Exhibit A

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
CHATTANOOGA DIVISION

STEPHEN CAHILL, *et al.*, individually and on behalf of all others similarly situated, Plaintiffs, v. MEMORIAL HEART INSTITUTE, LLC, d/b/a THE CHATTANOOGA HEART INSTITUTE, Defendant.	CASE NO.: 1:23-cv-00168-CLC-CHS Judge Curtis Collier

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Stephen Cahill, Sheila Edwards, Sidney Jackson, Christopher Cordes, Gisele Reed Allen, Jeff Bryden, and Elyn Painter ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Memorial Heart Institute, LLC d/b/a The Chattanooga Heart Institute ("Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") and protected health information ("PHI") including, but not limited to, name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance

information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information (collectively, "Private Information").

2. Defendant is a healthcare network headquartered in Chattanooga, Tennessee that primarily serves patients in Tennessee and Georgia.[1]

3. Plaintiffs and Class Members are current or former patients of Defendant.

4. On April 17, 2023, Defendant "identified indications of a cybersecurity attack on its IT network" (the "Data Breach"). Defendant launched a forensic investigation that "determined that an unauthorized third party gained access to [Defendant's] network between March 8, 2023, and March 16, 2023."[2]

5. Through the ransomware attack, criminal cyberthieves accessed and exfiltrated Plaintiffs' and Class Members' Private Information.

6. "On May 31, 2023, The Chattanooga Heart Institute learned that the unauthorized third party obtained copies of some of the data from its systems containing confidential patient information."[3]

7. Based upon the investigation, Defendant originally determined that approximately 170,450 individuals had their personal and private information accessed in the Data Breach.[4] Defendant has since supplemented this determination and now reports that the total number of affected persons is 411,383.[5]

---

[1] *The Chattanooga Heart Institute Data Breach Notification*, Me. Att'y Gen., https://apps.web.maine.gov/online/aeviewer/ME/40/24964dbe-2bcc-43d9-ad8a-cbe2b9e0aff0.shtml (last visited Nov. 2, 2023).
[2] *The Chattanooga Heart Institute Notice of Data Security Incident*, https://www.chattanoogaheart.com/the-chattanooga-heart-institute-notice-of-data-security-incident/ (last visited Nov. 2, 2023).
[3] *Id.*
[4] *Chattanooga Heart Institute Data Breach Notification*, *supra* note 1.
[5] *Id.*

8. The information accessed constituted PHI and PII.

9. Despite first becoming aware of the Data Breach on or around April 17, 2023, Defendant only notified less than half of the Plaintiffs and Class Members on or around July 28, 2023, and ultimately notified the additional Class Members on or about October 6, 2023. ("Notice of Data Breach").[6]

10. As part of the Notice of Data Breach, Defendant disclosed that "[t]he information that could have been subject to unauthorized access includes name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information."[7]

11. As a result of the Data Breach, Plaintiffs and over 411,000 Class Members suffered injury and ascertainable losses in the form of the present and imminent substantial threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their personal information.

12. Plaintiffs' and Class Members' sensitive confidential Private Information was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third-party cybercriminals, also remains in the possession of Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to additional hackers and theft.

---

[6] An exemplar of the first notice sent on or about July 28, 2023, is attached as **Exhibit A**, and the Supplemental Notice sent on or about October 6, 2023, is attached as **Exhibit B**.

[7] *Chattanooga Heart Notice of Data Security Incident*, *supra* note 2.

13. Particularly alarming is the fact that the Private Information compromised in the Data Breach included Social Security numbers and other immutable information, which are durable and difficult to change.

14. Further, following the Data Breach, Karakurt, a financially motivated cybercrime group that steals data before demanding payment from victims by threatening its publication, publicly claimed responsibility for the Data Breach.

15. Defendant did not notify Plaintiffs and all Class Members that their Private Information was subject to unauthorized access and exfiltration resulting from the Data Breach until as late as October 6, 2023.

16. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

17. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

18. Upon information and belief, Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks and ransomware malware.

19. The mechanism of the hacking and potential for improper disclosure of Private Information was a known risk to Defendant and entities like it, and thus Defendant was on notice

that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition and vulnerable to theft.

20. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiffs and Class Members prompt notice of the Data Breach.

21. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

22. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

23. Moreover, as a result of the Data Breach, given the criminal targeting of the Private Information, the sensitive nature of the Private Information, the likelihood of exfiltration, and reports of actual fraud following the Data Breach, Plaintiffs and Class Members are now experiencing a current, imminent, ongoing, and substantial risk of fraud and identity theft. The risk of identity theft is not speculative or hypothetical but is impending and has materialized.

24. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent, substantial risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

25. By waiting to notify Plaintiffs and Class Members, Defendant harmed Plaintiffs and Class Members. Put differently, if Defendant notified Plaintiffs and Class Members at or around the time the Data Breach was first discovered, Plaintiffs and Class Members would be in a better position to protect themselves.

26. Even though Defendant offered inadequate credit monitoring services for a limited period of time, Plaintiffs and Class Members will incur out of pocket costs including but not limited to purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft beyond the inadequate services offered by Defendant.

27. Plaintiffs and Class Members suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) out-of-pocket expenses associated with prevention, detection, and recovery from identity theft, tax fraud and/or unauthorized use of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) lost or diminished value of their Private Information; (v) loss of benefit of the bargain; (vi) future costs of ongoing credit and identity theft monitoring; (vii) statutory damages; (viii); nominal damages; (ix) and the ongoing risk of harm as long as Defendant maintains Plaintiffs and Class Members' Private Information with inadequate security practices.

28. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

29. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

30. Plaintiffs also seek injunctive and equitable relief to prevent future injury on behalf of themselves and the putative Class.

PARTIES

Plaintiff Stephen Cahill

31. Plaintiff Stephen Cahill is, and at all times mentioned herein was, an individual citizen of the State of Tennessee, residing in the city of Chattanooga, and is a patient of Chattanooga Heart Institute.

32. Plaintiff Cahill received a Notice of Data Breach Letter from Chattanooga Heart Institute dated July 28, 2023. It states that the breached files included his "name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information."

33. Plaintiff Cahill is especially alarmed and anxious that his Social Security number and extremely private health information (PHI) was identified as among the breached data on Defendant's computer system.

34. Plaintiff Cahill spends approximately thirty (30) minutes a week monitoring his financial accounts. He has also spent time since Defendant's Data Breach freezing his credit, deleting increased and annoying spam, and signing up for credit monitoring (with some difficulty doing so). The time he has spent dealing with these incidents resulting from the Data Breach is time Plaintiff Cahill otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Cahill lost was spent at Defendant's recommendations.

35. Since the Data Breach, and in addition to the injuries alleged above, Plaintiff Cahill also experienced actual identity theft and fraud, by virtue of his Private Information being stolen.

36. Plaintiff Cahill is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

37. Had Plaintiff Cahill been aware that Defendant's computer systems were not secure, he would not have trusted Defendant with his PII and PHI.

Plaintiff Sheila Edwards

38. Plaintiff Edwards is, and at all times mentioned herein was, an individual citizen of the State of Georgia, residing in Ringgold, Georgia. Plaintiff Edwards is a current/former patient of Defendant.

39. Plaintiff Edwards received a Notice of Data Breach Letter from Chattanooga Heart Institute dated July 28, 2023. It states that the breached files included her "name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information."

40. Plaintiff Edwards is especially alarmed and anxious that her Social Security number and extremely private health information (PHI) was identified as among the breached data on Defendant's computer system.

41. Since the Data Breach, and in addition to the injuries alleged above, Plaintiff Edwards also experienced actual identity theft and fraud by virtue of her Private Information being stolen.

42. Plaintiff Edwards has spent approximately five (5) hours responding to these incidents of identity theft and fraud, monitoring financial accounts, changing passwords, or

otherwise as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Edwards otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Edwards lost was spent at Defendant's recommendations.

43. Plaintiff Edwards is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

44. Had Plaintiff Edwards been aware that Defendant's computer systems were not secure, she would not have trusted Defendant with her PII and PHI.

Plaintiff Sidney Jackson

45. Plaintiff Sidney Jackson is, and at all times mentioned herein was, a citizen of the State of Tennessee residing in the city of Chattanooga, Tennessee. Plaintiff is a current/former patient of Defendant.

46. Plaintiff Jackson received a Notice of Data Breach Letter from Chattanooga Heart Institute dated July 28, 2023. It states that the breached files included her "name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information."

47. Plaintiff Jackson is especially alarmed and anxious that her Social Security number and extremely private health information (PHI) was identified as among the breached data on Chattanooga Heart Institute's computer system.

48. Since the Data Breach, and in addition to the injuries alleged above, Plaintiff Jackson also experienced actual identity theft and fraud, including a $14 fraudulent charge on her credit card. As a result, Plaintiff had to order a new credit card.

49. Plaintiff Jackson has spent approximately five (5) hours responding to these incidents of identity theft and fraud, monitoring financial accounts, changing passwords, and obtaining a new credit card as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Jackson otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Jackson lost was spent at Defendant's recommendations.

50. Plaintiff Jackson is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

51. Had Plaintiff Jackson been aware that Defendant's computer systems were not secure, she would not have trusted Defendant with her PII and PHI.

Plaintiff Christopher Cordes

52. Plaintiff Christopher Cordes is, and at all times material herein was, an individual citizen of the State of Tennessee and the Captain of the City of Chattanooga Fire Department. Plaintiff Cordes is a former patient of Chattanooga Heart Institute. He went to the Chattanooga Heart Institute in late 2022 for testing of his heart related to his pilot's license.

53. Plaintiff Cordes received a Notice of Data Breach Letter from Chattanooga Heart Institute dated July 28, 2023. It states that the breached files included his "name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information."

54. Plaintiff is very careful with his Private Information. He is not aware of any data breaches other than this one that exposed his Social Security number and PHI and is concerned that it and other private information has now been exposed to bad actors. As a result of the Data

Breach, he has taken multiple steps to avoid identity theft, including signing up for credit monitoring services, setting up notices and reports and carefully reviewing all his accounts.

55. Plaintiff Cordes has spent approximately eight (8) hours to date obtaining and reviewing the results of the credit monitoring service he enrolled in and additional monitoring of health and financial accounts as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Cordes otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Cordes lost was spent at Defendant's recommendations.

56. Plaintiff Cordes is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

57. Had Plaintiff Cordes been aware that Defendant's computer systems were not secure, he would not have trusted Defendant with his PII and PHI.

Plaintiff Giselle Reed Allen

58. Plaintiff Giselle Reed Allen is, and at all times material herein was, an individual citizen of the State of Georgia, who resides in Ringgold, Georgia.

59. Plaintiff Allen received a Notice of Data Breach Letter from Defendant dated July 28, 2023. It states that the breached files included her "name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information."

60. Plaintiff Allen is especially alarmed and anxious that her Social Security number and extremely private health information (PHI) was identified as among the breached data on Defendant's computer system.

61. Plaintiff Allen has spent several hours researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Allen otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Allen lost was spent at Defendant's recommendations.

62. Plaintiff Allen is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

63. Had Plaintiff Allen been aware that Defendant's computer systems were not secure, she would not have trusted Defendant with her PII and PHI.

Plaintiff Jeff Bryden

64. Plaintiff Jeff Bryden is, and at all times mentioned herein was, an individual citizen of the State of Tennessee, residing in the city of Soddy Daisy, and is a patient of Chattanooga Heart Institute.

65. Plaintiff Bryden received a Notice of Data Breach Letter from Chattanooga Heart Institute dated July 28, 2023. It states that the breached files included his "name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information."

66. Plaintiff Bryden is especially alarmed and anxious that his Social Security number and extremely private PHI was identified as among the breached data on Defendant's computer system.

67. Plaintiff Bryden has spent approximately five (5) hours monitoring financial and other accounts, changing passwords, or otherwise as a result of the Data Breach. The time spent dealing with the Data Breach is time Plaintiff Bryden otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Bryden lost was spent at Defendant's recommendations.

68. Plaintiff Bryden is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years thereafter.

69. Had Plaintiff Bryden been aware that Defendant's computer systems were not secure, he would not have trusted Defendant with his PII and PHI.

Plaintiff Elyn Painter

70. Plaintiff Elyn Painter is, and at all times mentioned herein was, an individual citizen of the State of Tennessee, residing in the city of Cleveland, and is a patient of Chattanooga Heart Institute.

71. Plaintiff Painter received a Notice of Data Breach Letter from Chattanooga Heart Institute dated July 28, 2023. It states that the breached files included her "name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information."

72. Plaintiff Painter is especially alarmed and anxious that her Social Security number and extremely private health information (PHI) was identified as among the breached data on Defendant's computer system.

73. Since the Data Breach, Plaintiff Painter has been receiving calls from strangers acting like they are from Medicaid or the Social Security Office, asking her to provide additional

personal information or press a number to continue. In addition, she has received texts about a fraudulent computer purchase made in her name and about a booking.com reservation that she did not make. She reasonably thinks these annoying and time-consuming communications are related to Defendant's Data Breach.

74. Since the Data Breach, and in addition to the injuries alleged above, Plaintiff Painter also experienced actual identity theft and fraud by virtue of her Private Information being stolen.

75. Since receiving the Data Breach notice in July 2023, Plaintiff Painter has spent approximately two to three hours each week responding to above incidents of identity theft and fraud, monitoring her financial accounts, and requesting a new debit card. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Painter otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Painter lost was spent at Defendant's recommendations.

76. Plaintiff Painter is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

77. Had Plaintiff Painter been aware that Defendant's Institute's computer systems were not secure, she would not have trusted Defendant with her PII and PHI.

Defendant Memorial Health Institute, LLC d/b/a The Chattanooga Heart Institute

78. Defendant Memorial Health Institute, LLC d/b/a The Chattanooga Heart Institute, is a Tennessee limited liability company that has its principal place of business at 2501 Citico Ave., Chattanooga, Tennessee 37404.

JURISDICTION AND VENUE

79. The Eastern District of Tennessee has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District

and Defendant conducts substantial business in Tennessee and this District through its headquarters, offices, parents, and affiliates.

80. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one member of the class, including Plaintiffs Allen and Edwards, are citizens of a state different from Defendant.

81. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

82. Defendant is a healthcare provider group that provides a wide range of cardiac health care services. Defendant offers comprehensive cardiac care and has three (3) vascular surgeons and 27 board certified cardiologists on staff and operates six offices in the Chattanooga, Tennessee area, including a single Georgia location.[8]

83. Defendant represents to its patients that, "[b]y choosing The Chattanooga Heart Institute, you're choosing among the leading cardiologists and surgeons in the Southeast in an environment dedicated to exceptional care and patient outcomes."[9]

84. As part of its medical and business operations, Defendant collects, maintains, and stores the highly sensitive PII and medical information provided by its current and former patients, including but not limited to: name, mailing address, email address, phone number, date of birth,

[8] *About Us*, The Chattanooga Heart Inst., https://www.chattanoogaheart.com/about-us/ (last visited Nov. 2, 2023).
[9] *Id.*

driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic, or financial information.

85. Defendant also creates and stores medical records and other protected health information for its patients, records of treatments and diagnoses.

86. Upon information and belief, Defendant's HIPAA Notice of Privacy Practices ("Privacy Policy") is provided to every patient both prior to receiving treatment and upon request.[10] Defendant's Privacy Notice makes clear that it understands that its patients' Private Information is personal and must be protected by law.

87. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

88. Plaintiffs and Class Members, as current and former patients of Defendant, entrusted their Private Information to Defendant with the reasonable expectation that Defendant would comply with its obligation to keep their sensitive and personal information confidential and secure from illegal and unauthorized access, and that Defendant would provide them with prompt and accurate notice of any unauthorized access to their Private Information.

89. Unfortunately for Plaintiffs and Class Members, Defendant failed to carry out their duty to safeguard sensitive Private Information and provide adequate data security, thus failing to

[10] *Notice of Privacy Practices*, The Chattanooga Heart Inst. (Oct. 2020), https://www.chattanoogaheart.com/wp-content/uploads/2022/06/Privacy-Notice_CHI_17X26-9-02-2020-handout.docx (last visited July 31, 2023).

protect Plaintiffs and Class Members from the exfiltration of their Private Information during the Data Breach.

THE CYBERATTACK AND RESULTING DATA BREACH

90. On or about April 17, 2023, Defendant became aware of irregularities in its IT network consistent with a cybersecurity event.[11]

91. On or about May 31, 2023, Defendant "discovered" the Data Breach, originally reporting that the cyberthieves had accessed 170,450 Class Members' Private Information.[12]

92. Defendant failed to notify these individuals identified as affected by the Data Breach until July 28, 2023.[13]

93. More than two months later, Defendant disclosed that in fact over 411,000 persons were affected by the Data Breach.[14]

94. The vast majority of Class Members were not notified the Data Breach occurred until October 6, 2023—seven months following the unauthorized access and exfiltration, six months after the Data Breach was first detected by Defendant, and over four months after the nature of the Data Breach was confirmed.

95. Plaintiffs and Class Members have never been fully informed about the scope of the intrusion, the vulnerabilities exploited, the remediation required, or the vulnerability of their data remaining in Defendant's possession.

96. Through the cyberattack, Plaintiffs' and Class Members' Private Information, including Social Security numbers, was accessed by criminal third parties.

---

[11] *Chattanooga Heart Notice of Data Security Incident*, *supra* note 2.
[12] *Chattanooga Heart Institute Data Breach Notification*, *supra* note 1.
[13] *Id.*
[14] *Id.*

97. Based on its investigation, Defendant admits that Plaintiffs' and Class Members' Private Information was accessed and exfiltrated via a cyberattack conducted by cybercriminals.

98. Since Defendant's discovery of the attack, Karakurt, a financially motivated cybercrime group that steals data before demanding payment from victims by threatening its publication, publicly claimed responsibility for the attack. [15] This criminal group relies exclusively on data theft to extort victims but does not deploy ransomware to encrypt files and systems. Instead, the group exploits vulnerabilities or weak credentials of the computer network. Once inside the network, it uses off-the-shelf tools and applications, often native to the victim system, to meet its objectives.

99. On information and belief, the Private Information accessed by hackers was not encrypted.

100. The Data Breach also highlights the inadequacies inherent in Defendant's network monitoring procedures. If Defendant had properly monitored its cyber security systems, it would have prevented the Data Breach, discovered the Data Breach sooner, and/or have prevented the hackers from accessing Plaintiffs' and Class Members' Private Information.

101. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of Plaintiffs and the Class Members.

102. Due to Defendant's inadequate security measures, Plaintiffs and the Class Members now face a substantial, present, imminent, and ongoing risk of fraud and identity theft and must deal with that threat forever.

---

[15] *The Chattanooga Heart Institute to notify 170,450 about March "data security incident"* (July 29, 2023), https://www.databreaches.net/the-chattanooga-heart-institute-to-notify-170450-about-march-data-security-incident/ (last accessed Nov. 1, 2023).

103. Due to Defendant's inadequate security measures, Plaintiffs' and Class Members' Private Information is now in the hands of cyberthieves.

104. Defendant failed to comply with its obligations to keep such information confidential and secure from unauthorized access, as well as its obligation to timely notify Plaintiffs and Class Members.

THE DATA BREACH WAS FORESEEABLE

105. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting corporations, preceding the date of the breach.

106. Data breaches, including those perpetuated against service providers that store personal information in their systems, have become widespread.

107. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.

108. Cyberattacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

109. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March

[16] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection.

2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

110. Therefore, the increase in such attacks, and the attendant risk of future attacks in light of the nature of Defendant's business, was surely known to Defendant. Anyone in Defendant's industry knew or should have known of the risks of a cyberattack and taken sufficient steps to fulfill its obligation to the people who entrust their personal data to the business. Defendant failed to do so.

111. In 2022, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury (Treasury), and the Financial Crimes Enforcement Network (FinCEN) released a joint Cybersecurity Advisory (CSA) to provide business like Defendant's information on the Karakurt data extortion group.[17]

112. Although Karakurt's primary extortion leverage is a promise to delete stolen data and keep the incident confidential, some victims reported Karakurt actors did not maintain the confidentiality of victim information after a ransom was paid. The U.S. government strongly discourages the payment of any ransom to Karakurt threat actors, or any cyber criminals promising to delete stolen files in exchange for payments.[18]

[17] *Cybersecurity Advisory: Karakurt Data Extortion Group*, Cybersecurity & Infrastructure Sec. Agency (June 2, 2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a.
[18] *Id.*

DEFENDANT FAILED TO PROPERLY PROTECT PLAINTIFFS' AND CLASS MEMBERS' PRIVATE INFORMATION

113. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted Private Information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for more than 411,000 individuals.

114. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

115. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[19] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[20]

116. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

[19] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[20] *Id.*

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

117. Defendant failed to properly implement basic data security practices explained and set forth by the FTC.

118. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

119. A data breach, such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI that is not permitted under HIPAA.

120. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. § 164.40.

121. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *See* the definition of security incident at 45 C.F.R. § 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R. § 164.308(a)(6).[21]

[21] *FACT SHEET: Ransomware and HIPPA* at 4, U.S. Dep't of Health & Human Servs. (July 11, 2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

122. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrates Defendant failed to comply with safeguards mandated by HIPAA.

DEFENDANT FAILED TO COMPLY WITH INDUSTRY STANDARDS

123. Defendant did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for more than 411,000 individuals.

124. As explained by the FBI, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."[22]

125. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

[22] *See How to Protect Your Networks from RANSOMWARE* at 3, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Nov. 2, 2023).

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[23]

126. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to

[23] *Id.* at 3–4.

the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)…

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[24]

127. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

[24] *See* Security Tip (ST19-001), *Protecting Against Ransomware* (Apr. 11, 2019) (rev. Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Nov. 2, 2023).

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[25]

128. As described above, experts studying cybersecurity routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the Private Information they collect and maintain.

129. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendant, including, but not limited to, the following:

[25] *See Human-Operated Ransomware Attacks: A Preventable Disaster* (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

130. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

131. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

132. Given that Defendant was storing the Private Information of more than 411,000 individuals, Defendant could and should have implemented all of the above measures to prevent cyberattacks.

133. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of approximately 411,000 individuals' Private Information.

DEFENDANT'S BREACH OF ITS OBLIGATIONS TO THE CLASS

134. Defendant breached its obligations to Plaintiffs and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyberattacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing or prior intrusions;

d. Failing to test and assess the adequacy of its data security system;

e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304 definition of encryption);

p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

q. Failing to adhere to industry standards for cybersecurity.

135. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

136. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, increased, and immediate risk of fraud and identity theft.

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT INDIVIDUALS AT AN INCREASED RISK OF FRAUD AND IDENTITY THEFT

137. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

138. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to

[26] *See* U.S. Gov't Accountability Off., GAO-07-737, *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/new.items/d07737.pdf.

monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Here, the cyberthieves already have Social Security numbers.

139. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[27]

140. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

[27] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited May 26, 2023).

141. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

142. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

143. Thus, even if certain information (such as insurance information) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

144. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

145. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[28]

[28] *See Data Breach Checklist*, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last visited Oct. 26, 2023).

146. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[29]

148. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

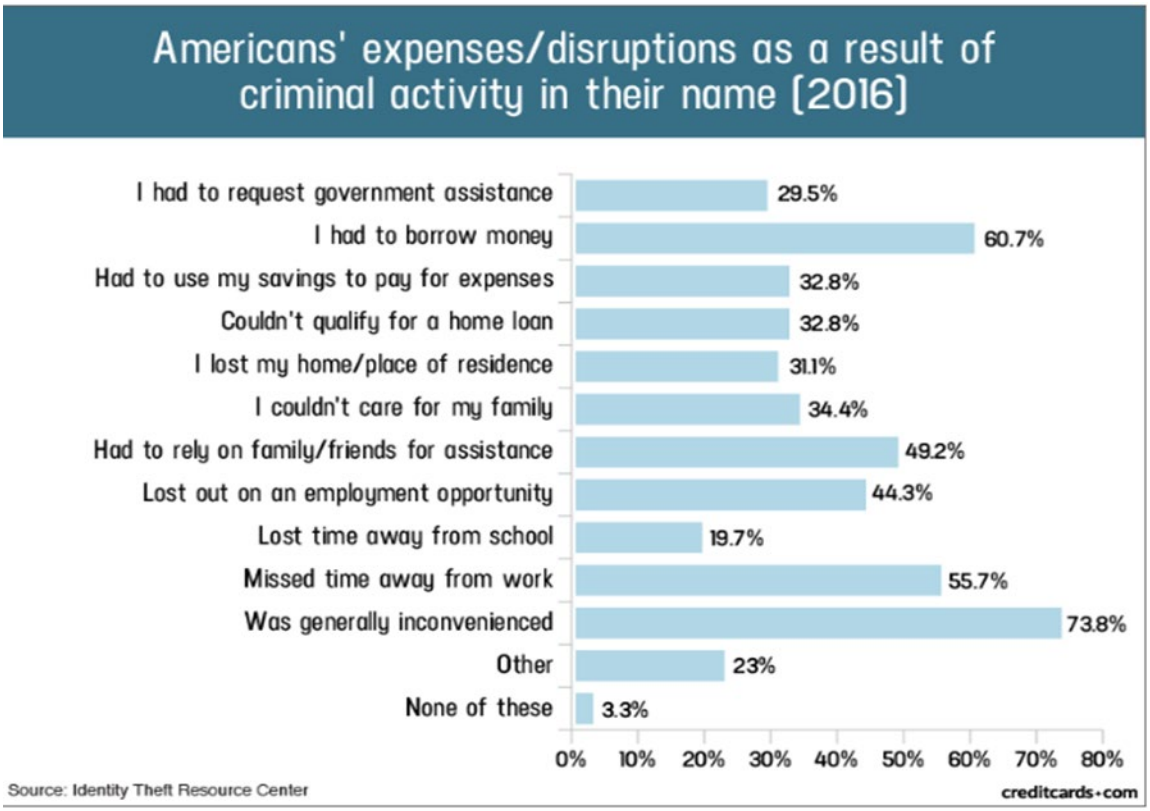
149. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

[29] *Identity Theft and Your Social Security Number*, Soc. Sec. Admin. (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

150. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

151. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



152. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card

[30] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[31]

153. Moreover, theft of Private Information is also gravely serious. The asset that is one's Private Information contains extremely valuable property rights.[32]

154. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

155. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

156. According to the U.S. Government Accountability Office, 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.

See GAO Report, at p. 29.

---

[31] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, COMPUTER WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[32] *See*, *e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11 at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

157. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

158. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

159. Thus, Plaintiffs and Class Members must vigilantly monitor their financial information for many years to come.

160. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[33] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams; once stolen, fraudulent use of that information and damage to victims may continue for years.

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

PLAINTIFFS' AND CLASS MEMBERS' HARMS AND DAMAGES

162. To date, Defendant has done little to adequately protect Plaintiffs and Class Members, or to compensate them for their injuries sustained in this data breach. Defendant's data breach notice letter completely downplays and disavows the theft of Plaintiffs' and Class Members' Private Information, when the facts demonstrate that the Private Information was accessed and exfiltrated. The complimentary fraud and identity monitoring service offered by Defendant is wholly inadequate as the services are only offered for 12 months and it places the

[33] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

163. Plaintiffs and Class Members have been injured and damaged by the compromise of their Private Information in the Data Breach.

164. Plaintiffs' Private Information (including without limitation names and Social Security numbers) was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's network. Class Members' Private Information, as described above, was similarly compromised and is now in the hands of the same cyberthieves.

165. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

166. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

167. Plaintiffs and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

168. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

169. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[34] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[35] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[36]

170. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

171. Plaintiffs and Class Members spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiffs and Class Members about the significant time that they will need to spend monitoring their own accounts and statements received.

172. Plaintiffs spent many hours over the course of several days attempting to verify the veracity of the notice of breach and to monitor financial and online accounts for evidence of fraudulent activities.

173. Plaintiffs and Class Members suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the

[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[35] https://datacoup.com/.
[36] https://digi.me/what-is-digime/.

value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security Number, bank accounts, and credit reports for unauthorized activity for years to come.

174. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, the breach occurred in March 2023, Defendant knew of it since April 17, 2023, and yet Defendant did not begin to notify the victims until July 28, 2023, and did not conclude notifying the Class Members until October 2023.

175. Defendant offered no explanation or purpose for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiffs and Class Members.

176. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential

personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

177. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

178. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members suffered a loss of privacy and are at a present, imminent, and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

179. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

180. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Defendant provided Notice of the Data Breach beginning on or around July 28, 2023 (the "Nationwide Class").**

181. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

182. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of individuals whose Private Information may have been improperly accessed in the

Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised the Maine Attorney General that the Data Breach affected more than 411,000 individuals.

183. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, *e.g.*, FTC Guidelines, HIPAA, etc.;

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

e. Whether Defendant owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Plaintiffs and Class Members to safeguard their Private Information;

g. Whether cybercriminals obtained Plaintiffs' and Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant owed a duty to provide Plaintiffs and Class Members timely notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant breached any contractual duties to provide adequate security for the Private Information entrusted to it, duties that were either explicit or implied by the imposition of the membership fee.

n. Whether Defendant was unjustly enriched;

o. Whether Defendant's conduct violated federal law;

p. Whether Defendant's conduct violated state law;

q. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or punitive damages.

184. Common sources of evidence may also be used to demonstrate Defendant's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Defendant's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

185. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach and due to Defendant's misfeasance.

186. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

187. Predominance, Fed. R. Civ. P. 23 (b)(3). Defendant engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

188. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

189. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Members with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that

experienced by the Class and will establish the right of each Class Members to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

190. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

191. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

192. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

193. Further, Defendant acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

194. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

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

d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

e. Whether Defendant breached any contractual duty, either explicit or implied, to provide adequate data security as part of the membership fee;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and,

h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

195. Defendant acted on grounds that apply generally to the Class as a whole, so that Class certification and the corresponding relief sought are appropriate on a Class-wide basis.

196. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

197. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

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

199. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for purposes that would benefit Plaintiffs and the Class and/or not disclose their Private Information to unauthorized third parties.

200. Defendant had full knowledge of the sensitive nature of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information was wrongfully disclosed.

201. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and the Class in Defendant's possession was adequately secured and protected.

202. Defendant had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' Private Information within their possession was compromised and precisely the type(s) of information that were compromised.

203. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

204. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPAA and/or Section 5 of the FTC Act, and other requirements discussed herein, and to

ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

205. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

206. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

207. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

208. Defendant systematically failed to provide adequate security for data in its possession.

209. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

210. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiffs' and Class Members' Private Information;

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

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

d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

211. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendant's possession.

212. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' Private Information.

213. Defendant, through its actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiffs and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

214. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs and Class Members' Private Information would result in injury to Plaintiffs and Class Members.

215. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would result in injuries to Plaintiffs and Class Members.

216. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

217. As a result of Defendant's ongoing failure to notify Plaintiffs and Class Members regarding what type of Private Information has been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

218. Defendant's breaches of duties caused Plaintiffs and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

219. As a result of Defendant's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

220. Plaintiffs seek the award of actual damages on behalf of the Class. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

221. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

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

223. Pursuant to Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

224. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

225. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. 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.

226. The harm that occurred as a result of the Data Breach is the type of harm that the Federal Trade Commission Act was intended to guard against.

227. Defendant breached their duties to Plaintiffs and Class Members under the Federal Trade Commission Act, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

228. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

229. In addition to the duties under the Federal Trade Commission Act, HIPAA also obligates Covered Entities and Business Associates to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" and "must reasonably safeguard protected health information." 45 CFR § 164.530(c).

230. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR §§ 164.400, *et seq.*

231. The Georgia Fair Business Practices Act ("GFBPA"), Ga. Code Ann. §§ 10-1-390, *et seq.*, and the Tennessee Consumer Protection Act ("TCPA"), Tenn. Code Ann. §§ 47-18-104, *et seq.*, prohibit unfair or deceptive acts or practices in the conduct of any trade or commerce.

232. Defendant violated HIPAA, GFBPA, TCPA, and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards, and by unduly delaying reasonable notice of the actual breach.

Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a Data Breach, and the exposure of Plaintiffs' and Class Members' sensitive PII.

233. Plaintiffs are within the class of person that these statutes were intended to protect and the harm resulting from the Data Breach is the type of injury against which these statutes were intended to guard.

234. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, as established by statute, rule and regulation, Plaintiffs and Class Members would not have been injured.

235. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure and compromise of their Private Information.

236. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, and consequential in an amount to be proven at trial.

THIRD COUNT
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

237. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

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

239. Defendant, as a condition of providing its services, required Plaintiffs' and Class Members to provide and entrust their Private Information.

240. By Plaintiffs and Class Members providing their Private Information, and by Defendant accepting this Private Information, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant would adequately safeguard Plaintiffs' and Class Members' Private Information from foreseeable threats, (2) that Defendant would delete the information of Plaintiffs and Class Members once it no longer had a legitimate need; and (3) that Defendant would provide Plaintiffs and Class Members with notice within a reasonable amount of time after suffering a data breach.

241. Defendant provided consideration by providing it services, while Plaintiffs and Class Members provided consideration by providing valuable property—i.e., their Private Information and payment to Defendant. Defendant benefitted from the receipt of this Private Information by increased income through providing medical services.

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

243. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information, or providing timely and accurate notice to them that their Private Information was compromised due to the Data Breach.

244. Defendant's breaches of contract have caused Plaintiffs and Class Members to suffer damages from the lost benefit of their bargain, out-of-pocket monetary losses and expenses, loss of time, and diminution of the value of their Private Information.

245. As a direct and proximate result of Defendant' above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent,

and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

FOURTH COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

246. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

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

248. This Count is pleaded in the alternative to the breach of contract claims above.

249. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information in exchange for medical treatment.

250. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

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

252. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

253. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

254. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide it to Defendant.

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

256. Plaintiffs and Class Members have no adequate remedy at law.

257. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

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

FIFTH COUNT
Bailment
(On Behalf of Plaintiffs and the Nationwide Class)

259. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

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

261. Plaintiffs and Class Members' Private Information was provided to Defendant.

262. In delivering their Private Information, Plaintiffs and Class Members intended and understood that their Private Information would be adequately safeguarded and protected.

263. Defendant accepted Plaintiffs and Class Members' Private Information.

264. By accepting possession of Plaintiffs and Class Members' Private Information, Defendant understood that Plaintiffs and Class Members expected their Private Information to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

265. During the bailment (or deposit), Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence, and prudence in protecting their Private Information.

266. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' Private Information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class Members' Private Information.

267. Defendant further breached its duty to safeguard Plaintiffs' and Class Members' Private Information by failing to timely notify them that their Private Information had been compromised as a result of the Data Breach.

268. Defendant failed to return, purge, or delete the Private Information belonging to Plaintiffs and Class Members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

269. As a direct and proximate result of Defendant's breach of its duties, Plaintiffs and the Class suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.

270. As a direct and proximate result of Defendant's breach of its duty, Plaintiffs' and Class Members Private Information that was entrusted to Defendant during the bailment (or deposit) was damaged and its value diminished.

SIXTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class)

271. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

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

273. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private

Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

274. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its current and former patients and employees to keep secure their Private Information. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give detailed notice of the Data Breach to Plaintiffs and Class in a reasonable and practicable period of time.

275. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

276. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

277. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

278. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching

how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

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

SEVENTH COUNT
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

280. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

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

282. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

283. As a result of Defendant's conduct, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII and PHI.

284. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

285. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

286. As a direct and proximate result of Defendant's public disclosure of private facts, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

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

288. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

EIGHTH COUNT
Declaratory and Injunctive Relief
(On Behalf of Plaintiffs and the Nationwide Class)

289. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

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

291. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

292. Defendant owed a duty of care to Plaintiffs and Class Members that require it to adequately secure Plaintiffs' and Class Members' Private Information.

293. Defendant failed to fulfill their duty of care to safeguard Plaintiffs' and Class Members' Private Information.

294. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant' contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendant' failure to address the security failings that led to such exposure.

295. There is no reason to believe that Defendant' employee training and security measures are any more adequate now than they were before the breach to meet Defendant' contractual obligations and legal duties.

296. Plaintiffs, therefore, seeks a declaration (1) that Defendant' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and duties of care,

Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

c. Ordering that Defendant audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for their provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, Plaintiffs and Class Members' Personally Identifiable Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiffs and Plaintiffs' counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

Dated: November 2, 2023

Respectfully submitted,

/s/ Lisa A. White

Lisa A. White (TN BPR # 026658)
Gary E. Mason (admitted *pro hac vice*)
Danielle L. Perry (admitted *pro hac vice*)
MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
lwhite@masonllp.com
gmason@masonllp.com
dperry@masonllp.com

Counsel for Plaintiffs Stephen Cahill, Elyn Painter, and Putative Class Members

R. Luke Widener (TN BPR #033623)
Alexandra M. Honeycutt (TN BPR #039617)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Tel: (865) 247-0080
Fax: (865) 522-0049
lwidener@milberg.com
ahoneycutt@milberg.com

Bryan L. Bleichner (admitted *pro hac vice*)
Philip J. Krzeski (admitted *pro hac vice*)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Tel: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

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

Counsel for Plaintiff Sheila Edwards and Putative Class Members

R. Luke Widener (TN BPR #033623)
Alexandra M. Honeycutt (TN BPR #039617)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Tel: (865) 247-0080
Fax: (865) 522-0049
lwidener@milberg.com
ahoneycutt@milberg.com

Joseph M. Lyon (admitted *pro hac vice*)
Kevin M. Cox (admitted *pro hac vice*)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Tel: (513) 381-2333
jlyon@thelyonfirm.com
kcox@thelyonfirm.com

Counsel for Plaintiff Sidney Jackson and Putative Class Members

J. Gerard Stranch, IV (TN BPR #23045)
Andrew E. Mize (admitted *pro hac vice*)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
T: (615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

Daniel O. Herrera (*pro hac vice* forthcoming)
Nickolas J. Hagman (admitted *pro hac vice*)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, IL 60603
Tel: (312) 782-4880
Fax: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Counsel for Plaintiff Giselle Reed Allen and Putative Class Members

Kenneth J. Grunfeld*
KOPELOWITZ OSTROW P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
T: (954) 525-4100
grunfeld@kolawyers.com

Counsel for Plaintiff Christopher Cordes and Putative Class Members

David C. Riley (TN BPR #21663)
Edwin E. Wallis III (TN BPR #23950)
GLASSMAN, WYATT, TUTTLE & COX, P.C.
26 North Second Street
Memphis, TN 38103
Tel: (901) 527-4673
Fax: (901) 521-0940
ewallis@gwtclaw.com
driley@gwtclaw.com

Mason A. Barney (*pro hac vice* forthcoming)
Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Counsel for Plaintiff Jeff Bryden and Putative Class Members

EXHIBIT A

The Chattanooga Heart Institute

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>

July 28, 2023

Dear <<Name 1>>:

The Chattanooga Heart Institute takes the protection and proper use of your Protected Health Information ("PHI") very seriously. With that in mind, we are writing to tell you about a data security incident involving some of your PHI. We are writing to you to explain the incident, our response to it, and steps you can take to protect your personal information, should you feel it appropriate to do so.

What happened?
On April 17, 2023, The Chattanooga Heart Institute identified indications of a cybersecurity attack on its IT network. The Chattanooga Heart Institute immediately took steps to secure its network and began an investigation with the assistance of an external forensics vendor. The investigation determined that an unauthorized third party gained access to The Chattanooga Heart Institute's network between March 8, 2023, and March 16, 2023. On May 31, 2023, The Chattanooga Heart Institute learned that the unauthorized third party obtained copies of some of the data from its systems containing confidential patient information, however, the unauthorized third party did not retrieve data directly from The Chattanooga Heart Institute's Electronic Medical Record ("EMR").

What information was involved?
The Chattanooga Heart Institute's investigation shows that you may have been either a patient or guarantor of The Chattanooga Heart Institute. You are being notified because some of your information was identified as potentially having been accessed or acquired by the unauthorized third party. The information in the files may have included your name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information.

What we are doing.
Upon discovering the unauthorized third party access, The Chattanooga Heart Institute took quick action to protect its systems, contain the incident, begin an investigation, and maintain continuity of care. In addition, The Chattanooga Heart Institute notified federal law enforcement. Once secured, systems were returned to the network with additional security and monitoring tools. To help relieve concerns and restore confidence following this incident, The Chattanooga Heart Institute has secured the services of Equifax to provide identity monitoring at no cost to you for <<one year/two years>>. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Enrollment Instructions.

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **<<Activation Code>>** to activate and take advantage of your identity monitoring services. You have until **<<Enrollment Deadline>>** to activate your identity monitoring services.

For more information about Equifax and your Identity Monitoring services, you can visit www.equifax.com. Additional information describing services available at no cost to you is included with this letter.

Actions you may wish to take.

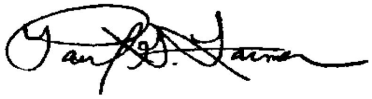
It is always prudent for patients to review health care statements for accuracy and report to your provider or insurance carrier any services or charges that were not incurred. Additionally, please review the enclosed "Additional Resources" section of this letter. That section describes further steps you can take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file, if you desire to do so.

For more information.

If you need more information about this IT security event, we have established a call center with a trusted third-party partner that can answer specific questions about this event. To contact this call center, please call 1-833-627-2719, Monday through Friday from 9:00 a.m. to 9:00 p.m. eastern time, excluding U.S. holidays.

We apologize for any concern this may cause. Protecting your information is important to us. We trust that this notification and additional resource information demonstrates our continued commitment to you.

Sincerely,



Paul G. Farmer, President
The Chattanooga Heart

Additional Resources

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1- 410-576-6300 or 1-888-743-0023; and www.marylandattorneygeneral.gov/. Imagine360 is located at 1550 Liberty Ridge Dr. Suite 330 Wayne, PA 19087.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov!f!201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

EXHIBIT B

The Chattanooga Heart Institute

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>

October 6, 2023

Dear <<Name 1>>:

The Chattanooga Heart Institute takes the protection and proper use of your Protected Health Information ("PHI") very seriously. With that in mind, we are writing to tell you about a data security incident involving some of your PHI. We are writing to you to explain the incident, our response to it, and steps you can take to protect your personal information, should you feel it appropriate to do so.

What happened?
On April 17, 2023, The Chattanooga Heart Institute identified indications of a cybersecurity attack on its IT network. The Chattanooga Heart Institute immediately took steps to secure its network and began an investigation with the assistance of an external forensics vendor. The investigation determined that an unauthorized third party gained access to The Chattanooga Heart Institute's network between March 8, 2023, and March 16, 2023. On May 31, 2023, The Chattanooga Heart Institute learned that the unauthorized third party obtained copies of some of the data from its systems containing confidential patient information, however, the unauthorized third party did not retrieve data directly from The Chattanooga Heart Institute's Electronic Medical Record ("EMR").

What information was involved?
The Chattanooga Heart Institute's investigation shows that you may have been either a patient or guarantor of The Chattanooga Heart Institute. You are being notified because some of your information was identified as potentially having been accessed or acquired by the unauthorized third party. The information in the files may have included your name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information.

What we are doing.
Upon discovering the unauthorized third party access, The Chattanooga Heart Institute took quick action to protect its systems, contain the incident, begin an investigation, and maintain continuity of care. In addition, The

Chattanooga Heart Institute notified federal law enforcement. Once secured, systems were returned to the network with additional security and monitoring tools. To help relieve concerns and restore confidence following this incident, The Chattanooga Heart Institute has secured the services of Equifax to provide identity monitoring at no cost to you for <<one year/two years>>. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Enrollment Instructions.

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **<<Activation Code>>** to activate and take advantage of your identity monitoring services. You have until **<<Enrollment Deadline>>** to activate your identity monitoring services.

For more information about Equifax and your Identity Monitoring services, you can visit www.equifax.com. Additional information describing services available at no cost to you is included with this letter.

Actions you may wish to take.

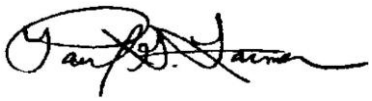
It is always prudent for patients to review health care statements for accuracy and report to your provider or insurance carrier any services or charges that were not incurred. Additionally, please review the enclosed "Additional Resources" section of this letter. That section describes further steps you can take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file, if you desire to do so.

For more information.

If you need more information about this IT security event, we have established a call center with a trusted third-party partner that can answer specific questions about this event. To contact this call center, please call 1-833-627-2719, Monday through Friday from 9:00 a.m. to 9:00 p.m. eastern time, excluding U.S. holidays.

We apologize for any concern this may cause. Protecting your information is important to us. We trust that this notification and additional resource information demonstrates our continued commitment to you.

Sincerely,



Paul G. Farmer, President
The Chattanooga Heart

Additional Resources

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1- 410-576-6300 or 1-888-743-0023; and www.marylandattorneygeneral.gov/. Imagine360 is located at 1550 Liberty Ridge Dr. Suite 330 Wayne, PA 19087.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov!f!201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.