IN THE UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF TENNESSEE NASHVILLE DIVISION

IN RE: HCA HEALTHCARE, INC. DATA SECURITY LITIGATION	)	**No. 3:23-cv-00684**
	)	**JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Gregory Crossman, Arthur Dekenipp, Mary Elena Del Vecchio, Carina Gutierrez, Kelsey Hinds, J.B., Deborah Jordan, Gregory Marcisz, Paula Menard, Gary Silvers, Linda Simon, Michael Tighe, Colleen Walters, Jared Terrell Watkins, and Justin Taylor Womack, individually and on behalf of the Class defined below of similarly situated persons, allege the following against Defendant, HCA Healthcare, Inc. ("HCA"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel as to all other matters:

SUMMARY OF THE CASE

1. This action arises from HCA's failure to secure the personal identifiable information ("PII")[1]and protected health information ("PHI")[2] (collectively "Private

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information.

Information") of Plaintiffs and the members of the proposed Classes (defined *infra* ¶ 236) for whom HCA provided healthcare services, *i.e.*, current or former patients of hospitals or physician offices owned by HCA.

2. HCA is a large healthcare organization made up of 182 hospitals and more than 2,300 care centers (surgery centers, urgent care centers, diagnostic and imaging centers, and physician clinics) in 20 U.S. states and the United Kingdom.[3]

3. As explained in detail herein, or about July 5, 2023, HCA discovered that an unauthorized party in late June had obtained Plaintiffs' and Class Members' Private Information from HCA's computer systems (the "Data Breach").[4]

4. The Private Information that intruders accessed and infiltrated from HCA's systems included, at the very least, patient name, city, state, zip code, email, telephone number, date of birth, gender, and appointment information (patient service date, location of appointment, and the date of next appointment).

5. The facts that an individual received a medical service and their patient status at a particular entity are themselves PHI. The U.S. Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phone book because it is not related to health data, "[i]f such information was listed with health condition, *health care provision* or payment data, *such as an indication that the individual was treated at a certain clinic*, then this information would be

---

Summary of the HIPAA Privacy Rule, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). HCA is clearly a "covered entity" and some of the data compromised in this action is "protected health information," subject to HIPAA.

[3] *Who We Are*, HCA HEALTHCARE, https://hcahealthcare.com/about/ (last visited Jan. 31, 2024).

[4] *See* Exemplar Notice Letter, attached as ***Exhibit A*** ("Notice Letter").

PHI."[5]

6. As a result of the Data Breach, which HCA failed to prevent, the Private Information of patients at hospitals or physician offices owned or operated by HCA, including Plaintiffs and the proposed Class Members, was stolen.[6]

7. HCA's investigation concluded that the Private Information compromised in the Data Breach included Plaintiffs' and approximately 11 million other patients' information, across 27 million rows of data.[7]

8. Among myriad industry standards and statutes for protection of sensitive information, PHI is specifically governed by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. HIPAA requires entities like HCA to take appropriate technical, physical, and administrative safeguards to secure the privacy of PHI, establishes national standards to protect PHI, and requires timely notice of a breach of unencrypted PHI.

9. Instead, HCA disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard its Customers' Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. HCA's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

10. Further exacerbating Plaintiffs' injuries, HCA has offered no assurances that all personal data or copies of data have been recovered or destroyed, or that HCA has adequately

---

[5] *Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (emphasis added) (last visited Jan. 31, 2024).

[6] *See* Ex. A.

[7] https://hcahealthcare.com/about/privacy-update.dot (last visited Jan. 31, 2024).

enhanced its security practices or dedicated sufficient resources and staff to avoid a similar breach of its network in the future.

11. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) lost work time; (m) anxiety, annoyance, and nuisance; (n) continued risk to their Private Information, which remains in HCA's possession and is subject to further breaches so long as HCA fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information; and (o) disgorgement damages associated with HCA's maintenance and use of Plaintiffs' data for its benefit and profit..

12. Plaintiffs and Class Members would not have provided their valuable PII and sensitive PHI to HCA had they known that HCA would make their Private Information internet-accessible, not encrypt personal and sensitive data elements and not delete the Private Information it no longer had reason to maintain.

13. Through this lawsuit, Plaintiffs seek to hold HCA responsible for the injuries it inflicted on Plaintiffs and approximately 11 million similarly situated people due to its impermissibly inadequate data security measures, and to seek injunctive relief to ensure the

implementation of security measures to protect the Private Information that remains in HCA's possession.

JURISDICTION AND VENUE

14. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of Class Members approaches 11 million, many of whom have different citizenship from HCA. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

15. This Court has general personal jurisdiction over HCA because HCA is incorporated in Tennessee and has its principal place of business in Nashville, Tennessee.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because it is the District in which HCA resides.

PARTIES

Plaintiff, Gregory Crossman

17. Plaintiff Gregory Crossman is, and at all relevant times has been, a resident and citizen of Florida, where he intends to remain.

18. Plaintiff Crossman was a patient of HCA Florida Summerfield Emergency beginning in December of 2022.

19. Plaintiff Crossman entrusted his Private Information to HCA as a condition of receiving medical treatment from HCA.

20. Plaintiff Crossman received a Notice Letter from HCA concerning the Data Breach which informed him that his Private Information had been compromised in the Data Breach.

21. Since the Data Breach, Plaintiff Crossman has noticed a marked spike in spam texts

asking him to respond. He has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his Private Information.

22. Plaintiff Crossman has received notifications through credential monitoring services that his information has been located on dark web forums. In addition, Plaintiff Crossman has experienced identity theft since the data breach, and has had to change his credit and debit cards numerous times because of fraudulent charges made using his financial and credit accounts.

23. Plaintiff Crossman had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to HCA had he known that HCA would not take reasonable steps to safeguard his information.

24. Plaintiff Crossman suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

25. Plaintiff Crossman has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

26. Plaintiff Crossman is very careful about sharing sensitive Private Information. He stores documents containing Private Information in safe and secure locations and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to HCA had he known of HCA's lax data security policies.

27. As a direct and proximate result of the Data Breach, Plaintiff Crossman has made

reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his financial accounts.

28. As a result of the Data Breach, Plaintiff Crossman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Arthur Dekenipp

29. Plaintiff, Arthur Dekenipp, is, and at all relevant times has been, a resident and citizen of Alvin, Texas, where he intends to remain.

30. Plaintiff Dekenipp was a patient at HCA Houston Healthcare Clear Lake in October 2021.

31. Plaintiff Dekenipp entrusted his Private Information to HCA as a condition of receiving medical treatment from HCA.

32. Plaintiff Dekenipp received an email from HCA on July 20, 2023, at 3:59 AM CDT, informing him about the Data Breach and that his Private Information had been compromised in the Data Breach. The following month he received a hard copy of the notice by U.S. Mail dated August 14, 2023.

33. Since the Data Breach, Plaintiff Dekenipp has noticed a marked spike in spam texts messages. He has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals using his Private Information.

34. Plaintiff Dekenipp is very careful about sharing sensitive Private Information. He stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other

unsecured source. Plaintiff would not have entrusted his Private Information to HCA had he known of HCA's lax data security policies.

35. Plaintiff Dekenipp had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to HCA had he known that HCA would not take reasonable steps to safeguard his information.

36. As a direct and proximate result of the Data Breach, Plaintiff Dekenipp has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to by regularly and closely monitoring his accounts for fraud.

37. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

38. Plaintiff Dekenipp has a continuing interest in ensuring that his Private Information, which upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

39. As a result of the Data Breach, Plaintiff Dekenipp anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Mary Elena Del Vecchio

40. Plaintiff Mary Elena Del Vecchio is, and at all relevant times has been, a resident and citizen of Hudson, Florida, where she intends to remain.

41. Plaintiff Del Vecchio was a patient of HCA Florida Trinity Hospital in 2022 and

2023.

42. Plaintiff Del Vecchio entrusted her Private Information to HCA as a condition of receiving medical treatment from HCA.

43. Plaintiff Del Vecchio received an email from HCA on or about July 17, 2023, informing her about the Data Breach and that her Private Information had been compromised in the Data Breach. The following month she received a hard copy of the Notice Letter by U.S. Mail.

44. Since the Data Breach, Plaintiff Del Vecchio has noticed a marked spike in spam telephone calls and texts asking her to respond. She had unauthorized activity on her debit card and she called Suncoast about this. Her debit card was cancelled, and she obtained a new debit card. She has been notified that her PII is for sale on the dark web. She has experienced anxiety and stress as a result of the Data Breach and has concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her Private Information.

45. Plaintiff Del Vecchio is very careful about sharing sensitive Private Information. She stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

46. Plaintiff Del Vecchio had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to HCA had she known that HCA would not take reasonable steps to safeguard her information.

47. Plaintiff would not have entrusted her Private Information to HCA had she known of HCA's lax data security policies.

48. As a direct and proximate result of the Data Breach, Plaintiff Del Vecchio has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her accounts for fraud.

49. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

50. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

51. As a result of the Data Breach, Plaintiff Del Vecchio anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Carina Gutierrez

52. Plaintiff Carina Gutierrez is, and at all relevant times has been, a resident and citizen of El Paso, Texas, where she intends to remain,

53. Plaintiff Gutierrez was a patient of Care Now Urgent Care in El Paso, Texas in 2021.

54. Plaintiff Gutierrez entrusted her Private Information to HCA as a condition of receiving medical treatment from HCA.

55. Plaintiff Gutierrez received a Notice Letter from HCA dated August 14, 2023, concerning the Data Breach and informing her that her Private Information had been compromised in the Data Breach.

56. Since the Data Breach, Plaintiff Gutierrez has noticed a marked spike in spam texts

and phishing phone calls asking her to respond. She has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect her credit. After the Data Breach, she was alerted that her PII is for sale on the dark web.

57. Plaintiff Gutierrez is very careful about sharing sensitive Private Information. She stores documents containing Private Information in safe and secure locations and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to HCA had she known of HCA's lax data security policies. '

58. Plaintiff Gutierrez had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted hers Private Information to HCA had she known that HCA would not take reasonable steps to safeguard her information.

59. As a direct and proximate result of the Data Breach, Plaintiff Gutierrez has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her accounts for fraud. She has purchased Identity Theft Protection and has frozen her credit reports at all three credit bureaus, Experian, Equifax, and Transunion.

60. Plaintiff Gutierrez suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

61. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

62. As a result of the Data Breach, Plaintiff Gutierrez anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Kelsey Hinds

63. Plaintiff Kelsey Hinds is, and at all relevant times has been, a resident and citizen of the State of Kansas, where she intends to remain.

64. Plaintiff Hinds was a patient of Wesley Medical Center, most recently in February 2023.

65. Plaintiff Hinds entrusted her Private Information to HCA as a condition of receiving medical treatment from HCA.

66. Plaintiff Hinds received a Notice Letter from HCA dated August 25, 2023, concerning the Data Breach and informing her that her Private Information had been compromised in the Data Breach.

67. Plaintiff Hinds is very careful about sharing sensitive Private Information. Plaintiff Hinds stores any documents containing Private Information in safe and secure locations, and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

68. Plaintiff Hinds had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to HCA had she known that HCA would not take reasonable steps to safeguard her information.

69. Since the Data Breach, Plaintiff Hinds has noticed a marked spike in spam texts

and emails asking her to respond. She has also been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect her credit. Indeed, Plaintiff Hinds conducted a dark web internet search, which revealed that her email address was on the dark web.Further, in or around November 2023, Plaintiff Hinds was informed by her bank that someone tried to use her bank account to make a fraudulent purchase. Plaintiff Hinds used this bank account to make payments to HCA for healthcare services. As a result of the Data Breach, Plaintiff Hinds was also charged $200 for anesthesiology services that she did not obtain. Plaintiff Hinds received a suspicious bill for this fraudulent charge on or about August 2023. Plaintiff Hinds has been forced to spend her valuable time and effort remedying and disputing this fraudulent anesthesia bill.

70. Plaintiff Hinds is very careful about sharing sensitive Private Information. She stores documents containing Private Information in safe and secure locations and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

71. As a direct and proximate result of the Data Breach, Plaintiff Hinds has made reasonable efforts to mitigate the impact of the Data Breach and future misuses of her Private Information, including by regularly and closely monitoring her credit reports and spending her valuable time and effort changing her passwords to her bank account and all other online accounts that her bank account was used to pay.

72. Plaintiff Hinds suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

73. Plaintiff Hinds has a continuing interest in ensuring that her Private Information, which upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

74. As a result of the Data Breach, Plaintiff Hinds anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced actual fraud and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, J.B.

75. Plaintiff J.B., a minor, and his guardian/mother, J.N., (hereinafter referred to as "J.N." to protect the identity of the minor Plaintiff J.B.) are, and at all relevant times have been, residents and citizens of Richmond, Virginia, where they intend to remain.

76. In September 28, 2022, J.N. gave birth to triplets at Plaintiff J.B. was one of the triplets and the hospital referred to him as "Baby B."

77. The Private Information of J.B., J.N., and J.N.'s other minor children was entrusted to HCA as a condition of receiving medical treatment from HCA.

78. Plaintiff J.B.'s mother, J.N. received a Notice Letter from HCA in the summer of 2023, addressed to "Baby B" concerning the Data Breach and informing them that their Private Information was compromised in the Data Breach. J.N. and her two other children, who were born on the same day and at the same hospital as Plaintiff J.B., did not receive Notice Letters from HCA.

79. Since the Data Breach, Plaintiff J.B.'s mother, J.N., is still investigating suspicious medical bills that have gone to collections. She is unsure if the medical bills are for services rendered to , Plaintiff J.B., to date and the hospital has not been able to confirm the services charged on the suspect bills. She has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect not only her credit but that of her three minor children as well.

80. Plaintiff J.B.'s mother J.N. is very careful about sharing sensitive Private Information. She stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

81. Plaintiff J.B's mother J.N. had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff J.B.'s mother J.N. would not have entrusted her Private Information and that of her children to HCA had she known that HCA would not take reasonable steps to safeguard their information.

82. As a direct and proximate result of the Data Breach, Plaintiff J.B.'s mother, J.N. has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her accounts for fraud and regularly and closely pulling her credit report. J.N. is also in the process of putting a hold on her children's credit, including Plaintiff J.B.'s.

83. Plaintiff J.B. has a continuing interest in ensuring that his Private Information and that of his mother and siblings, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

84. As a result of the Data Breach, Plaintiff J.B.'s mother, J.N., anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She and her three minor children, including Plaintiff J.B., face a present and continuing risk of fraud and identity theft for their lifetimes.

Plaintiff, Deborah Jordan

85. Plaintiff Deborah Jordan is, and at all relevant times has been, a resident and citizen

of Ocala, Florida, where she intends to remain.

86. Plaintiff Jordan was a patient at HCA Citrus Memorial Hospital (formally known as Citrus Memorial Hospital) and HCA Florida Ocala Hospital (formally named Ocala Regional Hospital) in 2012 and a patient HCA North Florida Hospital in 1997, 2011 and 2019.

87. Plaintiff Jordan entrusted her Private Information to HCA as a condition of receiving medical treatment from HCA.

88. Plaintiff Jordan received a Notice Letter from HCA in the summer of 2023 concerning the Data Breach and informing her that her Private Information was compromised in the Data Breach.

89. Since the Data Breach, Plaintiff Jordan has noticed a marked spike in spam phone calls and text messages receiving two or more a day. She was notified that there were at least two credit cards opened in her name. Also, she had to close her credit union account, which she maintained from 1997, due to unauthorized individuals attempting to make withdrawals from the account. Unauthorized accounts have appeared on her credit reports leading her to put a hold on her credit through the credit bureaus, Experian, Trans Union and Equifax.. Plaintiff Jordan has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect her credit, cause identity theft and cause her information to appear on the dark web allowing someone to possibly file false tax returns or conduct other serious fraudulent activities.

90. Plaintiff Jordan is very careful about sharing sensitive Private Information. She stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

91. Plaintiff Jordan had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted hers Private Information to HCA had she known that HCA would not take reasonable steps to safeguard her information.

92. As a direct and proximate result of the Data Breach, Plaintiff Jordan has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts. She uses Credit Karma to check her credit every 2 to 3 days. She also has alerts set up with Experian and has credit monitoring through her credit cards.

93. Plaintiff Jordan suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

94. Plaintiff Jordan has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

95. As a result of the Data Breach, Plaintiff Jordan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced, is facing and will face a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Gregory Marcisz

96. Plaintiff Gregory Marcisz is, and at all relevant times has been, a resident and citizen of Santa Cruz, California, where he intends to remain.

97. Plaintiff Marcisz was a patient of HCA, with his most recent visit in 2020. He received medical treatment at the Dignity Health's Dominican Hospital in Santa Cruz, California,

and the Good Samaritan Hospital in San Jose, California.

98. Plaintiff Marcisz entrusted his Private Information to HCA as a condition of receiving medical treatment from HCA.

99. Plaintiff Marcisz received a Notice Letter from HCA in dated August 21, 2023, concerning the Data Breach and informing him that his Private Information was compromised in the Data Breach.

100. Since the Data Breach, Plaintiff Marcisz has observed unauthorized attempts to make online purchases or withdraw cash using his bank accounts. Additionally, Plaintiff Marcisz has encountered a significant uptick in spam calls, texts, and emails. These include a surge in automated robocalls and deceptive phishing attempts, such as requests for gift cards purportedly from medical CEOs or CFOs, and attempts at taking cash advances of his entire credit limit from his credit card. Plaintiff Marcisz has been experiencing heightened anxiety and stress after the Data Breach, especially due to his process of purchasing a house. This anxiety is primarily driven by concerns that the exposure of his PII could significantly impact his credit standing and potentially disrupt the house-buying process.

101. Plaintiff Marcisz is very careful about sharing sensitive Private Information. He stores any documents containing Private Information in a safe and secure location, and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

102. Plaintiff Marcisz had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data

security incidents. Plaintiff would not have entrusted his Private Information to HCA had he known that HCA would not take reasonable steps to safeguard his information.

103. As a direct and proximate result of the Data Breach, Plaintiff Marcisz has made reasonable efforts to mitigate the impact of the Data Breach. These efforts include subscribing at a monthly expense to a credit monitoring service, regularly reviewing his credit reports and accounts, contacting banks for fraud alerts, and freezing his credit.

104. As a result of the Data Breach, Plaintiff Marcisz has been spending several hours per month monitoring his credit and financial accounts. Plaintiff Marcisz will continue to spend considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

105. Plaintiff Marcisz has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

106. Plaintiff Marcisz has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Paula Menard

107. Plaintiff Paula Menard is, and at all relevant times has been, a resident and citizen of Texas, where she intends to remain.

108. Plaintiff Menard was a patient of HCA Houston Healthcare North Cypress in early 2023.

109. Plaintiff Menard entrusted her Private Information to HCA as a condition of receiving medical treatment from HCA.

110. Plaintiff Menard received a Notice Letter from HCA dated August 14, 2023, concerning the Data Breach and informing her that her Private Information was compromised in the Data Breach.

111. Since the Data Breach, Plaintiff Menard has noticed a marked spike in spam text messages, and was notified by Norton Lifelock that her Private Information is on the dark web.

112. In addition, after the Data Breach, an unauthorized actor obtained access to her certificate of deposit account and transferred money out, including $2,000 to a checking account at a different bank, $100 to Walmart, and $50 to Zelle. She was told by her bank that someone used her driver's license number to obtain access to her account and open new accounts at her bank. New accounts were also opened in her name at another bank and other retail stores. As a result, Plaintiff was forced close her old account at her bank and open a new one, and report fraud at many entities. She has been experiencing anxiety and stress as a result of the Data Breach and has lost sleep from fear that her accounts will be breached or her credit will be affected.

113. Plaintiff Menard is very careful about sharing sensitive Private Information. She stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

114. Plaintiff Menard had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to HCA had she known that HCA would not take reasonable steps to safeguard her information.

115. would not have entrusted her Private Information to HCA had she known of

HCA's lax data security policies.

116. As a direct and proximate result of the Data Breach, Plaintiff Menard has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her accounts for fraud, purchasing Norton Lifelock on July 24, 2023, for a yearly charge of $246.22, and signing up for a credit freeze.

117. Plaintiff Menard suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

118. Plaintiff Menard has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

119. As a result of the Data Breach, Plaintiff Menard anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff Gary Silvers

120. Plaintiff Gary Silvers is, and at all relevant times has been, a resident and citizen of Florida, where

121. Plaintiff Silvers was a patient of HCA Florida Woodmont Hospital beginning in about 1994 and most recently in 2022.

122. Plaintiff Silvers received a Notice Letter from HCA dated August 21, 2023, concerning the Data Breach.

123. Since the Data Breach, Plaintiff Silvers has experienced an increase in spam calls using his Private Information and informing him that his Private Information was compromised in

the Data Breach.

124. In August and September 2023, unauthorized charges were made to Plaintiff's credit cards. As a result, he had to cancel two credit cards and have new cards reissued, as well as change the automatic payment information for approximately 16 vendors associated with those cards. He has been experiencing anxiety as a result of the Data Breach and his Private Information being disclosed, and is fearful of further identity theft and of ruining his credit.

125. Plaintiff Silvers is very careful about sharing sensitive Private Information. He stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

126. Plaintiff Silvers had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to HCA had she known that HCA would not take reasonable steps to safeguard her information..

127. As a direct and proximate result of the Data Breach, Plaintiff Silvers has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his accounts for fraud, and responding thoroughly to the two instances of identity fraud.

128. Plaintiff Silvers suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

129. Plaintiff Silvers has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

130. As a result of the Data Breach, Plaintiff Silvers anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Linda Simon

131. Plaintiff Linda Simon is, and at all relevant times has been, a resident and citizen of Tavernier, Florida, where she intends to remain

132. Plaintiff Simon was a patient at an HCA doctor's office in Key Largo, Florida in approximately July 2023.

133. Plaintiff Simon entrusted her Private Information to HCA as a condition of receiving medical treatment from HCA and informing her that her Private Information had been compromised in the Data Breach.

134. Plaintiff Simon received a Notice Letter from HCA dated August 21, 2023, concerning the Data Breach.

135. Since the Data Breach, Plaintiff Simon has experienced a marked spike in spam texts and phishing phone calls asking her to respond. She has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect her credit. She is very concerned about money being stolen from her bank account. Since the Data Breach, Plaintiff Simon has also experienced an unauthorized person attempting to obtain approximately $400.00 from her Venmo account which is connected to her bank account. An unauthorized charge of about $23.99 also appeared on Plaintiff's PayPal account; Plaintiff Simon has not yet been reimbursed for this unauthorized charge.

136. Plaintiff Simon is very careful about sharing sensitive Private Information. She stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

137. Plaintiff Simon had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to HCA had she known that HCA would not take reasonable steps to safeguard her information.

138. As a direct and proximate result of the Data Breach, Plaintiff Simon has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her accounts for fraud. After the Data Breach, Plaintiff purchased Credit Monitoring and Identity Theft Protection from MyScoreIQ and froze her accounts at the credit bureaus.

139. Plaintiff Simon suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

140. Plaintiff Simon has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

141. As a result of the Data Breach, Plaintiff Simon anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Michael Tighe

142. Plaintiff Michael Tighe is, and at all relevant times has been, a resident and citizen of Katy, Texas through June 2023 and Houston, Texas, where he intends to remain.

143. Plaintiff Tighe was a patient of CareNow Urgent Care and recalls visiting there at least as early as 2021.

144. Plaintiff Tighe entrusted his Private Information to HCA as a condition of receiving medical treatment from HCA.

145. Plaintiff Tighe received a Notice Letter from HCA dated August 14, 2023, concerning the Data Breach and informing him that his Private Information had been compromised in the Data Breach.

146. Since the Data Breach, Plaintiff Tighe has noticed a marked spike in spam calls and text messages. He also receives daily alerts from his Microsoft Authenticator application notifying him of unauthorized attempts to log into his email account. Additionally, an unauthorized individual(s) attempted to log into his Amazon account and successfully logged into his Netflix account and disabled it. These accounts use the same email address as the one he believes is he provided to HCA. Since the Data Breach, Plaintiff Tighe's bank account was also compromised by an unauthorized third party and unauthorized charges were made to his account. As a result, Plaintiff Tighe had to close his bank account and cancel his debit card. Plaintiff Tighe now keeps his debit card locked and monitors his bank account every morning. Plaintiff Tighe has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect his credit.

147. Plaintiff Tighe is very careful about sharing sensitive Private Information. He stores documents containing Private Information in safe and secure locations and has never knowingly

transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

148. Plaintiff Tighe had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to HCA had she known that HCA would not take reasonable steps to safeguard his information.

149. As a direct and proximate result of the Data Breach, Plaintiff Tighe has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his accounts for fraud.

150. Plaintiff Tighe suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

151. Plaintiff Tighe has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

152. As a result of the Data Breach, Plaintiff Tighe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Colleen Walters

153. Plaintiff Colleen Walters is, and at all relevant times has been, a resident and citizen of the state of Tennessee, where she intends to remain.

154. Plaintiff Walters was a patient of TriStar Summit Medical Center.

155. Plaintiff Walters entrusted her Private Information to HCA as a condition of receiving medical treatment from HCA.

156. Plaintiff Walters received a Notice Letter from HCA dated August 25, 2023, concerning the Data Breach and informing her that her Private Information had been compromised in the Data Breach.

157. Since the Data Breach, Plaintiff Walters has noticed a marked spike in spam calls and text messages, she has experienced unauthorized charges on her financial accounts, and she received a bill for a medical appointment that was not hers.

158. Plaintiff Walters is very careful about sharing sensitive Private Information. She stores documents containing Private Information in safe and secure locations and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

159. Plaintiff Walters had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to HCA had she known that HCA would not take reasonable steps to safeguard his information.

160. As a direct and proximate result of the Data Breach, Plaintiff Walters has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her accounts for fraud.

161. Plaintiff Walters suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

162. Plaintiff Walters has a continuing interest in ensuring that her Private Information,

which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

163. As a result of the Data Breach, Plaintiff Walters anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

Plaintiff, Jared Terrell Watkins

164. Plaintiff Jared Terrell Watkins is, and at all relevant times has been, a resident and citizen of Bowling Green, Kentucky, where he intends to remain.

165. Plaintiff Watkins was a patient of TriStar Greenview Regional Hospital in Bowling Green Kentucky in May 2023.

166. Plaintiff Watkins entrusted his Private Information to HCA as a condition of receiving medical treatment from HCA.

167. Plaintiff Watkins received a Notice Letter from HCA dated August 25, 2023, concerning the Data Breach and informing him that his Private Information had been compromised in the Data Breach.

168. Since the Data Breach, Plaintiff Watkins has experienced a marked spike in spam text messages.. He has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect his credit. In 2023, an unauthorized person also took money out of Plaintiff's bank account twice using debit card information. Plaintiff was forced to physically go to his bank to get temporary bank debit cards after his bank debit cards were cancelled due to fraud.

169. Plaintiff Watkins is very careful about sharing sensitive Private Information. He stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

170. Plaintiff Watkins had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to HCA had he known that HCA would not take reasonable steps to safeguard his information.

171. As a direct and proximate result of the Data Breach, Plaintiff Watkins has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his accounts for fraud.

172. Plaintiff Watkins has incurred late fees or declined payment fees that may have been as much as $300.00 altogether as a result of failed automatic payments tied to his bank debit cards.

173. Plaintiff Watkins has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

174. Plaintiff Watkins has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Plaintiff, Justin Taylor Womack

175. Plaintiff Justin Taylor Womack is, and at all relevant times has been, a resident and

citizen of Dallas, Texas, where he intends to remain.

176. Plaintiff Womack was a patient of HCA facilities on several dates within the last five years.

177. Plaintiff Womack received a Notice Letter from HCA dated August 14, 2023, concerning the Data Breach and informing him that his Private Information had been compromised in the Data Breach.

178. Since the Data Breach, Plaintiff Womack has noticed a marked spike in spam texts and phishing phone calls asking him to respond. He has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect his credit. After the Data Breach, Plaintiff Womack has also been alerted that his PII is presently for sale on the dark web.

179. Plaintiff Womack is very careful about sharing sensitive Private Information. He stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

180. Plaintiff Womack had the reasonable expectation and understanding that HCA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to HCA had he known that HCA would not take reasonable steps to safeguard his information.

181. As a direct and proximate result of the Data Breach, Plaintiff Womack has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his accounts for fraud. Plaintiff Womack also purchased LifeLock Identity Theft

Protection after the Data Breach.

182. Plaintiff Womack suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

183. Plaintiff Womack has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

184. As a result of the Data Breach, Plaintiff Womack anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

Defendant, HCA Healthcare, Inc.

185. HCA is a corporation formed and existing under the laws of Delaware with its headquarters and principal place of business at 1 Park Plaza, Nashville, Tennessee 37203-6527.

FACTUAL ALLEGATIONS

A. HCA

186. HCA is one of the largest healthcare providers in the United States. Originally formed in 1968 as Hospital Corporation of America, HCA has undergone several mergers, expansions, and at least two IPOs, the most recent of which raised approximately $3.79 billion, at that time the largest private equity-backed IPO in U.S. history.[8]

187. HCA's hospitals, physicians' offices, and other healthcare centers obtain the Private Information of their patients as part of the healthcare professional-patient relationship, and as a condition of providing services.

[8] *See* Clare Baldwin and Alina Selyukh, *HCA IPO prices at $30, sells more shares: sources*, https://www.reuters.com/article/us-hca-idUSTRE7280NV20110309 (last visited Jan. 31, 2024).

188. On its website, HCA states in bold font: "At HCA Healthcare, we are driven by a single mission: Above all else, we are committed to the care and improvement of human life."[9] HCA puts patient data at the center of this pitch, stating it "analyzes data from more than 37 million patient encounters each year."[10] HCA profits and benefits from patient data by using it to "develop technologies and best practices that improve patient care."[11]

189. In addition, HCA states on its website that "HCA HealthCare's use and disclosure of Protected Health Information [under HIPAA] is set forth in the HCA Healthcare Notice of Privacy Practice, which can be accessed at the bottom of the facility website."[12]

190. Moreover, HCA's Notices of Privacy Practices associated with its various facilities states: "Each time you visit a hospital, physician, or other healthcare provider, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, a plan for future care or treatment, and billing-related information." The Notices state: "We are required by law to maintain the privacy of your health information."[13] Despite this requirement, HCA failed.

191. HCA also maintains a "Code of Conduct," which was developed to provide "guidance to ensure our work is done in an ethical and legal manner."[14] With regard to patient information, HCA's Code of Conduct states that it collects "information about the patient's medical condition, history, medication, and family illnesses in order to provide quality care[,]" and

[9] https://hcahealthcare.com/about/our-mission-and-values.dot (last visited Jan. 31, 2024).
[10] https://hcahealthcare.com/about/ (last visited Jan. 31, 2024).
[11] https://hcahealthcaretoday.com/2022/06/02/seeking-new-ways-to-improve-more-lives-in-more-ways/ (last visited Feb. 2, 2024); *see also, e.g.*, https://www.theverge.com/2021/5/26/22454817/google-hca-patient-data-healthcare-algorithms (last visited Feb. 2, 2024).
[12] https://hcahealthcareshowsup.com/legal/index.dot#privacy-policy (last visited Feb. 2, 2024).
[13] *E.g.*, https://www.hcafloridahealthcare.com/legal/notice-of-privacy-practices (last visited Jan. 31, 2024).
[14] https://hcahealthcare.com/util/forms/ethics/Code-of-Conduct-Booklet-a.pdf (last visited Feb. 2, 2024).

represents that it realizes the sensitive nature of the patient information it collects and is "committed to maintaining its confidentiality."[15] HCA further represents:

> Consistent with HIPAA, we do not use, disclose or discuss patient-specific information, including patient financial information, with others unless it is necessary to serve the patient or required by law. HCA Healthcare colleagues must never use or disclose confidential information that violates the privacy rights of our patients. In accordance with our information privacy and security policies and procedures, which reflect HIPAA requirements, no HCA Healthcare colleague, affiliated physician, or other healthcare partner has a right to any patient information other than that necessary to perform his or her job.[16]

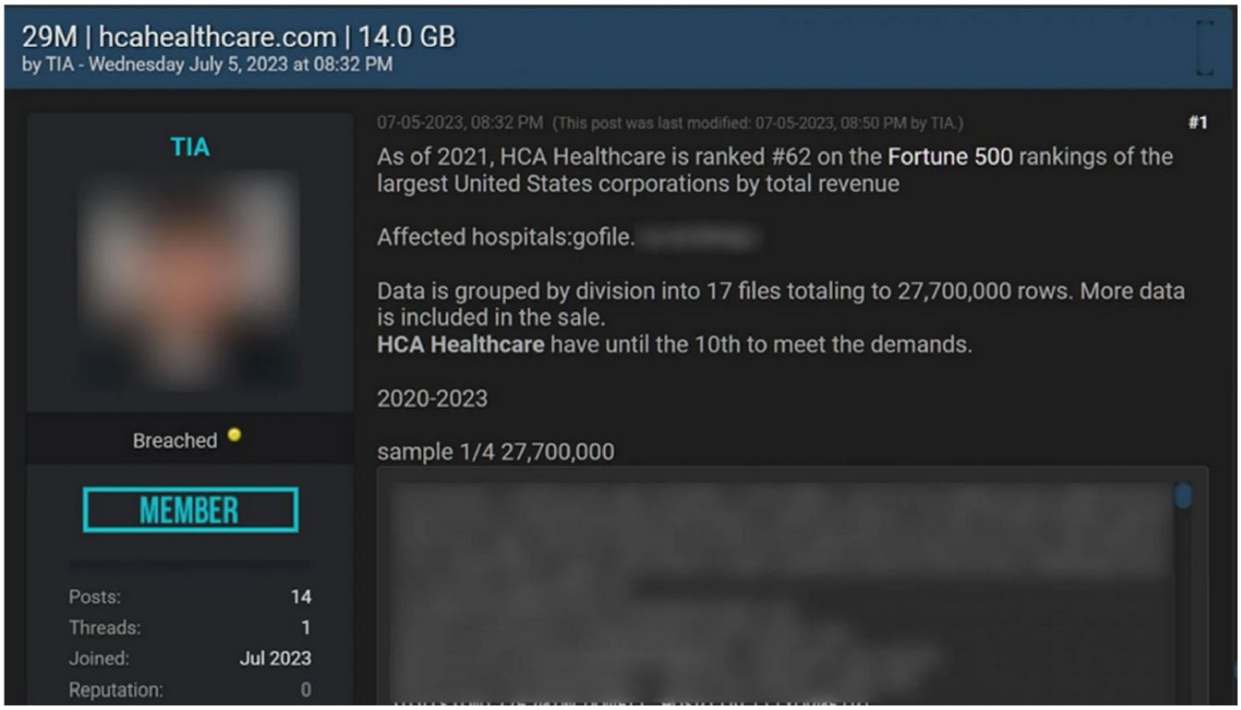
B. The Data Breach

192. In or about late June 2023, Plaintiffs' and Class Members' Private Information in possession of HCA was obtained by an unauthorized party, which HCA describes in its Notice Letter as "what appears to be a theft from an external storage location exclusively used to automate the formatting of email messages."[17]

193. The unauthorized party posted the entire data dump that it stole from HCA on a dark web hacking forum. On information and belief, these stolen files are now readily available to download from the dark web by anyone, to be used for fraudulent criminal purposes and resold.

194. A dark web post indicates that the stolen Private Information is available in 17 files and 27.7 million database records, and that there was a ransom demand to HCA with a deadline of July 10, 2023. Having not heard from HCA by that date, the full database became available for sale. Thus, it appears that HCA never attempted to prevent this leak.

[15] *Id*.
[16] *Id*.
[17] Ex. A.



195. On or about July 10, 2023, HCA posted a Data Security Incident report on its website, stating that it had "recently discovered that a list of certain information with respect to some of its patients was made available by an unknown and unauthorized party on an online forum [including] Patient name, city, state, and zip code; Patient email, telephone number, date of birth, gender; and Patient service date, location and next appointment date" and with a list of affected HCA-owned hospitals and physician offices.[18] On July 14, 2023, HCA began emailing some of the patients affected by the Data Breach to provide them with information about the Data Breach.[19] HCA began sending out formal Notice Letters in August 2023 to affected persons, informing them that their Private Information had been compromised in the Data Breach.

196. Defendant claims the information stolen in the attack did not include "clinical information, such as treatment, diagnosis, or condition;" "payment information, such as credit card

[18] *See* HCA Healthcare, *Privacy update* (Aug. 14, 2023), https://hcahealthcare.com/about/ privacy-update.dot (last visited Jan. 31, 2024), linking to "original July 10, 2023 news release."
[19] *Id*.

or account numbers;" or "sensitive information, such as passwords, driver's license or social security numbers."[20] However, that is contradicted by statements on the dark web, on which the hacker ostensibly responsible for the Data Breach stated "I have emails with health diagnosis that corresponds to a clientID."[21]

197. Moreover, HCA offered Plaintiffs and Class Members "complimentary credit monitoring and identity protection services for 2 years via IDX."[22] This offer supports that Plaintiffs' and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from HCA's computer systems. In addition, HCA's offer indicates that it recognizes that Plaintiffs and Class Members are at a present and continuing risk of identity theft and fraud as a result of the Data Breach.

C. The Value of Private Information

198. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[23]

199. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to

[20] https://hcahealthcare.com/about/privacy-update.dot#faq1 (last visited Jan. 31, 2024).
[21] *HCA Healthcare releases statement while hacker puts data up for sale on deep web (update1)*, DataBreaches.net, https://www.databreaches.net/hca-healthcare-releases-statement-while-hacker-puts-data-up-for-sale-on-deep-web/ (last visited Jan. 31, 2024).
[22] Ex. A.
[23] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 31, 2024).

release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[24]

200. Stolen Private Information is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

201. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[25]

202. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[26]

203. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web

---

[24] *See* https://www.cisa.gov/sites/default/files/2023-01-CISA_MSISAC_Ransomware%20Guide_8508C.pdf (last visited Jan. 31, 2024).

[25] *Shining a Light on the Dark Web with Identity Monitoring, IdentityForce*, Dec. 28, 2020, available at: https://www.identityforce.com/blog/shining-light-dark-web-identity- monitoring (last visited Jan. 31, 2024).

[26] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, available at: https://www.armor.com/resources/blog/stolen-pii- ramifications- identity-theft-fraud-dark-web/ (last visited Jan. 31, 2024).

pricing for stolen identity credentials. For example, Private Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $2009.[27] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[28] Criminals can also purchase access to entire company data breaches.[29]

204. In addition, due to the highly valuable nature of PHI, the FBI has warned healthcare providers that they are likely to be the targets of cyberattacks like the one at issue here.[30]

205. Once Private Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

206. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

207. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

208. Data breaches facilitate identity theft as hackers obtain consumers' Private Information and thereafter use it to siphon money from current accounts, open new accounts in the

---

[27] *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 visited Jan. 31, 2024).

[28] *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 visited Jan. 31, 2024).

[29] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the- dark/ (last visited Jan. 31, 2024).

[30] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK2 4U20140820.

names of their victims, or sell consumers' PII to others who do the same.

209. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use Private Information to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[31] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[32]

210. The market for Private Information has continued unabated to the present, and in 2023 the number of reported data breaches in the United States increased by 78% over 2022, reaching 3205 data breaches.[33]

211. The exposure of Plaintiffs' and Class Members' Private Information to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

D. Healthcare Organizations are Prime Targets for Cyberattacks

212. Healthcare organizations are prime targets for cyberattacks because of the information they collect and store, including financial information of patients, login credentials,

---

[31] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited Jan. 31, 2024).

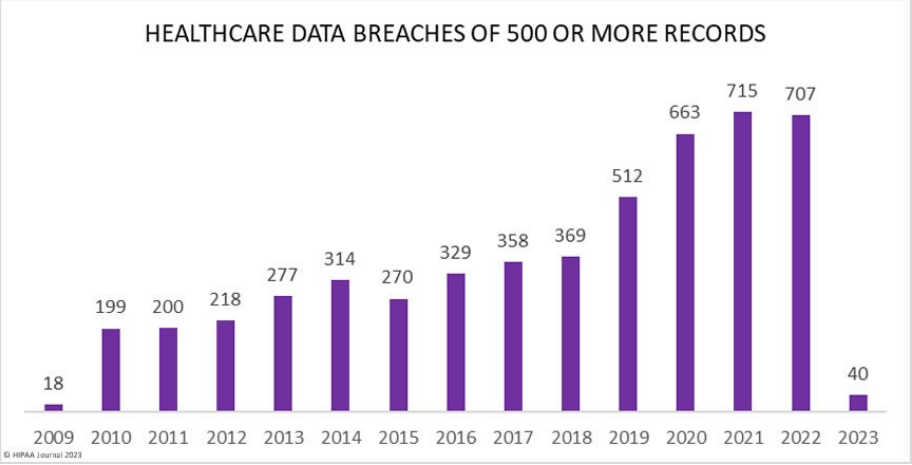
[32] *Id*.

[33] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, INFOSECURITY MAGAZINE (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/ (last visited Jan. 31, 2024); *see also* Identity Theft Resource Center, *2023 Data Breach Report*, https://www.idtheftcenter.org/publication/ 2023-data-breach-report/ (last visited Jan. 31, 2024).

insurance information, medical records and diagnoses, and personal information of employees, customers and patients—all extremely valuable in underground markets.

213. This was known and obvious to HCA as they observed frequent public announcements of data breaches affecting the healthcare industry and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of cybercriminals.

214. For example, a report by the HIPAA Journal noted that "Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more records have been reported to the HHS' Office for Civil Rights. Those breaches have resulted in the exposure or impermissible disclosure of 382,262,109 healthcare records. That equates to more than 1.2X the population of the United States. In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[34]



215. Ransomware attacks are especially prevalent in the industry. For years federal agencies have warned about the increasing risk of ransomware attacks on companies holding PII and PHI. For example, in October 2019 the Federal Bureau of Investigation published online an

[34] https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Feb. 2, 2024).

article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[35]

216. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[36]

217. In March 2021, Tenable Security Response Team conducted a root cause analysis of 293 healthcare breaches known to have exposed records between January 2020 and February 2021, and concluded that "ransomware was by far the most prominent root case of healthcare breaches, accounting for a whopping 54.95%."[37]

218. At all relevant times, HCA knew, or reasonably should have known, of the importance of safeguarding Private Information and the foreseeable consequences that would occur if its data security systems were breached, including, specifically, the significant costs that would be imposed on affected individuals as a result of the breach.

219. HCA was, or should have been, fully aware of the significant number of individuals whose Private Information it collected and stored, thus, the significant number of individuals who would be harmed by a breach of HCA's systems.

---

[35] https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Feb. 2, 2024).
[36] https://www.cisa.gov/stopransomware/ransomware-faqs#:~:text=Malicious%20actors%20continue%20to%20adjust,as%20secondary%20forms%20of%20extortion (last visited Feb. 2, 2024).
[37] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last visited Feb. 2, 2024).

220. Despite all the publicly available knowledge of the serious threat of compromises of personal information and despite holding the Private Information of millions of individuals, HCA failed to use reasonable care in maintaining the privacy and security of Plaintiff's and Class Members' Private Information. Had HCA implemented adequate security measures, cybercriminals never could have accessed millions of individuals' files and the Data Breach would have been prevented or much smaller in scope.

E. HCA Failed to Comply with Regulatory Requirements and Standards

199. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

200. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access. Florida is one such state and requires that entities like HCA "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. § 501.171(2).

201. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible

communication system; and training staff regarding critical points.[38]

202. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[39]

203. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[40]

204. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

205. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[41]

---

[38] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security (last visited Jan. 31, 2024).

[39] *Start With Security*, Fed. Trade Comm'n ("FTC"), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 31, 2024).

[40] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 31, 2024).

[41] *Supra* n.39.

206. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

207. HCA's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

208. HCA's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

209. Furthermore, HCA is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

210. The Security Rule requires HCA 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 its workforce.[42]

211. Pursuant to HIPAA's mandate that HCA follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, HCA was required to, at minimum, "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), and "[i]mplement 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).

212. HCA is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

213. Both HIPAA and HITECH obligate HCA to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

214. As alleged in this Complaint, HCA has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of PHI.

[42] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Jan. 31, 2024).

F. HCA Failed to Comply with Industry Practices

215. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[43] All organizations collecting and handling Private Information, such as HCA, are strongly encouraged to follow these controls.

216. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[44]

217. Cybersecurity experts normally have identified data management companies, like HCA, as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect, use, and maintain.[45]

218. Several best practices have been identified that a minimum should be implemented by data management companies like HCA, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software,

[43] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Jan. 31, 2024).
[44] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 31, 2024).
[45] *See Security Questions to Ask After the ZeroedIn Breach*, Information Week, https://www.informationweek.com/cyber-resilience/security-questions-to-ask-after-the-zeroedin-breach (last visited Jan. 31, 2024) (commenting that the growing outsourcing of data analytics work to third-party service providers may offer to malicious cyber-attackers novel "targets of opportunity – breach one data manager and gain access to data from a multitude of sources.).

maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[46]

219. Other best practices have been identified that a minimum should be implemented by companies like HCA using third-party providers, including but not limited to ensuring that Private Information is only shared with third parties when reasonably necessary and that those vendors have appropriate cybersecurity systems and protocols in place.[47]

220. HCA failed to follow these and other industry standards to adequately protect the Private Information of Plaintiffs and Class Members.

G. The Data Breach Caused Injury to Class Members and Will Result in Additional Harm Such as Fraud.

221. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiffs and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their Private Information for months without being able to take available precautions to prevent imminent harm.

222. The ramifications of HCA's failure to secure Plaintiffs' and Class Members' data are severe.

223. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

---

[46] *See* Center for Internet Security, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Jan. 31, 2024).
[47] *See id*.

224. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[48] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[49]

225. Identity thieves can use Private Information, such as that of Plaintiffs and Class Members, which HCA failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

226. As demonstrated herein, these and other instances of fraudulent misuse of the compromised Private Information has already occurred and are likely to continue.

227. As a result of HCA's delay between the Data Breach in August and the notice of the Data Breach sent to affected persons in November, the risk of fraud for Plaintiffs and Class Members increased exponentially.

228. Javelin Strategy and Research reported that identity thieves stole $112 billion from 2011 through 2016.[50]

229. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's

[48] 17 C.F.R. § 248.201 (2013).
[49] *Id*.
[50] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited Jan. 31, 2024).

Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[51]

230. The 2017 Identity Theft Resource Center survey[52] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

231. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[53]

[51] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Jan. 31, 2024).
[52] *Id.*
[53] *Id.*

232. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information 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.[54]

Thus, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

H. Plaintiffs and Class Members Suffered Damages

233. As a direct and proximate result of HCA's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

234. HCA's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' Private Information, causing

[54] GAO, *Report to Congressional Requesters*, at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 31, 2024).

them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiffs' and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages.

235. While Plaintiffs' and Class Members' Private Information has been stolen, HCA

continues to hold Plaintiffs' and Class Members' Private Information. Particularly because HCA have demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ALLEGATIONS

236. Plaintiffs bring this class action individually on behalf of themselves and on behalf of all members of the following Classes of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiffs seek certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Classes:

Nationwide Class

All persons residing in the United States whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

California Class

All persons residing in the state of California whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Florida Class

All persons residing in the state of Florida whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Kansas Class

All persons residing in the state of Kansas whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Kentucky Class

All persons residing in the Commonwealth of Kentucky whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Tennessee Class

All persons residing in the state of Texas whose Private Information was compromised in

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

Texas Class

All persons residing in the state of Texas whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Virginia Class

All persons residing in the Commonwealth of Virginia whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

237. Excluded from the Class are HCA and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which HCA has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

238. Plaintiffs reserve the right to modify or amend the foregoing Class definitions before the Court determines whether certification is appropriate.

239. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, it has been reported that approximately 11 million individuals' information was exposed in the Data Breach.

240. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether HCA engaged in the conduct alleged herein;

b. Whether HCA had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

c. Whether HCA's computer systems and data security practices used to protect Plaintiffs' and Class Members' Private Information violated the FTC Act and/or state laws, and/or HCA's other duties discussed herein;

d. Whether HCA failed to adequately respond to the 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 Class Members;

e. Whether HCA unlawfully shared, lost, or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether HCA's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether HCA's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Plaintiffs and Class Members suffered injury as a proximate result of HCA's negligent actions or failures to act;

i. Whether HCA failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' Private Information;

j. Whether HCA breached duties to protect Plaintiffs' and Class Members' Private Information;

k. Whether HCA's actions and inactions alleged herein were negligent;

l. Whether HCA were unjustly enriched by their conduct as alleged herein;

m. Whether an implied contract existed between Class Members and HCA with respect to protecting Private Information and privacy, and whether that contract was breached;

n. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages or other relief, and the measure of such damages and relief;

o. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

p. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

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

242. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their Private Information compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by HCA, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

243. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs are adequate representatives of the Class and have no interests adverse to, or conflict with, the Class(es) they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

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

245. Injunctive and Declaratory Relief: HCA has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

246. Likewise, particular issues are appropriate for certification under Rule 24(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this mater and the parties' interests therein. Such issues include, but are not limited to: (a) whether HCA owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, and safeguarding their Private Information; (b) whether HCA failed to adequately monitor and audit their data security systems; and (c) whether HCA failed to take reasonable steps to safeguard the Private Information of Plaintiffs and Class Members.

247. All members of the proposed Class are readily ascertainable. HCA has access to the names in combination with addresses and/or e-mail addresses of Class Members affected by the

Data Breach. Indeed, impacted Class Members already have been preliminarily identified and sent a breach notice letter.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Classes)

248. Plaintiffs restate and reallege paragraphs 1 through 247 above as if fully set forth herein.

249. HCA's clients, including HCA, require their employees to submit non-public Private Information as a condition of healthcare services.

250. HCA gathered and stored the Private Information of Plaintiffs and Class Members as part of its business, which affects commerce.

251. Plaintiffs and Class Members entrusted HCA with their Private Information with the understanding that the information would be safeguarded.

252. HCA had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if their Private Information were wrongfully disclosed.

253. By assuming the responsibility to collect and store this data, HCA had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

254. HCA owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

255. HCA's duty to use reasonable security measures arose as a result of the special relationship that existed between HCA, on the one hand, and Plaintiffs and Class Members, on the other hand. That special relationship arose because HCA was entrusted with their confidential Private Information, a necessary part of healthcare services, and HCA (and possibly other employers) shared the information with HCA.

256. HCA also had a duty to exercise appropriate clearinghouse practices to remove former employees' Private Information they were no longer required to retain pursuant to regulations.

257. Moreover, HCA had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach, but failed to do so.

258. HCA had and continues to have duties to adequately disclose that Plaintiffs' and Class Members' Private Information within HCA's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

259. HCA breached its duties and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by HCA include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former employees' Private Information they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

260. HCA breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

261. HCA knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and the Class.

262. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

263. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of HCA's inadequate security practices.

264. It was foreseeable that HCA's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

265. HCA had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

266. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. HCA knew or should have known of the inherent risks in collecting and storing Private Information, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on its systems.

267. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, HCA's possession.

268. HCA was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

269. HCA's duties extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

270. HCA has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

271. But for HCA's wrongful and negligent breaches of duties owed to Plaintiffs and the Class, Plaintiffs' and Class Members' Private Information would not have been compromised.

272. There is a close causal connection between HCA's failure to implement security measures to protect Plaintiffs' and Class Members' Private Information, and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. Private Information was lost and accessed as the proximate result of HCA's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

273. As a direct and proximate result of HCA's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in HCA's possession and is subject to further unauthorized disclosures so long as HCA fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by HCA's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

274. As a direct and proximate result of HCA's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

275. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

276. HCA's negligent conduct is ongoing, in that it still possesses Plaintiffs' and Class Members' Private Information in an unsafe and insecure manner.

277. Plaintiffs and Class Members are entitled to injunctive relief requiring HCA to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Classes)

278. Plaintiffs restate and reallege paragraphs 1 through 247 above as if fully set forth herein.

279. HCA had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Plaintiffs' and Class Members' Private Information.

280. HCA breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by HCA include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove former employees' Private Information they were no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

281. HCA's violation of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

282. Plaintiffs and Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

283. The harm that has occurred is the type of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

284. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

285. HCA breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

286. In addition, under state data security and consumer protection statutes such as those outlined herein, HCA had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

287. Plaintiffs and Class Members were foreseeable victims of HCA's violations of HIPAA, HITECH, and the FTC Act, and state data security and consumer protection statutes. HCA knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and the Class.

288. As a direct and proximate result of HCA's negligence per se, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls,

texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in HCA's possession and is subject to further unauthorized disclosures so long as HCA fails to undertake appropriate and adequate measures to protect the Private Information.

289. As a direct and proximate result of HCA's negligence per se Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

290. Finally, as a direct and proximate result of HCA's negligence per se, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in HCA's possession and is subject to further unauthorized disclosures so long as HCA fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Classes)

291. Plaintiffs restate and reallege paragraphs 1 through 247 above as if fully set forth herein.

292. Plaintiffs and Class Members were required to provide their Private Information to HCA as a condition of receiving healthcare services.

293. Plaintiffs and Class Members entrusted their Private Information to HCA. In doing so, Plaintiffs and the Class entered into implied contracts with HCA by which HCA agreed to safeguard and protect such information to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

294. The Notices of Privacy Practices that govern HCA-owned hospitals and other healthcare centers state: "We are required by law to maintain the privacy of your health information."[55]

295. In entering into the implied contracts, Plaintiffs and Class Members reasonably believed and expected that HCA's data security practices complied with relevant laws and regulations and were consistent with industry standards, and that HCA would thoroughly vet and select vendors that adequately protect Private Information.

296. Implicit in the agreement between Plaintiffs and Class Members and HCA was HCA's obligation to: (a) take reasonable steps to safeguard that Private Information, including through proper vetting of third party vendors to whom Private Information is provided; (b) prevent unauthorized disclosure of the Private Information; (c) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (d) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses; and (e) retain or allow third parties to retain Private Information only under conditions that kept such information secure and confidential.

297. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and HCA on the other, is demonstrated by their conduct and course of dealing. HCA required Plaintiffs and Class Members to provide their Private Information as a condition of healthcare services. Plaintiffs and Class Members accepted the offers for healthcare services and provided their Private Information.

298. In accepting the Private Information, HCA understood and agreed that they were required to reasonably safeguard and otherwise ensure protection of the Private Information from unauthorized access or disclosure.

[55] *E.g.*, https://www.hcafloridahealthcare.com/legal/notice-of-privacy-practices (last visited Jan. 31, 2024).

299. Plaintiffs and Class Members would not have entrusted their Private Information to HCA in the absence of the implied contract between them and HCA that HCA would keep, and require the third-party vendors it selects to house Private Information to keep, their Private Information reasonably secure.

300. Plaintiffs and Class Members would not have entrusted their Private Information to HCA in the absence of their implied promise to monitor and ensure that the Private Information entrusted to it would remain protected by reasonable data security measures and remain confidential, either in HCA's hands or the hands of its vendor, HCA.

301. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with HCA by providing their Private Information at HCA's request.

302. HCA breached the implied contracts made with Plaintiffs and the Class by failing to safeguard and protect their Private Information, by entrusting the Private Information to a vendor that fails to safeguard Private Information, by failing to delete the Private Information of Plaintiffs and the Class or requiring vendors to delete information once the relationship ended, and by failing to provide accurate notice to them that their Private Information was compromised as a result of the Data Breach.

303. Moreover, implied in these exchanges was a promise by HCA to ensure that the Private Information of Plaintiffs and Class Members was only used in connection with the agreed-upon healthcare services.

304. Plaintiffs and Class Members therefore did not receive the benefit of the bargain with HCA, because they provided their Private Information in exchange for an implied agreement by HCA to keep it safe and secure, whether as housed by HCA or in connection with providing the Private Information to a third-party vendor.

305. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do. Likewise, all conditions required for HCA's performance were met.

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

307.

308. As a direct and proximate result of HCA's breaches, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

309. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

310. Plaintiffs and Class Members are also entitled to injunctive relief requiring HCA to, *e.g.*, (i) strengthen its data monitoring procedures; (ii) evaluate, audit, and improve its processes for vetting third party vendors and the selection processes for vendors to which HCA provides sensitive Private Information; (iii) submit to future annual audits of those systems and monitoring procedures; and (iv) immediately provide or continue providing adequate credit monitoring to all Class Members.

COUNT IV
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiffs and the Classes)

311. Plaintiffs restate and reallege paragraphs 1 through 247 as if fully set forth herein.

312. Plaintiffs and Class Members were required to provide their Private Information to HCA as a condition of receiving healthcare services.

313. Plaintiffs and Class Members entrusted their Private Information to HCA. In doing so, Plaintiffs and the Class entered into implied contracts with HCA by which HCA agreed to safeguard and protect such information to keep such information secure and confidential, and to timely

and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

314. Notices of Privacy Practices that govern HCA-owned hospitals and other healthcare centers state: "We are required by law to maintain the privacy of your health information."[56]

315. Plaintiffs and Class Members reasonably believed and expected that HCA's data security practices complied with relevant laws and regulations and were consistent with industry standards, and that HCA would thoroughly vet and select vendors that adequately protect Private Information.

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

317. HCA breached this implied covenant of good faith and fair dealing when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC, HIPAA, and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' Private Information; selection of and providing Private Information to a vendor that does not adequately safeguard Private Information; storing the Private Information of former employees, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiffs and Class Members at the time they provided their Private Information to it that HCA's security systems and those of its vendors, e.g., HCA, failed to meet applicable legal and industry standards.

318. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do. Likewise, all conditions required for HCA's performance were met.

[56] *E.g.*, https://www.hcafloridahealthcare.com/legal/notice-of-privacy-practices (last visited Jan. 31, 2024).

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

320. Plaintiffs and Class Members have been or will be harmed by HCA's breach of this implied covenant in the numerous ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Private Information, and the attendant long-term expense of attempting to mitigate and insure against these risks.

321. HCA is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

322. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

323. Plaintiffs and Class Members are also entitled to injunctive relief requiring HCA to, *e.g.*, (i) strengthen its data monitoring procedures; (ii) evaluate, audit, and improve its processes for vetting third party vendors and the selection processes for vendors to which HCA provides sensitive Private Information; (iii) submit to future annual audits of those systems and monitoring procedures; and (iv) immediately provide or continue providing adequate credit monitoring to all Class Members.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Classes)

324. Plaintiffs restate and reallege paragraphs 1 through 247 above as if fully set forth herein.

325. At all times during Plaintiffs' and Class Members' interactions with HCA as its employees, HCA was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information.

326. Plaintiffs' and Class Members' Private Information constitutes confidential and unique information. Indeed, Plaintiffs' and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim.

327. As alleged herein, HCA's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence—both by HCA and its vendors to which it provides that Private Information—and would not be disclosed to unauthorized third parties.

328. Plaintiffs and Class Members provided their respective Private Information to HCA with the explicit and implicit understandings that it would protect and not permit the Private Information to be disseminated to any unauthorized parties.

329. Due to HCA's failure to protect Plaintiffs' and Class Members' Private Information, or retain vendors that protect the Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

330. As a direct and proximate cause of HCA's actions and/or omissions, Plaintiffs and Class Members have suffered damages as alleged herein.

331. But for the disclosure of Plaintiffs' and Class Members' Private Information, in violation of the parties' mutual understanding of confidence including that HCA would only provide Private Information to trusted vendors that adequately safeguard the information, Plaintiffs' and Class

Members' Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information, as well as the resulting damages.

332. The disclosure of Plaintiffs' and Class Members' Private Information, and provision of Private Information to a vendor that does adequately secure Private Information, constitute violations of Plaintiffs' and Class Members' understanding that HCA would safeguard and protect the confidential and unique Private Information.

333. The concrete injury and harm that Plaintiffs and Class Members suffered was the reasonably foreseeable result of HCAs' failure to ensure protection of their Private Information.

334. As a direct and proximate result of HCA's conduct, Plaintiffs and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their Private Information is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in both HCA's possession and is subject to further unauthorized disclosures; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (h) nominal damages.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Classes)

335. Plaintiffs restate and reallege paragraphs 1 through 247 above as if fully set forth herein.

336. This count is pleaded in the alternative to the breach of implied contract claim above against HCA (Count III).

337. Plaintiffs and Class Members conferred a monetary benefit on HCA in connection with obtaining healthcare services, specifically providing HCA with their Private Information. In exchange, Plaintiffs and Class Members should have received from HCA services or benefits that were the subject of the transaction, and should have had their Private Information protected with adequate data security.

338. HCA knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. HCA profited from Plaintiffs' retained data and use Plaintiffs' and Class Members' Private Information for business purposes.

339. HCA failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

340. HCA acquired the Private Information through inequitable record retention as it failed to disclose the inadequate vendor vetting and data security practices previously alleged.

341. If Plaintiffs and Class Members had known HCA would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, or vendors that house their Private Information, they would not have entrusted their

Private Information with HCA.

342. Under the circumstances, it would be unjust for HCA to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

343. As a direct an proximate result of HCA's conduct, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in HCA's possession and is subject to further unauthorized disclosures or further entrustment to inadequate third party vendors so long as HCA fails to undertake appropriate and adequate measures to protect the Private Information; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by HCA's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

344. Plaintiffs and Class Members are entitled to restitution and/or damages from HCA and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by HCA from its wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

345. Plaintiffs and Class Members may not have an adequate remedy at law against

HCA, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VII
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Classes)

346. Plaintiffs restate and reallege paragraphs 1 through 247 above as if fully set forth herein.

347. HCA became the guardian of Plaintiffs' and Class Members' Private Information. HCA became a fiduciary, created by its undertaking and guardianship of Plaintiffs' and Class Members' Private Information, to act primarily for their benefit. This duty included the obligation to safeguard Plaintiffs' and Class Members' Private Information and to timely detect and notify Plaintiffs and Class Members in the event of a data breach.

348. In order to provide Plaintiffs and Class Members healthcare services benefits and compensation, or to even consider Plaintiffs and Class Members for healthcare services, HCA required that they provide their Private Information.

349. HCA knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class Members' Private Information in order to provide them with healthcare services and healthcare services benefits and compensation.

350. HCA has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matter within the scope of its relationship with them. HCA breached its fiduciary duties owed to Plaintiffs and Class Members by failing to properly protect Plaintiffs' and Class Members' Private Information. HCA further breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely detect the Data Breach and notify and/or warn Plaintiffs and Class Members of the Data Breach.

351. As a direct and proximate result of HCA's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their Private Information is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in HCA's possession and is subject to further unauthorized disclosures so long as HCA fails to undertake appropriate and adequate measures to protect Private Information in its continued possession and ensure that it retains vendors who adequately protect Private Information; (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (h) nominal damages.

352. As a direct and proximate result of HCA's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VIII
DECLARATORY JUDGMENT ACT
(On Behalf of Plaintiffs and the Classes)

353. Plaintiffs restate and reallege paragraphs 1 through 247 above as if fully set forth herein.

354. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

355. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether HCA are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that HCA's data security measures and third-party vendor vetting remain inadequate. Furthermore, Plaintiffs continue to suffer injuries as result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

356. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (a) HCA owes a legal duty to secure employees' Private Information, select vendors who handle Private Information that will adequately safeguard that information, and to timely notify impacted individuals of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes, and (b) HCA continues to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

a. Order HCA to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with HCA's explicit or implicit contractual obligations and duties of care, HCA must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. prohibiting HCA from engaging in the wrongful and unlawful acts alleged herein;

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

iii. requiring HCA to delete and purge the Private Information of Plaintiffs and Class Members unless HCA 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 HCA to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring HCA to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on HCA's systems on a periodic basis;

vi. prohibiting HCA from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

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

viii. requiring HCA to conduct regular database scanning and securing checks;

ix. requiring HCA to monitor ingress and egress of all network traffic;

x. requiring HCA 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 Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring HCA 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 HCA's policies, programs, and systems for protecting personal identifying information;

xii. requiring HCA to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor HCA's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring HCA to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

357. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at, or implicating, HCA. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily

quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

358. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to HCA if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to HCA of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and HCA has a pre-existing legal obligation to employ such measures.

359. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at HCA, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

COUNT IX
CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code §§ 56 *et seq.*
(On Behalf of Plaintiff Marcisz and the California Class)

360. Plaintiff Marcisz (for the purposes of this section, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 247 above, as if fully set forth herein.

361. Plaintiff brings this claim on behalf of himself and the California Class.

362. HCA is "a provider of health care," as defined in Cal. Civ. Code §56.05(m), and is therefore subject to the requirements of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

363. At all relevant times, HCA was a health care provider because it had the "purpose of maintaining medical information to make the information available to the individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manager his or her information, or for the diagnosis or treatment of the individual."

364. As a provider of health care or a contractor, HCA is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated or released without patient's authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

365. As a provider of health care or a contractor, HCA is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

366. HCA is a person licensed under California under California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code §§ 4000 *et seq*.

367. Plaintiff Marcisz and California Class Members are "patients" as defined in the CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains."). Furthermore, Plaintiff and California Class Members, as patients and customers of HCA, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on HCA's computer network, and were patients on or before the date of the Data Breach.

368. HCA disclosed "medical information," as defined in CMIA, Cal. Civ. Code 196. § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of HCA's employees, which allowed the hacker to see and obtain Plaintiff and California Class Members' medical information.

369. HCA negligently created, maintained, preserved, stored, and then exposed Plaintiff

and California Class Members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff and California Class Members' names, cities, states, zip codes, emails, telephone numbers, dates of birth, gender, patient service dates, patient service locations, and next appointment dates, that alone or in combination with other publicly available information, reveals their identities. Specifically, HCA knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access and actually view Plaintiff and California Class Members' confidential Private Information.

370. HCA's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and California Class Members to unauthorized persons and the breach of the confidentiality of that information. HCA's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff and California 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).

371. HCA also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

372. Plaintiff and California Class Members' medical information was accessed, removed and actually viewed by a hacker and other unauthorized parties during and following the Data Breach.

373. Plaintiff and California Class Members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

374. HCA's computer systems did not protect and preserve the integrity of electronic

medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of HCA's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the California Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (a) present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (b) invasion of privacy, (c) breach of the confidentiality of the PHI, (d) statutory damages under the CMIA, (e) deprivation of the value of their PHI, for which there is well-established national and international markets, and/or, (f) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

375. As a direct and proximate result of HCA's wrongful actions, inaction, omission, and want of ordinary care that directly and proximately caused the release of Plaintiff and California Class Members' Private Information, Plaintiff and California Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff and California Class Members' written authorization.

376. HCA's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff and California Class Members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

377. Plaintiff and the California Class Members were injured and have suffered damages, as described above, from HCA's illegal and unauthorized 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, which allows for actual damages, nominal statutory

damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT X
CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code §§ 17200 *et seq.*
(On Behalf of Plaintiff Marcisz and the California Class)

378. Plaintiff Marcisz (for the purposes of this section, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 247 above, as if fully set forth herein.

379. Plaintiff brings this claim on behalf of himself and the California Class.

380. HCA is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

381. HCA violated Cal. Bus. & Prof. Code §§ 17200 *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

382. HCA's "unfair" acts and practices include:

a. HCA failed to implement and maintain reasonable security measures to protect Plaintiff's and California Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. HCA failed to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as alleged herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and California Class Members, whose Private Information has been compromised;

c. HCA's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data

and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100;

d. HCA's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as alleged above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of HCA's grossly inadequate security, consumers could not have reasonably avoided the harms that HCA caused; and

e. HCA engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

383. HCA has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures), the FTC Act, 15 U.S.C. § 45, and California common law.

384. HCA's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Class Members' Private Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and California Class Members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

h. Failing to provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

385. HCA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of HCA's data security and ability to protect the confidentiality of consumers' Private Information.

386. As a direct and proximate result of HCA's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Class Members were injured and suffered monetary and non-

monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for HCA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

387. HCA acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Class Members' rights.

388. Plaintiff and California Class Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from HCA's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT XI
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FUDTPA")
Fla. Stat. §§ 501.201 *et seq.*
(On Behalf of Plaintiffs Crossman, Del Vecchio, Jordan, Silvers, and Simon and the Florida Class)

389. Plaintiffs Crossman, Del Vecchio, Jordan, Silvers, and Simon (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 247 above, as if fully set forth herein.

390. Plaintiffs bring this claim on behalf of themselves and the Florida Class.

391. Plaintiffs and Florida Class Members are "consumers" as defined by Fla. Stat. § 501.203.

392. HCA advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

393. HCA engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Florida Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Florida Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Florida Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2).

394. HCA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of HCA's data security and ability to protect the confidentiality of consumers' Private Information.

395. HCA intended to mislead Plaintiffs and Florida Class Members and induce them to rely on its misrepresentations and omissions.

396. Had HCA disclosed to Plaintiffs and Florida Class Members that its data systems were not secure and, thus, were vulnerable to attack, HCA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. HCA was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and Florida Class Members. HCA accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Florida Class Members acted reasonably in relying on HCA's misrepresentations and omissions, the truth of which they could not have discovered.

397. As a direct and proximate result of HCA's unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for HCA's services; loss of the

value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

398. Plaintiffs and Florida Class Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

COUNT XII
KANSAS CONSUMER PROTECTION ACT
Kan. Stat. Ann. §§ 50-623 *et seq.*
(On Behalf of Plaintiff Hinds and the Kansas Class)

399. Plaintiff Hinds (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 247 above, as if fully set forth herein.

400. Plaintiff brings this claim on behalf of herself and the Kansas Class.

401. K.S.A. §§ 50-623 *et seq*. is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

402. Plaintiff and Kansas Class Members are "consumers" as defined by K.S.A. § 50-624(b).

403. The acts and practices alleged herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

404. HCA is a "supplier" as defined by K.S.A. § 50-624(l).

405. HCA advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

406. HCA engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Kansas Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas' identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Kansas Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, Kansas' identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Kansas Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Class Members' Private Information, including duties imposed by

the FTC Act, 15 U.S.C. § 45, and Kansas' identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b; and

h. Omitting, suppressing, and concealing the material fact that it did not implement and maintain reasonable security and privacy measures to protect Plaintiff's and Kansas Class Members' Private Information, which was a direct and proximate cause of the Data Breach.

407. HCA' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of HCA' data security and ability to protect the confidentiality of consumers' Private Information.

408. HCA intended to mislead Plaintiff and Kansas Class Members and induce them to rely on its misrepresentations and omissions.

409. Had HCA disclosed to Plaintiff and Kansas Class Members that its data systems were not secure and, thus, vulnerable to attack, HCA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. HCA was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and Kansas Class Members. HCA accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Kansas Class Members acted reasonably in relying on HCA' misrepresentations and omissions, the truth of which they could not have discovered.

410. HCA also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Class to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and the Kansas Class to enter into a consumer transaction on terms that HCA knew were substantially one-sided in favor of HCA (see K.S.A. § 50- 627(b)(5)).

411. Plaintiff and the Kansas Class had unequal bargaining power with respect to their ability to control the security and confidentiality of their Private Information in HCA' possession.

412. The above unfair, deceptive, and unconscionable practices and acts by HCA were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

413. HCA acted intentionally, knowingly, and maliciously to violate Kansas' Consumer Protection Act, and recklessly disregarded Plaintiff's and Kansas Class Members' rights.

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

415. Plaintiff will provide notice of this action to the Attorney General of Kansas.

416. Plaintiff and Kansas Class Members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XIII
KENTUCKY CONSUMER PROTECTION ACT
Ky. Rev. Stat. §§ 367.110 *et seq.*
(On Behalf of Plaintiff Watkins and the Kentucky Class)

417. Plaintiff Watkins (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 247 above, as if fully set forth herein.

418. Plaintiff brings this claim on behalf of himself and the Kentucky Class.

419. HCA is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

420. HCA advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

421. HCA engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised;

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have

entered had the information been disclosed.

422. HCA's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Kentucky Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Kentucky Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Kentucky Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Kentucky Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Kentucky Class Members' Private Information; and

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

Plaintiffs' and Kentucky Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164.

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

424. HCA intended to mislead Plaintiff and Kentucky Class Members and induce them to rely on its misrepresentations and omissions.

425. Plaintiff and Kentucky Class Members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of HCA's unlawful acts and practices.

426. The above unlawful acts and practices by HCA were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

427. HCA acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Class Members' rights. HCA's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

428. As a direct and proximate result of HCA's unlawful acts and practices, Plaintiff and Kentucky Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII;

overpayment for HCA's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

429. Plaintiff and Kentucky Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

COUNT XIV
TENNESSEE CONSUMER PROTECTION ACT
Tenn. Code Ann. §§ 47-18-101 *et seq.*
(On Behalf of Plaintiff Walters and the Tennessee Class)

430. Plaintiff Walters (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 247 above, as if fully set forth herein.

431. Plaintiff brings this claim on behalf of herself and the Tennessee Class.

432. HCA is a "person," as defined by Tenn. Code § 47-18-103(13).

433. Plaintiff and Tennessee Class Members are "consumers," as meant by Tenn. Code § 47-18-103(2).

434. HCA advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

435. HCA advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And HCA's acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

436. HCA's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Tennessee Class Members' Private Information, which

was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Tennessee Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Tennessee Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Tennessee Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Tennessee Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Tennessee Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164.

437. HCA intended to mislead Plaintiff and Tennessee Class Members and induce them to rely on its misrepresentations and omissions.

438. HCA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of HCA's data security and ability to protect the confidentiality of consumers' Private Information.

439. Had HCA disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, HCA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. HCA was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Class. HCA accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Class Members acted reasonably in relying on HCA's misrepresentations and omissions, the truth of which they could not have discovered.

440. HCA had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the Private Information in its possession, and the generally accepted professional standards. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Tennessee Class, and HCA because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in HCA. HCA's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Tennessee Class that contradicted these representations.

441. HCA's "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

442. The injury to consumers was and is substantial because it was non-trivial and non-speculative, and involved a monetary injury and/or an unwarranted risk to the safety of their Private Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

443. Consumers could not have reasonably avoided injury because HCA's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, HCA created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

444. HCA's inadequate data security had no countervailing benefit to consumers or to competition.

445. By misrepresenting and omitting material facts about its data security and failing to comply with its common law and statutory duties pertaining to data security (including its duties under the FTC Act), HCA violated the following provisions of Tenn. Code § 47-18-104(b):

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve.

446. HCA acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiff and Tennessee Class Members' rights. HCA's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

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

448. HCA's violations present a continuing risk to Plaintiff and Tennessee Class Members as well as to the general public.

449. Plaintiff and Tennessee Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

COUNT XV
TEXAS DECEPTIVE TRADE PRACTICES–CONSUMER PROTECTION ACT
Texas Bus. & Com. Code §§ 17.41 *et seq.*
(On Behalf of Plaintiffs Dekenipp, Menard, Tighe, and Womack and the Texas Class)

450. Plaintiffs Dekenipp, Menard, Tighe, and Womack (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 247 above, as if fully set forth herein.

451. Plaintiffs bring this claim on behalf of themselves and the Texas Class.

452. HCA is a "person," as defined by the Texas Trade Practices–Consumer Protection Act ("DTPA"), Tex. Bus. & Com. Code § 17.45(3).

453. Plaintiffs and the Texas Class Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

454. HCA advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

455. HCA engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised;

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

456. HCA's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Texas Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Texas Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Texas Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and Texas' data security statute, Tex. Bus. & Com. Code § 521.052.

457. HCA intended to mislead Plaintiffs and Texas Class Members and induce them to

rely on its misrepresentations and omissions.

458. HCA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of HCA's data security and ability to protect the confidentiality of consumers' Private Information.

459. Had HCA disclosed to Plaintiffs and Texas Class Members that its data systems were not secure and, thus, vulnerable to attack, HCA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. HCA was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and Texas Class Members. HCA accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Texas Class Members acted reasonably in relying on HCA's misrepresentations and omissions, the truth of which they could not have discovered.

460. HCA had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and Texas Class Members, and HCA because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in HCA. HCA's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiffs and Texas

Class Members that contradicted these representations.

461. HCA engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). HCA engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

462. Consumers, including Plaintiffs and Texas Class Members, lacked knowledge about deficiencies in HCA's data security because this information was known exclusively by HCA. Consumers also lacked the ability, experience, or capacity to secure the Private Information in HCA's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Class Members lack expertise in information security matters and do not have access to HCA's systems in order to evaluate its security controls. HCA took advantage of its special skill and access to Private Information to hide its inability to protect the security and confidentiality of Plaintiffs' and Texas Class Members' Private Information.

463. HCA intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from HCA's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from HCA's unconscionable business acts and practices, exposed Plaintiffs and Texas Class Members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Class Members cannot mitigate this unfairness because they cannot undo the Data Breach.

464. HCA acted intentionally, knowingly, and maliciously to violate Texas' Deceptive Trade Practices–Consumer Protection Act, and recklessly disregarded Plaintiffs' and Texas Class

Members' rights.

465. As a direct and proximate result of HCA's unconscionable and deceptive acts or practices, Plaintiffs and Texas Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for HCA's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach. HCA's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Class Members' injuries, ascertainable losses, economic damages, and non- economic damages, including their mental anguish.

466. HCA's violations present a continuing risk to Plaintiffs and Texas Class Members, as well as to the general public.

467. On February 2, 2024, counsel for Plaintiffs provided written notice via certified mail to HCA of the intent to pursue claims under the DTPA and an opportunity for HCA to cure. Plaintiffs' written notice set forth the violations of HCA's duty to implement and maintain reasonable security procedures and practices alleged in this Complaint.

468. Contemporaneous with the filing of this Complaint, pursuant to Tex. Bus. & Com. Code Ann. § 17.501, Plaintiffs' counsel will send to the Consumer Protection Division a copy of the written notice sent to HCA.

469. Plaintiffs and Texas Class Members seek damages, including economic damages, damages for mental anguish, statutory damages in the amount of three times the economic and mental anguish damages, as HCA's acts were committed intentionally or knowingly, injunctive relief, other

equitable relief the Court deems proper, costs, and reasonable and necessary attorneys' fees.

COUNT XVI
VIRGINA CONSUMER PROTECTION ACT
Va. Code Ann. §§ 59.1-196 *et seq.*
(On Behalf of Plaintiff J.B. and the Virginia Class)

470. Plaintiff J.B. (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 247 above, as if fully set forth herein.

471. Plaintiff brings this claim on behalf of himself and the Virginia Class.

472. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

473. HCA is a "person" as defined by Va. Code Ann. § 59.1-198.

474. HCA is a "supplier," as defined by Va. Code Ann. § 59.1-198.

475. HCA engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. HCA advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

476. HCA engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Texas Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Texas Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Texas Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164.

477. HCA intended to mislead Plaintiff and Virginia Class Members and induce them to rely on its misrepresentations and omissions.

478. HCA's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Virginia Class Members, about the adequacy of HCA's computer and data security and the quality of the HCA brand.

479. Had HCA disclosed to Plaintiffs and Class Members that its data systems were not

secure and, thus, vulnerable to attack, HCA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. HCA was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Class. HCA accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Class Members acted reasonably in relying on HCA's misrepresentations and omissions, the truth of which they could not have discovered.

480. HCA had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers including Plaintiff and the Virginia Class—and HCA, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in HCA. HCA's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiffs and Texas Class Members that contradicted these representations.

481. The above-described deceptive acts and practices also violated the following provisions of Va. Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain characteristics, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised;

d. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.

482. HCA acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Class Members' rights. HCA's numerous past data breaches put it on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish HCA for its wrongdoing, and warn or deter others from engaging in similar conduct.

483. As a direct and proximate result of HCA's deceptive acts or practices, Plaintiffs and Virginia Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for HCA's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

484. HCA's violations present a continuing risk to Plaintiffs and Virginia Class Members as well as to the general public.

485. Plaintiff and Virginia Class Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief;

punitive damages; and attorneys' fees and costs.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the class, respectfully request that the Court enter judgment in Plaintiffs' favor and against HCA as follows:

A. Certifying the Class(es) as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: February 2, 2024.

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (BPR 23045)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
E: gstranch@stranchlaw.com

Jean S. Martin (admitted *pro hac vice*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 559-4908
E: jeanmartin@forthepeople.com

Co-Lead Counsel for Plaintiffs

Jillian Dent (admitted *pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
E: dent@stuevesiegel.com

Gary Klinger (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
E: gklinger@milberg.com

Jeff Ostrow (admitted *pro hac vice*)
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
E: ostrow@kolawyers.com

James Pizzirusso (admitted *pro hac vice*)
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, DC 20006
Tel: (202) 540-7200
E: jpizzirusso@hausfeld.com

Sabita J. Soneji (admitted *pro hac vice*)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Tel: (510) 254-6808
E: ssoneji@tzlegal.com

Plaintiffs' Executive Committee

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing has been served via email via the CM/ECF system on all counsel of record on this 2nd day of February, 2024, as follows:

Andrew J. Shamis
Shamis & Gentile, PA
14 NE 1st Avenue
Suite 1205
Miami, FL 33132
(305) 479-2299
Fax: (786) 623-0915
Email:
ashamis@shamisgentile.com

Jeffrey M. Ostrow
Kopelowitz Ostrow P.A.
One West Las Olas Blvd
Suite 500
Fort Lauderdale, FL 33301
954-525-4100
Fax: 954-525-4300
Email: ostrow@kolawyers.com

Kristen Lake Cardoso
Kopelowitz Ostrow P.A.
One West Las Olas Blvd
Suite 500
Fort Lauderdale, FL 33301
954-990-2218
Fax: 954-525-4300
Email: cardoso@kolawyers.com

Steven Sukert
Kopelowitz Ostrow P.A.
One West Las Olas Blvd
Suite 500
Fort Lauderdale, FL 33301
954-284-1520
Fax: 954-525-4300
Email: sukert@kolawyers.com

William B. Federman
Federman & Sherwood
10205 N Pennsylvania Avenue
Oklahoma City, OK 73120
(405) 235-1560
Fax: (405) 239-2112
Email: wbf@federmanlaw.com

Alexandra M. Honeycutt
Milberg Coleman Bryson Phillips Grossman, PLLC
800 S. Gay Street
Suite 1100
Knoxville, TN 37929
865-247-0080
Fax: 865-522-0049
Email: ahoneycutt@milberg.com

David K. Lietz
Milberg Coleman Bryson Phillips Grossman, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, DC 20015
866-252-0878
Fax: 202-686-2877
Email: dlietz@milberg.com

Gary M. Klinger
Milberg Grossman Bryson Phillips Grossman PLLC
227 W. Monroe Street
Suite 2100
Chicago, IL 60606
866-252-0878
Email: gklinger@milberg.com

J. Corey Asay
Morgan & Morgan (Lexington Office)
333 W. Vine St.
Suite 1200
Lexington, KY 40507

(859) 286-8368
Fax: (859) 286-8384
Email: casay@hkm.com

Anthony A. Orlandi
Benjamin A. Gastel
Joey P. Leniski
Tricia Herzfeld
Herzfeld, Suetholz, Gastel, Leniski & Wall, PLLC
223 Rosa L Parks Ave
Suite 300
Nashville, TN 37203
615-800-6225
Email: tony@hsglawgroup.com
Email: ben@hsglawgroup.com
Email: joey@hsglawgroup.com
Email: tricia@hsglawgroup.com

Brandon P. Jack
Arnold Law Firm
865 Howe Avenue
Sacramento, CA 92825
916-239-4784
Email: bjack@justice4you.com

Gregory Haroutunian
Arnold Law Firm
865 Howe Avenue
Sacramento, CA 92825
916-777-7777
Email:
gharoutunian@justice4you.com

M. Anderson Berry
Arnold Law Firm
865 Howe Avenue
Sacramento, CA 92825
916-777-7777
Email: aberry@justice4you.com

Jalle H. Dafa
Lieff, Cabraser, Heimann & Bernstein, LLP (San Francisco)
275 Battery Street
29th Floor
San Francisco, CA 94111-3339
(415) 956-1000
Email: jdafa@lchb.com
Jason Lichtman
Lieff, Cabraser, Heimann & Bernstein, LLP
250 Hudson Street
8th Floor
New York, NY 10013-1413
(212) 355-9500
Email: jlichtman@lchb.com

John Tate Spragens
Spragens Law PLC
311 22nd Ave. N.
Nashville, TN 37203
(615) 983-8900
Fax: (615) 682-8533
Email: john@spragenslaw.com

Kenneth S. Byrd
Lieff, Cabraser, Heimann & Bernstein, LLP (Nashville Office)
222 2nd Avenue South
Suite 1640
Nashville, TN 37201
(615) 313-9000
Fax: (615) 313-9965
Email: kbyrd@lchb.com

Mark P. Chalos
Lieff, Cabraser, Heimann & Bernstein, LLP (Nashville Office)
222 2nd Avenue South
Suite 1640
Nashville, TN 37201
(615) 313-9000
Email: mchalos@lchb.com

Michael W. Sobol
Lieff, Cabraser, Heimann &
Bernstein, LLP
275 Battery Street
30th Floor
San Francisco, CA 94111-3339
(415) 956-1000
Email: msobol@lchb.com

Bart D. Cohen
Bailey Glasser LLP
1622 Locust Street
Philadelphia, PA 19103
304-345-6555
Fax: 304-342-1110
Email: bcohen@baileyglasser.com

Abby E. McClellan Paradise
Stueve Siegel Hanson LLP
460 Nichols Road
Ste 200
Kansas City, MO 64112
816-714-7100
Fax: 816-714-7101
Email: mcclellan@stuevesiegel.com

Brandi S. Spates
Stueve Siegel Hanson LLP
460 Nichols Road
Ste 200
Kansas City, MO 64112
816-714-7100
Email: spates@stuevesiegel.com

Jillian R. Dent
460 Nichols Road
Suite 200
Kansas City, MO 64112
(816) 714-7100
Email: dent@stuevesiegel.com

John Austin Moore
Stueve Siegel Hanson LLP
460 Nichols Road
Ste 200
Kansas City, MO 64112
(816) 714-7100
Email: moore@stuevesiegel.com

Norman Siegel
Stueve Siegel Hanson LLP
460 Nichols Road
Suite 200
Kansas City, MO 64112
816-714-7100
Email: siegel@stuevesiegel.com

Gary S. Graifman
Kantrowitz, Goldhamer &
Graifman, P.C.
747 Chestnut Ridge Road
Suite 200
Chestnut Ridge, NY 10977
(845) 356-2570
Fax: (845) 356-4335
Email: ggraifman@kgglaw.com

Melissa R. Emert
Kantrowitz, Goldhamer &
Graifman, P.C.
747 Chestnut Ridge Road
Suite 200
Chestnut Ridge, NY 10977
(845) 356-2570
Fax: (845) 356-4335
Email: memert@kgglaw.com

Adam S. Nightingale
Eastman & Smith Ltd.
One SeaGate, 17th Floor
P O Box 10032
Toledo, OH 43604
(419) 247-1728
Email:
asnightingale@eastmansmith.com

Amanda V. Boltax
Hausfeld LLP
888 16th Street, NW
Suite 300
Washington, DC 20006
516-477-8339
Email: mboltax@hausfeld.com

James J. Pizzirusso
Hausfeld LLP
888 16th Street, NW
Suite 300
Washington, DC 20006
202-540-7200
Email: jpizzirusso@hausfeld.com

Steven M. Nathan
Hausfeld LLP
33 Whitehall Street
14th Floor
New York, NY 1100
646-357-1100
Fax: 212-202-4322
Email: snathan@hausfeld.com

Francesca K. Burne
Morgan & Morgan (Tampa Office)
201 N Franklin Street
7th Floor
Tampa, FL 33602
813-424-5618
Email: fburne@forthepeople.com
ATTORNEY TO BE NOTICED

Jean Sutton Martin
Morgan & Morgan (Tampa Office)
201 N Franklin Street
7th Floor
Tampa, FL 33602
(813) 223-5505
Fax: (813) 221-7366
Email:
jeanmartin@forthepeople.com
ATTORNEY TO BE NOTICED

Robert B. Keaty , II
Morgan & Morgan (Nashville Office)
810 Broadway
Suite 105
Nashville, TN 37203
(615) 928-9901
Email: bkeaty@forthepeople.com
ATTORNEY TO BE NOTICED

James E. Cecchi
Carella, Byrne, Cecchi, Olstein, Brody & Agnello, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
Email: jcecchi@carellabyrne.com

Jason H. Alperstein
Carella, Byrne, Cecchi, Olstein, Brody & Agnello, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
Email:
jalperstein@carellabyrne.com

Lori G. Feldman
George Feldman McDonald PLLC
102 Half Moon Bay Drive
Croton on Hudson, NY 10520
917-983-9321
Fax: 888-421-4173
Email: lfeldman@4-Justice.com

Lucy McShane
McShane & Brady, LLC
1656 Washington Street
Suite 120
Kansas City, MO 64108
(816) 888-8010
Email:
lmcshane@mcshanebradylaw.com

Maureen M. Brady
McShane & Brady, LLC
1656 Washington Street
Suite 120
Kansas City, MO 64108
816-888-8010
Email:
mbrady@mcshanebradylaw.com

Michael Liskow
George Feldman McDonald, PLLC
745 Fifth Ave
Suite 500
New York, NY 10151
561-232-6002
Email: mliskow@4-justice.com

John G. Emerson
Emerson Firm, PLLC
2500 Wilcrest Drive
Suite 300
Houston, TX 77042
(800) 551-8649
Fax: (501) 286-4659
Email:
jemerson@emersonfirm.com

Samuel M. Ward
Barrack, Rodos & Bacine
One America Plaza
600 W Broadway
Suite 900
San Diego, CA 92101
(619) 230-0800
Fax: (619) 230-1874
Email: sward@barrack.com

Sidney W. Gilreath
Gilreath & Associates
550 Main Street
Suite 600
Knoxville, TN 37902-1270
(865) 637-2442
Email: gilknox@sidgilreath.com

Stephen R. Basser
Barrack, Rodos & Bacine
One America Plaza
600 W Broadway
Suite 900
San Diego, CA 92101
(619) 230-0800
Fax: (619) 230-1874
Email: sbasser@barrack.com

Gemma Seidita
2000 Pennsylvania Avenue
Suite 1010
Washington, DC 20006
202-964-7691
Email: gseidita@tzlegal.com

Sabita J. Soneji
Tycko & Zavareei LLP
1970 Broadway
Suite 1070
Oakland, CA 94612
510-254-6808
Email: ssoneji@tzlegal.com

Brian C. Gudmundson
Zimmerman Reed, PLLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
612-341-0400
Email:
brian.gudmundson@zimmreed.com

Charles R. Toomajian III
Zimmerman Reed, PLLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
(612) 341-0400
Email:
charles.toomajian@zimmreed.com

Rachel K. Tack
Zimmerman Reed, PLLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
612-341-0400
Email: rachel.tack@zimmreed.com

David A. McLaughlin
901Attorneys, LLC
200 Jefferson Avenue
Suite 900

Memphis, TN 38103
901-671-1551
Fax: 901-671-1571
Email: david@901attorneys.com
ATTORNEY TO BE NOTICED

Gary F. Lynch
Lynch Carpenter, LLP
1133 Penn Avenue
5th Floor
Pittsburgh, PA 15222
412-322-9243
Email: gary@lcllp.com
ATTORNEY TO BE NOTICED

Kelly Iverson
Lynch Carpenter LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
412-322-9243
Email: kelly@lcllp.com
ATTORNEY TO BE NOTICED

Nicholas A. Colella
Lynch Carpenter LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
(412) 322-9243
Fax: (412) 231-0246
Email: nickc@lcllp.com
ATTORNEY TO BE NOTICED

Cecily C. Jordan
Tousley Brain Stephens PLLC
1200 Fifth Avenue
Suite 1700
Seattle, WA 98101
(206) 682-5600
Fax: (206) 682-2992
Email: cjordan@tousley.com
ATTORNEY TO BE NOTICED

Kim D. Stephens
Tousley Brain Stephens PLLC
1200 Fifth Avenue
Suite 1700
Seattle, WA 98101
(206) 682-5600
Fax: (206) 682-2992
Email: kstephens@tousley.com

Ari Y. Basser
Pomerantz LLP (CA Office)
1100 Glendon Ave
15th Floor
Los Angeles, CA 90024
310-432-8492
Email: abasser@pomlaw.com

Jordan L. Lurie
Capstone Law APC
1875 Century Park East
Suite 1000
Los Angeles, CA 90067
(310) 556-4811
Fax: (310) 943-0396
Email:
Jordan.Lurie@capstonelawyers.com

Paul Kent Bramlett
Bramlett Law Offices
40 Burton Hills Blvd.
Suite 200
P O Box 150734
Nashville, TN 37215
(615) 248-2828
Fax: (615) 254-4116
Email: pknashlaw@aol.com

Robert P. Bramlett
Bramlett Law Offices
40 Burton Hills Blvd.
Suite 200
P O Box 150734
Nashville, TN 37215
(615) 248-2828
Fax: (615) 254-4116
Email:
robert@bramlettlawoffices.com

Claire Torchiana
Cohen, Milstein, Sellers & Toll

PLLC (NY Office)
88 Pine Street
14th Floor
New York, NY 10005
(212) 838-7797
Email:
ctorchiana@cohenmilstein.com

Douglas J. McNamara
Cohen Milstein Sellers & Toll
PLLC
1100 New York Avenue N.W.
Suite 500
Washington, DC 20005
202-408-4600
Fax: 202-408-4699
Email:
dmcnamara@cohenmilstein.com

Krysta Kauble Pachman
Susman Godfrey L.L.P.
1900 Avenue of the Stars
Suite 1400
Los Angeles, CA 90067
(310) 789-3100
Email:
kpachman@susmangodfrey.com

Stephen E. Morrissey
Susman Godfrey LLP
401 Union Street
Suite 3000
Seattle, WA 98101
(206) 516-3880
Email:
smorrissey@susmangodfrey.com

Vineet Bhatia
Susman Godfrey LLP
1000 Louisiana Street
Suite 5100
Houston, TX 77002-5096
(713) 653-7855
Email:
vbhatia@susmangodfrey.com

Hannah R. Lazarz
Lieff, Cabraser, Heimann &
Bernstein, LLP (Nashville Office)
222 2nd Avenue South
Suite 1640
Nashville, TN 37201
(765) 418-7273
Email: hlazarz@lchb.com

Blake G. Abbott
Poulin / Willey Anastopoulo, LLC
32 Ann Street
Charleston, SC 29403
843-614-8888
Email:
blake.abbott@poulinwilley.com

Paul J. Doolittle
Poulin / Willey Anastopoulo, LLC
32 Ann Street
Charleston, SC 29403
843-834-4712
Email:
paul.doolittle@poulinwilley.com

Annemarie Janine De Bartolomeo
Tadler Law LLP
22 Bayview Avenue
Suite 200
Manhasset, NY 11030
(212) 946-9300
Email: ajd@tadlerlaw.com

Ariana J. Tadler
Tadler Law LLP
22 Bayview Avenue
Suite 200
Manhasset, NY 11030
212-946-9453
Fax: 646-844-0331
Email: atadler@tadlerlaw.com

Michael Kind
Kind Law
8860 S. Maryland Parkway
Suite 106

Las Vegas, NV 89123
(702) 337-2322
Fax: (702) 329-5881
Email: mk@kindlaw.com

Andrew B. Clubok
Latham & Watkins LLP (DC Office)
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004-1304
202-637-2200
Email: andrew.clubok@kirkland.com

Kathryn Hannen Walker
Bass, Berry & Sims (Nashville Office)
150 Third Avenue South
Suite 2800
Nashville, TN 37201
615-742-7855
Email: kwalker@bassberry.com

Marissa Alter-Nelson
Latham & Watkins LLP (NY Office)
1271 Avenue of the Americas
New York, NY 10020-1345
212-906-1200
Email: marissa.alter-nelson@lw.com

Melanie M. Blunschi
Latham & Watkins LLP
505 Montgomery Street
Suite 2000
San Francisco, CA 94111
415-391-0600
Email: melanie.blunschi@lw.com

Peter C. Rathmell
Bass, Berry & Sims (Nashville Office)
150 Third Avenue South
Suite 2800
Nashville, TN 37201
(615) 742-6268
Email: peter.rathmell@bassberry.com

Susan E. Engel
Latham & Watkins LLP (DC Office)
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004-1304
202-637-2200
Fax: 202-637-2201
Email: susan.engel@lw.com

Taylor M. Sample
Bass, Berry & Sims (Nashville Office)
150 Third Avenue South
Suite 2800
Nashville, TN 37201
615-742-7909
Email: taylor.sample@bassberry.com

W. Brantley Phillips , Jr.
Bass, Berry & Sims (Nashville Office)
150 Third Avenue South
Suite 2800
Nashville, TN 37201
615-742-6200
Email: bphillips@bassberry.com

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV