

**UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA**

<p>Jacob Whitehead, on behalf of minor child M.W., <i>and on behalf of M.W. and all others similarly situated,</i></p> <p style="text-align: center;">Plaintiff,</p> <p>v.</p> <p>Keystone Health,</p> <p style="text-align: center;">Defendant.</p>	<p>CASE NO. _____</p> <p>CLASS ACTION COMPLAINT</p> <p>JURY TRIAL DEMANDED</p>
--	---

Plaintiff M.W. (“Plaintiff”) brings this Class Action Complaint against Keystone Health (“Defendant”), individually and on behalf of all others similarly situated (“Class Members”), and alleges, upon personal knowledge as to her own actions and her counsel’s investigations, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including, but not limited to, Plaintiff’s and Class Members’ names, Social Security numbers, and clinical information (collectively, “Private Information” or “PII and PHI”).

2. Defendant is a health network based in central Pennsylvania that has “more than 540 employees and sees over 59,000 patients annually.”¹

3. Defendant collects its patients’ Private Information as a condition of receiving treatment at Defendant’s hospitals and medical centers.

¹ <https://keystonehealth.org/about-us/> (last accessed: October 24, 2022).

4. On or around August 19, 2022, Defendant detected that it was the target of a cybersecurity attack (the “Data Breach”).

5. Defendant immediately launched an investigation into the Data Breach and confirmed that an unauthorized actor accessed Defendant’s systems between July 28, 2022 and August 19, 2022 and copied and exfiltrated certain files containing Plaintiff’s and Class Members’ Private Information, including, but not limited to, the following: names, Social Security numbers, and clinical information.²

6. Defendant did not send notice of the Data Breach (the “Notice of Data Breach Letter”) until on or around October 14, 2022.

7. Defendant’s website states the following:

On August 19, 2022, we identified an incident that temporarily disrupted our computer systems. We reported the incident to law enforcement and worked with a third-party cybersecurity firm to determine what happened. Our investigations found that an unauthorized party accessed files within [Defendant’s] system between July 28, 2022 and August 19, 2022. Some of those files contained patient information, including names, Social Security numbers, and clinical information.³

8. Plaintiff’s Notice of Data Breach states the following:

What happened? On August 19, 2022, [Defendant] identified an incident that shut down some of [Defendant’s] computer systems for a short period of time. [Defendant] took measures to contain the incident, reported it to law enforcement, and did an investigation with the help of a third-party cybersecurity firm. [Defendant’s] investigation found that an unauthorized party accessed [Defendant’s] systems and took some files from [Defendant’s] network between July 28, 2022 and August 19, 2022.

What Information Was Involved? The files contained your child’s name, Social Security number, and records regarding your child’s care with Keystone Health.

² https://methodistmckinneyhospital.com/wp-content/uploads/2022/08/Revised-Preliminary-Website-Notice_8.3.22.pdf (last accessed: October 12, 2022).

³ https://keystonehealth.org/wp-content/notice_pdf/notice_of_security_incident.pdf (last accessed: October 24, 2022).

9. Defendant, in its Notice of Data Breach, admits that Plaintiff's and Class Members' Private Information was unlawfully accessed and exfiltrated.

10. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal and Medical Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

11. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Personal and Medical Information was a known risk to the Defendant and thus the Defendant was on notice that failing to take steps necessary to secure the Personal and Medical Information from those risks left that information in a dangerous condition.

12. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

13. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted Private Information impacted during the Data Breach.

14. The exposed Private Information of Plaintiff and Class Members can—and likely will—be sold on the dark web. Indeed, Plaintiff’s and Class Members’ Private Information has already been published on the dark web.

15. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves.

16. This Private Information was compromised due to Defendant’s negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members. In addition to Defendant’s failure to prevent the Data Breach, after discovering the breach, Defendant waited several months to report it to government agencies and affected individuals.

17. As a result of this delayed response, Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

18. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant’s failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant’s inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant’s conduct amounts to negligence and violates federal and state statutes.

19. Plaintiff and Class Members have suffered injury as a result of Defendant’s conduct. These injuries include: (i) lost or diminished value of Private Information; (ii) out-of-

pocket expenses associated with the 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, including but not limited to lost time, and (iv) the continued and substantially increased risk to their Private Information which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up 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.

20. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

21. As a result of the Data Breach, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

22. Plaintiff is a citizen of Pennsylvania.

23. Defendant Keystone Health is a 501(c) Pennsylvania-based healthcare provider that is the only federally qualified Community Health Center serving Franklin County, Pennsylvania. Its principal place of business is located at 111 Chambers Hill Dr., Chambersburg, PA 17201.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant.⁴ Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

25. This Court has personal jurisdiction over Defendant because it operates and are headquartered in this District and conduct substantial business in this District.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

Keystone Health

27. Defendant is a health network located in Central Pennsylvania.

28. In its ordinary course of business, Defendant requires its patients to provide names, Social Security numbers, and clinical information as a condition to receive treatment from Defendant.

29. As a healthcare network and provider, Defendant is a HIPAA covered business associate that provides healthcare services to patients.

30. As a healthcare network and provider, Defendant collects and stores patients' Private Information.

⁴ See, e.g., <https://dojmt.gov/consumer/databreach/> (showing 78 Montanans affected by the Data Breach).

31. Defendant is required under federal and state law to maintain the strictest confidentiality of the patients' Private Information that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

32. As a HIPAA covered business entity, Defendant is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule⁵ and to report any unauthorized use or disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

33. As a condition of receiving treatment and/or treatment-related services, Defendant requires that patients, including Plaintiffs and Class Members, entrust it with highly sensitive personal information.

34. Due to the nature of Defendant's business of providing healthcare services, Defendant would be unable to engage in its regular business activities without collecting and aggregating Personal Information that it knows and understands to be sensitive and confidential.

35. Defendant's Privacy Policy recognizes its responsibility to safeguard Plaintiff's and Class Members' Private Information.⁶

36. Defendant's Notice of Privacy Policies states that Defendant is "required by law to maintain the privacy and security of your protected health information."⁷ It also states that

⁵ The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. See 45 C.F.R. Part 160 and Part 164, Subparts A and C.

⁶ <https://keystonehealth.org/wp-content/uploads/2019/01/notice-of-privacy-practices-January-2019.pdf> (last accessed: October 24, 2022).

⁷ *Id.*

Defendant “will let [patients] know promptly if a breach occurs that may have comprised the privacy or security of [patients’] information.”⁸

37. Plaintiffs and Class members are or were patients whose medical records were maintained by, or who received health-related or other services from, Keystone and directly or indirectly entrusted Keystone with their Personal Information. Plaintiffs and Class members reasonably expected that Defendant would safeguard their highly sensitive information and keep their Private Information confidential.

The Data Breach

38. On or around August 19, 2022, Defendant discovered that an unauthorized third party accessed files within its system between July 28 and August 9.⁹

39. The accessed files contained patient names, clinical information, and Social Security numbers.¹⁰

40. Despite learning of the Data Breach in August, Defendant did not notify Plaintiff and Class Members until on or around October 14, 2022.

41. According to Defendant’s submission to the United States Department of Health and Human Services Office for Civil Rights, Defendant’s Data Breach affected 235,237 individuals.

42. Based on Defendant’s admittance that an unauthorized third party accessed Defendant’s network, it is only logical to conclude that cybercriminals did in fact access Defendant’s network and exfiltrate the Plaintiff’s and Class Members’ Private Information.

⁸ *Id.*

⁹ <https://healthitsecurity.com/news/keystone-health-data-breach-impacts-phi-of-235k-individuals> (last accessed: October 24, 2022).

¹⁰ *Id.*

43. Moreover, the Private Information accessed and exfiltrated was likely not encrypted because if properly encrypted, then cybercriminals would not have acquired and accessed Plaintiff's and Class Members' Private Information.

44. Defendant had obligations under HIPAA, contract, industry standards, and common law to reasonably protect and safeguard Plaintiff's and Class Members' Private Information from unauthorized access.

45. Defendant agreed to and undertook legal duties to maintain the protected Private Information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including HIPAA.

46. The patient information held by Defendant in computer system and network included the Private Information of Plaintiff and Class Members.

47. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

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

49. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosure of this Private Information.

50. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

51. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their Private Information.

52. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

53. On information and belief, Defendant maintained the Private Information of Plaintiff and Class Members, including, but not limited to, the following: name, Social Security number, and clinical information.

54. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information.

55. As a result of Defendant's failure to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, upon information and belief, cybercriminals infiltrated Defendant's systems and stole Plaintiff's and Class Members' Private Information.

56. The unencrypted PII and PHI of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII and PHI may fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

57. Defendant admitted that Private Information potentially impacted in the Data Breach contained names, Social Security numbers, and clinical information.

58. Because Defendant failed to properly protect safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Plaintiff's and Class Members' Private Information stored on Defendant's system.

Plaintiff M.W.'s Experience

59. Plaintiff entrusted her Private Information to Defendant in order to receive medical care.

60. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

61. Plaintiff provided her Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law.

62. On or around October 14, 2022, Defendant notified Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

63. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

64. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

65. As a result of the Data Breach, Defendant directed Plaintiff to take certain steps to protect her Private Information and otherwise mitigate her damages.

66. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

67. Even with the best response, the harm caused to Plaintiff cannot be undone.

68. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

69. Defendant admits that Plaintiff's Private Information was exfiltrated by criminal third-parties. Thus, Plaintiff's and Class Members' information is already being misused by cybercriminals.

70. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

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

The Data Breach was Foreseeable

72. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹¹

73. Defendant’s data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

74. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.¹² The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

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

¹¹ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last accessed Aug. 23, 2021).

¹² See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

76. Indeed, cyberattacks 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, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals... because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹³

77. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.¹⁴

78. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Value of PII and PHI

79. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁵ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁶ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁷

¹³ FBI, Secret Service Warn of Targeted, Law360(Nov.18,2019), <https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware>

¹⁴ See Maria Hernandez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

¹⁵ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Oct. 27, 2021).

¹⁶ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Oct. 27, 2021).

¹⁷ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Oct. 27, 2021).

80. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

81. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information...[is] worth more than 10x on the black market.”¹⁸

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

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

84. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”

85. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds’ medical insurance premiums.

¹⁸ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Aug. 23, 2021).

86. According to account monitoring company LogDog, medical data, such as PHI, sells for \$50 and up on the Dark Web.¹⁹

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

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁰

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

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

90. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s network, amounting to potentially millions of individuals’ detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

¹⁹ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed July 20, 2021).

²⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Aug. 23, 2021).

91. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiff and Class Members.

92. As a condition of providing medical treatment and services, processing medical claims, sending bills, and providing collection services for treatment, Defendant requires that its patients entrust it with Private Information.

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

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

95. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendant Acquires, Collects, and Stores the Private Information of Plaintiff and Class Members

96. Defendant acquired, collected, and stored the Private Information of Plaintiff and Class Members.

97. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

98. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Failed to Properly Protect Plaintiff's and Class Members' Private Information

99. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

100. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

101. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

102. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

103. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiff and Class Members are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

104. To prevent and detect unauthorized cyber-attacks, 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 ransomware 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.
- 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 ransomware 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.²¹

105. To prevent and detect cyber-attacks, including the cyber-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 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

²¹ *Id.* at 3-4.

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....²²

106. To prevent and detect cyber-attacks, including the cyber-attack 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;

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

²² See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last accessed Aug. 23, 2021).

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].²³

107. Given that Defendant was storing the PII and PHI of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

108. 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 the PII and PHI of Plaintiff and Class Members.

109. 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 Plaintiff' and Class Members' Private Information.

110. Because Defendant failed to properly protect safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files.

²³ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last accessed Aug. 23, 2021).

111. Specifically, Defendant admits that on or around December 4, 2021, an unauthorized party accessed Defendant's network and deleted databases and system configuration files.

112. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

113. 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 the PII of Plaintiff and Class Members.

114. 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 Plaintiff's and Class Members' Private Information.

Defendant Failed to Comply with FTC Guidelines

115. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses 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.

116. 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 patient 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.²⁴

117. 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.

118. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

119. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

120. Defendant failed to properly implement basic data security practices. 56. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized

²⁴ Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

access to Plaintiff's and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

121. Defendant was always fully aware of its obligation to protect the PII and PHI of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant failed to Comply with Industry Standards

122. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

123. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

124. Other best cybersecurity practices that are standard in the healthcare industry 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; and training staff regarding critical points.

125. 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.

126. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

127. HIPAA requires covered entities and business associates of covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information. 64. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

128. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

129. 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.

130. 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." *See* 45 C.F.R. 164.40.

131. 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. See 45 C.F.R.164.308(a)(6).²⁵

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

Defendant's Negligent Acts and Breaches

133. Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their 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;
- b. Failing to adequately protect the Personal and Medical Information of Plaintiff and the Class;
- c. Failing to properly monitor their own data security systems for existing intrusions;
- d. Failing to train employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to and maintain adequate email security practices;
- e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

²⁵ See <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> at 4.

- f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- g. 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);
- h. 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);
- i. 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);
- j. 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);
- k. 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);
- l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- m. 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);
- n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it 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);
- o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and
- p. Failing to adhere to industry standards for cybersecurity.

134. As the result of antivirus and malware protection software in need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would

protect against cyberattacks like the one here, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Personal and Medical Information by allowing providing unsecured and unencrypted Personal and Medical Information to Defendant which in turn allowed cyberthieves to access its IT systems.

135. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

As a Result of Defendant's Failure to Safeguard Private Information, Plaintiff and the Class Members have Experienced Substantial Harm and Will Face Significant Risk of Continued Identity Theft.

136. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PHI that can be directly traced to Defendant.

137. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

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

139. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PHI is used;
- b. The diminution in value of their PHI;

- c. The compromise and continuing publication of their PHI;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended 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 and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PHI; and
- h. The continued risk to their PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PHI in their possession.

140. Stolen PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to \$1,000.00 depending on the type of information obtained.

141. The value of Plaintiff's and the proposed Class's PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

142. It can take victims years to spot identity or PHI theft, giving criminals plenty of time to milk that information for cash.

143. One such example of criminals using PHI for profit is the development of "Fullz" packages.

144. Cyber-criminals can cross-reference two sources of PHI 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. These dossiers are known as "Fullz" packages.

145. The development of “Fullz” packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff’s and the proposed Class’s 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 PHI stolen by the cyber-criminals in the Data Breach, criminals can 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. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and other members of the proposed Class’s stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

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

147. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.” Defendant did not rapidly report to Plaintiff and the Class that their PHI had been stolen.

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

149. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their

reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

150. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

151. The Federal Trade Commission (“FTC”) has also recognized that consumer data is a new and valuable form of currency. In a FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.”²⁶

152. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.

²⁶ Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited October 6, 2022).

153. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.²⁷ The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

154. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Plaintiff's and Class Members' Damages

155. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

156. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

²⁷ See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen> (last visited October 10, 2022).

157. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

158. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

159. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

160. Plaintiff 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 more effectively target such schemes to Plaintiff and Class Members.

161. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

162. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

163. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

164. Plaintiff and Class Members have been damaged by the compromise of their Personal and Medical Information in the cyber-attack. Moreover, Defendant's delay in noticing

affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

165. Plaintiff and Class Members have suffered or will suffer 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 value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts; and
- f. Closely reviewing and monitoring Social Security number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

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

167. Moreover, Plaintiff and Class Members have an interest in ensuring that their Personal and Medical 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 Personal and Medical Information is not accessible online and that access to such data is password protected.

CLASS ALLEGATIONS

168. Plaintiff brings this nationwide class action on behalf of herself 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.

169. The Nationwide Class that Plaintiff seek to represent is defined as follows:

All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach (the “Class”).

170. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

171. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

172. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are in excess of 235,000 individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant’s records.

173. 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 and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

- b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. 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;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- k. Whether Defendant violated the consumer protection statutes invoked herein;
- l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

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

175. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

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

177. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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.

178. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff 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 Member 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 Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member 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.

179. 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 demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

181. Unless a Class-wide injunction is issued, Defendant may continue in their 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.

182. Further, Defendant has 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.

183. 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 Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff 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 an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendant breached the implied contract;
- f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. 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;
- h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and
- i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

(On Behalf of Plaintiff and the Putative Rule 23 Class)

184. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

185. Plaintiff and the Class entrusted Defendant with their Private Information.

186. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

187. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

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

189. Defendant 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 includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class Members in Defendant's possession was adequately secured and protected.

190. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations.

191. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

192. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

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

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

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

196. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

197. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

198. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

199. Defendant had and continue to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Info by third parties.

200. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

201. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

202. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

203. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

204. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

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

206. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information they were no longer required to retain pursuant to regulations.

207. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

208. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

209. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

210. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

211. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

212. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

213. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

214. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act 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 Plaintiff and the Class.

215. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of 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, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and 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 Plaintiff and the Class.

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

217. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain 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 its continued possession.

218. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Putative Rule 23 Class)

219. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

220. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

221. In its Privacy Policy, Defendant represented that it would not disclose Plaintiff's and Class Members' Private Information to unauthorized third-parties.

222. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

223. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

224. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff 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.

225. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
NEGLIGENCE PER SE
(On behalf of Plaintiff and the Putative Rule 23 Class)

226. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

227. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

228. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff and Class Members' Private Information.

229. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, 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." *See* definition of encryption at 45 C.F.R. § 164.304.

230. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

232. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

233. The injury and harm suffered by Plaintiff 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 Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

COUNT IV
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Putative Rule 23 Class)

235. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

236. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Private Information; (2) to timely notify Plaintiff 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.

237. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure their Private Information.

238. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

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

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

241. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

242. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff 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 Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

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

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Putative Rule 23 Class)

244. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

245. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information.

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

247. 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 Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

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

250. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

251. Plaintiff and Class Members have no adequate remedy at law.

252. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their PII; (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 remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails 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 Plaintiff and Class Members.

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

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

COUNT VI
PROMISSORY ESTOPPEL
(On behalf of Plaintiff and the Putative Rule 23 Class)

255. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

256. Defendant promised through its Privacy Policy that its “office privacy policy regarding [patient] medical record[s] is designed to be compliant with all applicable state and Federal laws, including HIPAA.”

257. It was foreseeable that Plaintiff and Class Members would reasonably rely on this promise because Defendant is a reputed and established medical services provider with multiple locations.

258. Plaintiff and Class Members, to their substantial detriment, did in fact rely on Defendant’s promise as contained in its Privacy Policy.

259. Furthermore, if Defendant had made it known to Plaintiff and Class Members that it would not have safeguarded Plaintiff and Class Members’ Private Information, Plaintiff and Class Members would not have agreed to receive medical services from Defendant.

260. As a direct and proximate result of their reliance on Defendant’s promise through its Privacy Policy, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, 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 remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails 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 Plaintiff and Class Members.

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

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiff and the Putative Rule 23 Class)

262. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

263. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

264. Defendant owes a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiffs' and Class members' Private Information.

265. Defendant failed to fulfill its duty of care to safeguard Plaintiff's and Class Members' Private Information.

266. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's 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's failure to address the security failings that led to such exposure.

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

268. Plaintiff therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, 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 its 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 its 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, patient personally identifiable information and patient protected health information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class, and appointing Plaintiff and her 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 the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;

- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal

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

- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: October 25, 2022

Respectfully Submitted,

/s/

Randi Kassan

Randi Kassan

MILBERG COLEMAN BRYSON PHILLIPS

GROSSMAN, PLLC

100 Garden City Plaza

Garden City, NY 11530

Telephone: (212) 594-5300

rkassan@milberg.com

Gary M. Klinger *
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (202) 429-2290
gklinger@milberg.com

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

**Pro Hac Vice Application forthcoming*

Counsel for Plaintiff and Putative Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Keystone Health Hit with Class Action Over 2022 Data Breach Affecting 235K Patients](#)
