' PHI and PII confidential and to protect such PHI and PII from unauthorized access.

400. Plaintiffs and Class Members were required to provide their PHI and PII to Defendants with the reasonable expectation and mutual understanding that they would comply with their obligations to keep such information confidential and secure from unauthorized access.

401. The stolen PHI and PII at issue has great value to the hackers, due to the large number of individuals affected and the fact that medical treatment and diagnosis information as well as health insurance information, dates of birth, names, addresses and Social Security numbers were part of the information that was compromised.

C. Cyber Criminals Will Use Plaintiffs' and Class Members' Personal and Medical Information to Defraud Them

402. Plaintiffs and Class Members' PHI and PII is of great value to hackers and cyber criminals, and the data stolen in the Healthcare Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

403. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[39] For example, with the PHI and PII stolen in the Healthcare Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[40] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

404. PHI and PII are such valuable commodities to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[41]

405. For example, it is believed that certain Personal and Medical Information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma.[42]

406. This was a financially motivated Healthcare Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off of the sale of Plaintiffs' and the Class Members' PHI and PII on the dark web. The PHI and PII exposed in this Healthcare Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

407. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[43]

---

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

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

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

[42] *See https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

[43]Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017),

408. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[44]

409. For instance, with a stolen Social Security number, which is part of the PHI and PII compromised in the Healthcare Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[45] Identity thieves can also use the information stolen from Plaintiffs and Class Members to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

410. Medical identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[46]

411. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[47]

---

https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[44] *Data Breaches Are Frequent*, *supra* note 11.

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

[46] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

[47] *Id.*

412. As indicated by James Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where [personal health information] can go from $20 say up to—we've seen $60 or $70 [(referring to prices on dark web marketplaces)]."[48] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[49]

413. If cyber criminals manage to steal financial information, health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants have exposed the Plaintiffs and Class Members.

414. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[50] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[51]

415. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[52]

---

[48] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowedge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[49] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[50] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[51] *Id.*; *see also Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

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

416. The danger of identity theft is compounded when, like here, a minor's PHI and PII are compromised, because minors typically have no credit reports to monitor. Thus, it can be difficult to monitor because a minor cannot simply place an alert on their credit report or "freeze" their credit report when no credit report exists.

417. Defendants' failure to offer identity monitoring to a majority of the Class, including to Plaintiffs, is egregious. Moreover, Defendants' offer of one year of identity theft monitoring to only a limited number of Class Members is, in and of itself, woefully inadequate, as the worst is yet to come.

418. With this Healthcare Data Breach, it is likely that identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

419. Victims of the Healthcare Data Breach, like Plaintiffs and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Healthcare Data Breach.[53]

420. In fact, as a direct and proximate result of the Healthcare Data Breach, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Healthcare Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

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

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

a. Trespass, damage to, and theft of their personal property including PHI and PII;

b. Improper disclosure of their PHI and PII;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PHI and PII being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendants untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Healthcare Data Breach;

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

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

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

j. Damage to their credit due to fraudulent use of their PHI and PII; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

422. Moreover, Plaintiffs and Class members have an interest in ensuring that their information, which remains in the possession of Defendants, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiffs' and Class members' PHI and PII.

423. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendants have caused them but, given the kind of PHI and PII Defendants made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their PHI and PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the

rest of their lives. Some, including babies and young children, may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[54]

424. None of this should have happened. The Healthcare Data Breach was preventable.

VI. THE BREACH HARMED AND CAUSED DAMAGE TO PLAINTIFFS AND THE CLASS MEMBERS

425. Defendants flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiffs' and the other Class Members' prior written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal company standards.

426. Defendants flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons.

427. Upon information and belief, Defendants flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PHI and PII wrongfully disclosed in the Breach.

428. Defendants flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and the other Class Members' PHI and PII to protect against anticipated threats to the security or integrity of such information. Defendants' unwillingness or inability to establish and maintain the proper information security procedures and controls is an

[54] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

429. The actual harm and adverse effects to Plaintiffs and the other Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendants' above wrongful actions and/or inaction and the resulting Healthcare Data Breach requires Plaintiffs and the other Class Members to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost. Plaintiffs and the other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

430. Victims and potential victims of identity theft, identity fraud and/or medical fraud—such as Plaintiffs and the other Class Members—typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. *See Defend: Recover from Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html; *Fight Identity Theft*, www.fightidentitytheft.com. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. *Id*. at 6.

431. Other statistical analyses are in accord. The GAO found that identity thieves use PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating

and finances. Moreover, unlike other PHI and PII, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

432. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiffs' and the other Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Healthcare Data Breach, Plaintiffs and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iii) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Healthcare Data Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Healthcare Data Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Healthcare Data Breach, (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not, and (vii) emotional distress.

VII. CLASS ACTION ALLEGATIONS

433. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

434. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiffs asserts all claims on behalf of the Nationwide Class, defined as follows:

> All persons residing in the United States whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.

435. Alternatively, Plaintiffs propose the following alternative classes by state, as follows:

> Arizona Subclass: All residents of Arizona whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> California Subclass: All residents of California whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> Florida Subclass: All residents of Florida whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> Maryland Subclass: All residents of Maryland whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> Missouri Subclass: All residents of Missouri whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> New York Subclass: All residents of New York whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> North Carolina Subclass: All residents of North Carolina whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> Oklahoma Subclass: All residents of Oklahoma whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> South Carolina Subclass: All residents of South Carolina whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> Texas Subclass: All residents of Texas whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.
>
> Virginia Subclass: All residents of Virginia whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June

and July 2020.

Washington Subclass: All residents of Washington whose PHI and PII was compromised as a result of the MEDNAX Breach which occurred in June and July 2020.

436. Also, in the alternative, Plaintiffs request additional subclasses as necessary based on the types of Personal and Medical Information that were compromised.

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

438. Plaintiffs reserve the right to amend the above definitions or to propose alternative or additional subclasses in subsequent pleadings and motions for class certification.

439. The proposed Nationwide Class or, alternatively, the separate Statewide Subclasses (collectively referred to herein as the "Class" unless otherwise specified) meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

440. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

441. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendants' uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive Personal and Medical Information compromised in the same way by the same conduct of Defendants.

442. **Adequacy:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class and proposed Subclasses that they seek to

represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

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

444. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants failed to adequately safeguard Plaintiffs' and the Class's PHI and PII;

c. Whether Defendants' email and computer systems and data security practices used to protect Plaintiffs' and Class members' PHI and PII violated the FTC Act, CMIA, and/or state laws and/or Defendants' other duties discussed herein;

d. Whether Defendants owed a duty to Plaintiffs and the Class to adequately protect their PHI and PII, and whether they breached this duty;

e. Whether Defendants knew or should have known that their computer and network security systems and business email accounts were vulnerable to a breach of their patients' PHI and PII;

f. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Healthcare Data Breach;

g. Whether Defendants breached contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PHI and PII;

h. Whether Defendants failed to adequately respond to the Healthcare Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

i. Whether Defendants continue to breach duties to Plaintiffs and the Class;

j. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendants' negligent actions or failures to act;

k. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class and the general public, including but not limited to an order:

    a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

    b. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

d. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

e. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

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

g. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

h. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

i. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

j. requiring Defendants to conduct regular database scanning and securing checks;

k. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

l. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

m. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

n. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

o. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their

confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

p. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

m. Whether Defendants' actions alleged herein constitute gross negligence; and

n. Whether Plaintiffs and Class members are entitled to punitive damages.

VIII. CAUSES OF ACTION

COUNT I

BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

445. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

446. As described above, Defendants made promises and representations to Plaintiffs and the Class that they would comply with applicable laws and industry best practices.

447. These promises and representations became a part of the contract between Defendants and Plaintiffs and the Class.

448. While Defendants had discretion in the specifics of how they met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

449. Defendants breached this implied covenant when they engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations, and when they engaged in unlawful practices under HIPAA, HITECH and other state personal and medical privacy laws and consumer protection laws. These acts and omissions included: representing that they would maintain adequate data privacy and security practices and procedures to safeguard the PHI and PII from unauthorized disclosures, releases, breaches, and theft; omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class' PHI and PII; and failing to disclose to the Class at the time they provided their PHI and PII to them that Defendants' data security systems and protocols, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

450. Plaintiffs and Class members did all or substantially all the significant things that the contract required them to do.

451. Likewise, all conditions required for Defendants' performance were met.

452. Defendants' acts and omissions unfairly interfered with Plaintiffs' and Class Members' rights to receive the full benefit of their contracts.

453. Plaintiffs and Class Members have been harmed by Defendants' breach of this implied covenant in the many ways described above, including overpayment for services, the purchase of identity theft monitoring services not provided by Defendants, imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Personal and Medical Information, and the attendant long-term time and expenses spent attempting to mitigate and insure against these risks.

454. Defendants are liable for this breach of these implied covenants, whether or not they are found to have breached any specific express contractual term.

455. Plaintiffs and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT II

VIOLATIONS OF STATE CONSUMER LAWS

456. The preceding factual statements and allegations are incorporated herein by reference.

457. State consumer protection statutes prohibit the use of any "deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce" …

458. An "unfair practice" is defined by consumer protection statutes, as any practice which:

(A) Either-

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

459. An unfair practice is defined provides that an "Unfair Practice in General" is

(1) An unfair practice is any practice which –

(A) Either –

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

460. An "Unfair Practice" is defined under state consumer protection laws that for any person in connection with the advertisement or sale of merchandise to violate the duty of good faith in solicitation, negotiation and performance, or in any manner fail to act in good faith.

461. Plaintiffs and Defendants are "persons" within the meaning of consumer protection statutes.

462. Defendants are "persons" under the state consumer protection statutes, which addresses how statutes are to be construed, provides that "the word 'person' may extend and be applied to bodies politic and corporate."

463. Merchandise is defined by the state consumer protections statutes, to include the providing of "services" and, therefore, encompasses Healthcare services. Healthcare services are a good.

464. Efforts to maintain the privacy and confidentiality of medical records are part of the healthcare services associated with a good.

465. Maintenance of medical records are "merchandise" within the meaning of state consumer protection statutes.

466. Plaintiffs' and the Class' goods and services purchased from Defendants were for "personal, family or household purposes" within the meaning of the state consumer protection statutes.

467. Defendants' unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Personal and Medical Information, which was a direct and proximate cause of the Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PHI and PII, including duties imposed by the FTC Act, HIPAA, and the CMIA;

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

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PHI and PII, including duties imposed by the FTC Act, HIPAA, HITECH and state consumer protection statutes and common law;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Class members' PHI and PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PHI and PII, including duties imposed by the FTC Act and HIPAA.

468. Defendants' representations and omissions were material because they were likely to deceive reasonable patient consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of their PHI and PII.

469. Defendants intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

470. Had Defendants disclosed to Plaintiffs and Class Members that their data security protocols and business emails (where highly sensitive personal data was exchanged and/or stored) were not secure and, thus, vulnerable to attack, Defendants would not have been able to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law.

471. The above unlawful practices and acts by Defendants were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial and continuous injury to Plaintiffs and Class Members.

472. Defendants acted intentionally, knowingly, and maliciously to violate state consumer protection statutes, including without limitation: Defendants' conduct described in this Consolidated Amended Complaint, including without limitation, Defendants' failure to maintain adequate computer systems and data security practices to safeguard patients' PHI and PII, Defendants' failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect patients' PHI and PII, Defendants' failure to provide timely and accurate notice to Plaintiffs and Class members of the material fact of Breach, and Defendants' continuing to accept PHI and PII from their patients knowing that there had been multiple breaches, constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation ofthe following state consumer statutes:

a. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

b. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *etseq*., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*;

c. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.201, *et seq*.;

d. The Maryland Consumer Protection Act, Md. Code Commercial Law, §13-301(1) and (2)(i), and (iv) and (9)(i), *et seq*;

e. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq*;

f. New York Business Law, N.Y. Gen. Bus. Law § 349(a);

g. The North Carolina Unfair and Deceptive Trade Practices, N.C. Gen. Stat §75-1.1, *et seq*;

h. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 751, *et seq.*; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 50, *et seq*;

i. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*;

j. The Texas Deceptive Trade Practices- Consumer Protection Act,V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq.*;

k. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*;

l. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq*.

473. As a direct and proximate result of Defendants' unlawful practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including time and expenses related to monitoring their credit and medical accounts; an increased, imminent risk of fraud and identity theft; and loss of value of their PHI and PII.

474. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

475. As set forth herein, Defendants' acts, practices and conduct violate the above-named consumer protection statutes in that, among other things, Defendants have used and/or continues to use unfair practices, concealment, suppression and/or omission of material facts in connection with the advertising, marketing, and offering for sale of services associated with healthcare services. Such acts offend the public policy established by state consumer protection statutes and constitute an "unfair practice" as that term is used in state consumer protection statutes.

476. Defendants' unfair, unlawful and deceptive acts, practices and conduct include: (1) representing to its patients that it will not disclose their sensitive personal health information to an unauthorized third party or parties; (2) failing to implement security measures such as securing the records in a safe place; and (3) failing to train personnel.

477. Defendants' conduct also violates the enabling regulations for the state consumer protection statutes because it: (1) offends public policy; (2) is unethical, oppressive and unscrupulous; (3) causes substantial injury to consumers; (4) it is not in good faith; (5) is unconscionable; and (6) is unlawful.

478. As a direct and proximate cause of Defendants' unfair and deceptive acts, Plaintiffs and members of the Class have suffered damages in that they (1) paid more for medical record privacy protections than they otherwise would have, and (2) paid for medical record privacy protections that they did not receive. In this respect, Plaintiffs and members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

479. Plaintiffs, on behalf of themselves and the Class, seek actual damages for all monies paid to the Defendants in violation of the state consumer protection statutes. In addition, Plaintiffs seek attorneys' fees.

COUNT III

VIOLATIONS OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code § 56, *et seq.*

480. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

481. Plaintiffs bring this Count against Defendants on behalf of the Class or, alternatively, the California Subclass.

482. Defendants are "provider[s] of healthcare," as defined in Cal. Civ. Code § 56.06, and are therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

483. Defendants are persons licensed under California under California's Business and Professions Code, Division 2. *See* Cal. Bus. Prof. Code § 4000, *et seq.* Defendants therefore qualify as "provider[s] of healthcare," under the CMIA.

484. Plaintiffs and the Class are "patients," as defined in CMIA, Cal. Civ. Code § 56.05(k) ("'Patient' means any natural person, whether or not still living, who received healthcare services from a provider of healthcare and to whom medical information pertains.").

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

486. Defendants' negligence resulted in the release of individually identifiable medical information pertaining to Plaintiffs and the Class to unauthorized persons and the breach of the

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

487. Defendants' computer and email systems and protocols did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A).

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

COUNT IV

BREACH OF IMPLIED CONTRACT

489. The preceding factual statements and allegations are incorporated herein by reference.

490. Plaintiffs and the other Class Members, as part of their agreement with Defendants, provided Defendants their PHI and PII.

491. In providing such PHI and PII, Plaintiffs and the other Class Members entered into an implied contract with Defendants, whereby Defendants became obligated to reasonably safeguard Plaintiffs' and the other Class members' PHI and PII.

492. Under the implied contract, Defendants were obligated to not only safeguard the PHI and PII, but also to provide Plaintiffs and Class Members with prompt, adequate notice of any Healthcare Data Breach or unauthorized access of said information.

493. Defendants breached the implied contract with Plaintiffs and the other Class

Members by failing to take reasonable measures to safeguard their PHI and PII.

494. Plaintiffs and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Healthcare Data Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Healthcare Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and (vi) the increased risk of identity theft. At the very least, Plaintiffs and Class Members are entitled to nominal damages.

COUNT V

NEGLIGENCE

495. The preceding factual statements and allegations are incorporated herein by reference.

496. Defendants owed a duty to Plaintiffs and the other Class Members to safeguard and protect their PHI and PII.

497. Defendants breached their duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII.

498. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class Members' PHI and PII would result in an unauthorized third party gaining access to such information for no lawful purpose.

499. Plaintiffs' and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Healthcare Data Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv)

out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Healthcare Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and (vi) the increased risk of identity theft. At the very least, Plaintiffs and the other Class members are entitled to nominal damages.

500. Defendants' wrongful actions and/or inaction and the resulting Healthcare Data Breach (as described above) constituted (and continue to constitute) negligence at common law.

COUNT VI

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

501. The preceding factual statements and allegations are incorporated herein by reference.

502. Plaintiffs' and the other Class Members' PHI and PII was (and continues to be) sensitive and personal private information.

503. By virtue of Defendants' failure to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII and the resulting Breach, Defendants wrongfully disseminated Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons.

504. Dissemination of Plaintiffs' and the other Class Members' PHI and PII is not of a legitimate public concern; publicity of their PHI and PII was, is and will continue to be offensive to Plaintiffs, the other Class Members and all reasonable people. The unlawful disclosure of same violates public norms.

505. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Healthcare Data Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket

expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Healthcare Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and (vi) the increased risk of identity theft. At the very least, Plaintiffs and the other Class Members are entitled to nominal damages.

506. Defendants' wrongful actions and/or inaction and the resulting Healthcare Data Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT VII

BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY

507. The preceding factual statements and allegations are incorporated herein by reference.

508. At all times relevant hereto, Defendants owed, and owes, a fiduciary duty to Plaintiffs and the proposed Class pursuant to common law to keep Plaintiffs' medical and other PHI and PII information confidential.

509. For example, the fiduciary duty of privacy imposed by Missouri law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530 which requires a covered entity, health care provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

510. Defendants breached their fiduciary duty to Plaintiffs by disclosing Plaintiffs' and the other Class Members' PHI and PII to unauthorized third parties.

511. As a direct result of Defendant's breach of fiduciary duty of confidentiality and the disclosure of Plaintiffs' confidential medical information, Plaintiffs and the proposed Class Members suffered damages.

512. Plaintiffs and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Healthcare Data Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Healthcare Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and (vi) the increased risk of identity theft. At the very least, Plaintiffs and the other Class Members are entitled to nominal damages.

513. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' confidential medical information, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, humiliation and loss of enjoyment of life.

COUNT VIII

NEGLIGENT TRAINING AND SUPERVISION

514. The preceding factual statements and allegations are incorporated herein by reference.

515. At all times relevant hereto, Defendants owed a duty to Plaintiffs and the Class to train and supervise employees to ensure they recognized the duties owed to their patients and their patients' parents and guardians.

516. Defendants breached their duty to Plaintiffs and the members of the Class by allowing their employees to fall victim to a phishing scam.

517. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' confidential medical information, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, humiliation and loss of enjoyment of life.

COUNT IX

NEGLIGENCE *PER SE*

518. Plaintiffs incorporate by reference and re-alleges all paragraphs previously alleged herein

519. Plaintiffs and proposed class members were under the medical care of the Defendants.

520. Defendants are covered entities for purposes of HIPAA and HITECH.

521. Plaintiffs and the proposed class members are members of the class HIPAA and HITECH were created to protect.

522. Plaintiffs' and proposed class member's private health information is the type of information HIPAA and HITECH were created to protect. HIPAA and HITECH were created to protect against the wrongful and unauthorized disclosure of an individual's health information.

523. Defendants gave protected medical information to an unauthorized third party or unauthorized third parties without the written consent or authorization of Plaintiffs.

524. Defendants gave protected medical information to unauthorized third parties without Plaintiffs' oral consent or written authorization.

525. The information disclosed to an unauthorized third party or unauthorized third parties included private health information about medical treatment.

526. Defendants' disclosure of the private health information of Plaintiffs without consent or authorization is a violation of HIPAA and HITECH and is negligence *per se*.

527. Alternatively, Defendants violated HIPAA and HITECH in that it did not reasonably safeguard the private health information of Plaintiffs from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements pursuant to HIPAA and HITECH including, but not limited to, 42 C.F.R. §§ 164.302-164.318, 45 C.F.R. § 164.500, *et seq*, and 42 U.S.C. §17902, and was therefore negligent *per se*.

528. As a direct result of Defendants' negligence, Plaintiffs suffered damages and injuries, including, without limitation, loss of the benefit of their bargain, a reduction in value of their private health information, loss of privacy, loss of medical expenses, loss of trust, loss of confidentiality, embarrassment, humiliation, emotional distress, and loss of enjoyment of life.

529. As a direct result of Defendants' negligence, Plaintiffs have a significantly increased risk of being future victims of identity theft relative to what would be the case in the absence of the Defendants' wrongful acts.

530. As a direct result of Defendants' negligence, future monitoring, in the form of identity-theft or related identity protection is necessary in order to properly warn Plaintiffs of, and/or protect Plaintiffs from, being a victim of identity theft or other identity-related crimes.

531. Defendants' conduct was outrageous because Defendants acted with an evil motive and/or with reckless indifference to the rights of Plaintiffs, thereby entitling Plaintiffs to recover punitive damages from Defendants.

532. Plaintiffs, on behalf of themselves and the Class, seek actual damages for all monies paid to Defendants in violation of the HIPAA and HITECH. In addition, Plaintiffs seek attorneys' fees.

IX. REQUEST FOR RELIEF

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

A. Declaring that this action is a proper class action, certifying the Class or, in the alternative Sub-Classes, as requested herein;

B. Declaring that Defendants breached their implied covenant of good faith and fair dealings with Plaintiffs and Class Members;

C. Declaring that Defendants violated State Consumer laws of Arizona, California, Florida, Maryland, Missouri, New York, North Carolina, Oklahoma, South Carolina, Texas, Virginia, and/or Washington;

D. Declaring that Defendants violated the California Confidentiality of Medical Information Act;

E. Declaring that Defendants breached their implied contract with Plaintiffs and Class Members;

F. Declaring that Defendants negligently disclosed Plaintiffs' and the Class Members PII and PHI;

G. Declaring that Defendants have invaded Plaintiff's and Class Members' privacy;

H. Declaring that Defendants breached their fiduciary duty to Plaintiffs and the Class

Members;

I. Declaring that Defendants violated the Missouri Merchandising Practices Act;

J. Declaring that Defendants were negligent by negligently training and supervising its employees;

K. Ordering Defendants to pay actual damages to Plaintiffs and the Class Members;

L. Ordering Defendants to disseminate individualized notice of the Healthcare Data Breach to all Class Members;

M. For an Order enjoining Defendants from continuing to engage in the unlawful business practices alleged herein;

N. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

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

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a

breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

O. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiffs;

P. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

Q. Ordering such other and further relief as may be just and proper.

X. JURY DEMAND

Plaintiffs, on behalf of themselves and the other Class Members, respectfully demands a trial by jury on all of their claims and causes of action so triable.

Dated: August 5, 2021

Respectfully submitted,

Maureen M. Brady MO#57800
Lucy McShane MO#57957
McSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com
Co-Lead Counsel for Plaintiffs and the Proposed Classes

William B. Federman (admitted *pro hac vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com
Co-Lead Counsel for Plaintiffs and the Proposed Classes

Elizabeth M. Dalzell Fed ID #7619
Kenneth E. Berger Fed ID #11083
THE LAW OFFICE OF KENNETH BERGER, LLC

5205 Forest Dr., Ste. 2
Columbia, SC 29206
Telephone: (803) 790-2800
Facsimile: (803) 790-2870
Email: edazell@bergerlaw.com
kberger@bergerlaw.com
Members of Plaintiffs' Steering Committee

John A. Yanchunis
Ryan D. Maxey
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Email: jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com
Members of Plaintiffs' Steering Committee

Robert J. Kuntz Jr., Esq. FL #094668
DEVINE GOODMAN & RASCO, LLP
2800 Ponce de Leon Blvd., Suite 1400
Coral Gables, FL 33134
Telephone: 305-374-8200
Email: rkuntz@devinegoodman.com
Members of Plaintiffs' Steering Committee

Elaine A. Ryan
Carrie A. Laliberte
BONNET, FAIRBOURNE, FRIEDMAN &
BALINT, P.C.
2325 E. Camelback Rd., Suite 300
Phoenix, AZ 85016
Telephone: (602) 274-1100
Email: eryan@bffb.com
claliberte@bffb.com
Members of Plaintiffs' Steering Committee

Bibianne U. Fell
FELL LAW, P.C.
11956 Bernardo Drive Plaza Dr., Box 531
San Diego, CA 92128
Telephone: (858) 201-3960
Facsimile: (858) 201-3966
Email: bibi@fellfirm.com
Members of Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I hereby certify that on the 5th of August 2021, I electronically filed the forgoing with the Clerk of the Court using the CM/ECF system, which will send notice of such filing to all registered users.

Co-Lead Counsel for Plaintiffs and the Proposed Classes